AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

EMERGING THREATS: OVERCLASSFICATION AND PSEUDO-CLASSIFICATION

HEARING

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS, AND INTERNATIONAL RELATIONS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

MARCH 2, 2005

Serial No. 109–18

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

20–922 PDF WASHINGTON : 2005

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 GOVERNMENT REFORM

TOM DAVIS, Virginia, *Chairman*

CHRISTOPHER SHAYS, Connecticut
DAN BURTON, Indiana
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
JOHN L. MICA, Florida
GIL GUTKNECHT, Minnesota
MARK E. SOUDER, Indiana
STEVEN C. LATOURETTE, Ohio
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
JOHN J. DUNCAN, JR., Tennessee
CANDICE S. MILLER, Michigan
MICHAEL R. TURNER, Ohio
DARRELL E. ISSA, California
GINNY BROWN-WAITE, Florida
JON C. PORTER, Nevada
KENNY MARCHANT, Texas
LYNN A. WESTMORELAND, Georgia
PATRICK T. MCHENRY, North Carolina
CHARLES W. DENT, Pennsylvania
VIRGINIA FOXX, North Carolina

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
DANNY K. DAVIS, Illinois
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
CHRIS VAN HOLLEN, Maryland
LINDA T. SANCHEZ, California
C.A. DUTCH RUPPERSBERGER, Maryland
BRIAN HIGGINS, New York
ELEANOR HOLMES NORTON, District of Columbia

BERNARD SANDERS, Vermont (Independent)

MELISSA WOJCIAK, *Staff Director*
DAVID MARIN, *Deputy Staff Director/Communications Director*
ROB BORDEN, *Parliamentarian*
TERESA AUSTIN, *Chief Clerk*
PHIL BARNETT, *Minority Chief of Staff/Chief Counsel*

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS, AND INTERNATIONAL RELATIONS

CHRISTOPHER SHAYS, Connecticut, *Chairman*

KENNY MARCHANT, Texas
DAN BURTON, Indiana
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
STEVEN C. LATOURETTE, Ohio
TODD RUSSELL PLATTS, Pennsylvania
JOHN J. DUNCAN, JR., Tennessee
MICHAEL R. TURNER, Ohio
JON C. PORTER, Nevada
CHARLES W. DENT, Pennsylvania

DENNIS J. KUCINICH, Ohio
TOM LANTOS, California
BERNARD SANDERS, Vermont
CAROLYN B. MALONEY, New York
CHRIS VAN HOLLEN, Maryland
LINDA T. SANCHEZ, California
C.A. DUTCH RUPPERSBERGER, Maryland
STEPHEN F. LYNCH, Massachusetts
BRIAN HIGGINS, New York

EX OFFICIO

TOM DAVIS, Virginia

HENRY A. WAXMAN, California

LAWRENCE J. HALLORAN, *Staff Director and Counsel*
J. VINCENT CHASE, *Chief Investigator*
ROBERT A. BRIGGS, *Clerk*
ANDREW SU, *Minority Professional Staff Member*

CONTENTS

	Page
Hearing held on March 2, 2005	1
Statement of:	
Ben-Veniste, Richard, Commissioner, National Commission on Terrorist Attacks Upon the United States	88
Blanton, Thomas, executive director, National Security Archive, George Washington University; Harry A. Hammitt, editor and publisher, Access Reports: Freedom of Information; Sibel Edmonds, former Contract Linguist, Federal Bureau of Investigation	109
Blanton, Thomas	109
Edmonds, Sibel	147
Hammitt, Harry A.	128
Leonard, J. William, Director, Information Security Oversight Office, National Archives and Records Administration; Rear Admiral Christopher A. McMahon, U.S. Maritime Service, Acting Director, Departmental Office of Intelligence, Security and Emergency Response, Department of Transportation; and Harold C. Relyea, Specialist in National Government, Congressional Research Service, Library of Congress	44
Leonard, J. William	44
McMahon, Rear Admiral Christopher A.	53
Relyea, Harold C.	66
Letters, statements, etc., submitted for the record by:	
Ben-Veniste, Richard, Commissioner, National Commission on Terrorist Attacks Upon the United States:	
Letters dated February 11 and March 1, 2005	107
Prepared statement of	93
Blanton, Thomas, executive director, National Security Archive, George Washington University, prepared statement of	114
Edmonds, Sibel, former Contract Linguist, Federal Bureau of Investigation:	
Letters dated June 19, 2002 and August 13, 2002	149
Prepared statement of	186
Report dated January 2005	154
Hammitt, Harry A., editor and publisher, Access Reports: Freedom of Information, prepared statement of	130
Higgins, Hon. Brian, a Representative in Congress from the State of New York, prepared statement of	42
Kucinich, Hon. Dennis J., a Representative in Congress from the State of Ohio, prepared statement of	9
Leonard, J. William, Director, Information Security Oversight Office, National Archives and Records Administration, prepared statement of	47
Maloney, Hon. Carolyn B., a Representative in Congress from the State of New York, prepared statement of	33
McMahon, Rear Admiral Christopher A., U.S. Maritime Service, Acting Director, Departmental Office of Intelligence, Security and Emergency Response, Department of Transportation, prepared statement of	55
Relyea, Harold C., Specialist in National Government, Congressional Research Service, Library of Congress, prepared statement of	68
Shays, Hon. Christopher, a Representative in Congress from the State of Connecticut, prepared statement of	3
Waxman, Hon. Henry A., a Representative in Congress from the State of California:	
Letter dated March 1, 2005	15
Prepared statement of	27

EMERGING THREATS: OVERCLASSFICATION AND PSEUDO-CLASSIFICATION

WEDNESDAY, MARCH 2, 2005

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS, AND INTERNATIONAL RELATIONS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The committee met, pursuant to notice, at 1 p.m., in room 2154, Rayburn House Office Building, Hon. Christopher Shays (chairman of the subcommittee) presiding.

Present: Representatives Shays, Kucinich, Maloney, Waxman, Marchant, Turner, Dent, Van Hollen, Higgins, and Ruppersberger.

Staff present: Lawrence Halloran, staff director and counsel; J. Vincent Chast, chief investigator; R. Nicholas Palarino, senior policy advisor; Robert Briggs, clerk; Hagar Hajjar, professional intern; Andrew Su, minority professional staff member; and Jean Gosa, minority assistant clerk.

Mr. SHAYS. A quorum being present, the Subcommittee on National Security, Emerging Threats, and International Relations hearing entitled, "Emerging Threats, Overclassification and Pseudo-Classification," is called to order.

The cold war cult of secrecy remains largely impervious to the new security imperatives of the post-September 11 world. Overclassification is a direct threat to national security. Last year, more Federal officials classified more information and declassified less than the year before.

In our previous hearing on official secrecy policies, the Department of Defense [DOD], witness estimated that fully half of all the data deemed "confidential, secret or top secret" by the Pentagon was needlessly or improperly withheld from public view. Further resisting the call to move from a need to know to a need to share standard, some agencies have become proliferators of new categories of shielded data. Legally ambiguous markings, like sensitive but unclassified, sensitive homeland security information and for official use only, create new bureaucratic barriers to information sharing. These pseudo-classifications can have persistent and pernicious practical effects on the flow of threat information.

Today Chairman Davis, Government Management Subcommittee Chairman Platts and I asked the Government Accountability Office [GAO], to analyze the scope and impact of these categories on critical information sharing. The National Commission on Terrorist Attacks upon the United States, referred to as the 9/11 Commission, concluded that "Current security requirements nurture overclassi-

fication and excessive compartmentalization of information among agencies. Each agency's incentive structure opposes sharing with risks, criminal, civil and internal administrative sanctions, but few rewards for sharing information. No one has to pay the long term cost of overclassifying information, though these costs are substantial."

Those costs are measured in lives as well as dollars. Somewhere in the vast cache of data that never should have been classified, and may never be declassified is that tiny nugget of information that if shared, it could be used to detect and prevent the next deadly terrorist attack. Recently enacted reforms should help focus and coordinate disparate elements of the so-called intelligence community to broaden our view of critical threat information.

The previously ignored, but still unfunded public interest declassification board has new authority to push for executive branch adherence to disclosure standards, particularly with regard to congressional committee requests. But those promising initiatives still confront deeply entrenched habits and cultures of excessive secrecy. The 9/11 Commission successfully worked through security barriers to access and publish the information they needed. But as soon as the Commission's legal mandate expired, heavy-handed declassification practices reasserted themselves. As a result, release of the final staff report on threats to civil aviation was delayed, and the version finally made public contains numerous redactions, some of which needlessly seek to shield information already released by other agencies.

The cold war was a struggle of the industrial age. The global war against terrorism is being waged and must be won by the new rules of the information age. Data and knowledge are the strategic elements of power. With such a few keystrokes, individuals and groups can now acquire technologies and capabilities once the solve province of Nation States. Modern adaptable networks asymmetrically attack the rigid hierarchical structures of the past.

In this environment, there is security in sharing, not hoarding information that many more people need to know. We asked our witnesses this afternoon in our three panels to help us assess the impact of current access restrictions on efforts to create the trusted networks and new information sharing pathways critical to our national security. We look forward to their testimony and thank them for their presence.

At this time the Chair would recognize the ranking member of the subcommittee, Mr. Kucinich.

[The prepared statement of Hon. Christopher Shays follows:]

TOM DAVIS, VIRGINIA,
CHAIRMAN

CHRISTOPHER SHAYS, CONNECTICUT
DAN BURTON, INDIANA
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
JOHN L. MICA, FLORIDA
GIL GUTKNECHT, MINNESOTA
[illegible]K E. SOLIDER, INDIANA
[illegible]N C. LATOURETTE, OHIO
RUSSELL PLATTS, PENNSYLVANIA
[illegible]S CANNON, UTAH
JOHN J. DUNCAN, JR., TENNESSEE
CANDICE MILLER, MICHIGAN
MICHAEL R. TURNER, OHIO
DARRELL ISSA, CALIFORNIA
VIRGINIA BROWN-WAITE, FLORIDA
JON C. PORTER, NEVADA
KENNY MARCHANT, TEXAS
LYNN A. WESTMORELAND, GEORGIA
PATRICK T. McHENRY, NORTH CAROLINA
CHARLES W. DENT, PENNSYLVANIA
VIRGINIA FOXX, NORTH CAROLINA

ONE HUNDRED NINTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
FACSIMILE (202) 225–3974
MINORITY (202) 225–5051
TTY (202) 225–6852

http://reform.house.gov

HENRY A. WAXMAN, CALIFORNIA,
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
DANNY K. DAVIS, ILLINOIS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
CHRIS VAN HOLLEN, MARYLAND
LINDA T. SANCHEZ, CALIFORNIA
C.A. DUTCH RUPPERSBERGER,
MARYLAND
BRIAN HIGGINS, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA

BERNARD SANDERS, VERMONT,
INDEPENDENT

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS,
AND INTERNATIONAL RELATIONS
Christopher Shays, Connecticut
Chairman
Room B-372 Rayburn Building
Washington, D.C. 20515
Tel: 202 225-2548
Fax: 202 225-2382

Statement of Rep. Christopher Shays
March 2, 2005

The Cold War cult of secrecy remains largely impervious to the new security imperatives of the post-9/11 world. Overclassification is a direct threat to national security.

Last year, more federal officials classified more information, and declassified less, than the year before. In our previous hearing on official secrecy policies, the Department of Defense (DOD) witness estimated that fully half of all the data deemed "Confidential," "Secret" or "Top Secret" by the Pentagon was needlessly or improperly withheld from public view. Further resisting the call to move from a "need to know" to a "need to share" standard, some agencies have become proliferators of new categories of shielded data. Legally ambiguous markings like "Sensitive but Unclassified", "Sensitive Homeland Security Information" and "For Official Use Only" create new bureaucratic barriers to information sharing. These pseudo-classifications can have persistent and pernicious practical effects on the flow of threat information.

The National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission) concluded that, "Current security requirements nurture overclassification and excessive compartmentation of information among agencies. Each agency's incentive structure opposes sharing, with risks (criminal, civil and internal administrative sanctions) but few rewards for sharing information. No one has to pay the long-term costs of over-classifying information, though these costs… are substantial."

Those costs are measured in lives as well as dollars. Somewhere in the vast cache of data that never should have been classified, and may never be declassified, is that tiny nugget of information that, if shared, could be used to detect and prevent the next deadly terrorist attack.

Recently enacted reforms should help focus and coordinate disparate elements of the so-called "intelligence community" to broaden our view of critical threat information. The previously ignored, and still unfunded, Public Interest Declassification Board has new authority to push for executive branch adherence to disclosure standards, particularly with regard to congressional committee requests.

But those promising initiatives still confront deeply entrenched habits and cultures of excessive secrecy. The 9/11 Commission successfully worked through security barriers to access and publish the information they needed. But as soon as the Commission's legal mandate expired, heavy-handed classification practices reasserted themselves. As a result, release of the final staff report on threats to civil aviation was delayed. And the version finally made public contains numerous redactions, some of which needlessly seek to shield information already released by other agencies.

The Cold War was a struggle of the Industrial Age. The global war against terrorism is being waged, and must be won, by the new rules of the Information Age. Data and knowledge are the strategic elements of power. With just a few keystrokes, individuals and groups can now acquire technologies and capabilities once the sole province of nation-states. Modern, adaptable networks asymmetrically attack the rigid, hierarchical structures of the past.

In this environment, there is security in sharing, not hording, information that many more people need to know. We asked our witnesses this afternoon to help us assess the impact of current access restrictions on efforts to create the trusted networks and new information sharing pathways critical to our national security. We look forward to their testimony.

TOM DAVIS, VIRGINIA,
CHAIRMAN

CHRISTOPHER SHAYS, CONNECTICUT
DAN BURTON, INDIANA
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
JOHN L. MICA, FLORIDA
GIL GUTKNECHT, MINNESOTA
MARK E. SOUDER, INDIANA
STEVEN C. LaTOURETTE, OHIO
TODD RUSSELL PLATTS, PENNSYLVANIA
CHRIS CANNON, UTAH
JOHN J. DUNCAN, JR., TENNESSEE
CANDICE MILLER, MICHIGAN
MICHAEL R. TURNER, OHIO
DARRELL ISSA, CALIFORNIA
VIRGINIA BROWN-WAITE, FLORIDA
JON C. PORTER, NEVADA
KENNY MARCHANT, TEXAS
LYNN A. WESTMORELAND, GEORGIA
PATRICK T. McHENRY, NORTH CAROLINA
CHARLES W. DENT, PENNSYLVANIA
VIRGINIA FOXX, NORTH CAROLINA

ONE HUNDRED NINTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
FACSIMILE (202) 225–3974
MINORITY (202) 225–5051
TTY (202) 225–6852

http://reform.house.gov

HENRY A. WAXMAN, CALIFORNIA,
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
DANNY K. DAVIS, ILLINOIS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
CHRIS VAN HOLLEN, MARYLAND
LINDA T. SANCHEZ, CALIFORNIA
C.A. DUTCH RUPPERSBERGER, MARYLAND
BRIAN HIGGINS, NEW YORK
ELEANOR HOLMES NORTON, DISTRICT OF COLUMBIA

BERNARD SANDERS, VERMONT,
INDEPENDENT

March 1, 2005

The Honorable David M. Walker
Comptroller General of the United States
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Walker:

We are writing to request a Government Accountability Office (GAO) study of a critical aspect of homeland security -- the ability of the Federal government to share information.

Information sharing continues to be a significant challenge for federal, state and local government despite efforts by Congress to improve information sharing at all levels. Most recently, the Intelligence Reform and Terrorism Prevention Act of 2004 established specific information sharing requirements for federal agencies. In addition, GAO recently added homeland security information sharing to its list of high-risk programs and initiatives in the government.

One of the challenges facing federal information sharing efforts stems from the lack of government-wide policies and procedures for handling sensitive but unclassified information. Since September 11, 2001, a number of different categories of information are increasingly being combined. For example, law enforcement sensitive information, security sensitive information, critical infrastructure information, could all potentially be placed into a single document. However, these categories of information all have different methods of care, penalties for unauthorized disclosure, and written guidance. As a result, it becomes very difficult to share data among federal agencies. Furthermore, some protection requirements hinder the timely dissemination of the data to state and local entities. This is only one small example of the challenges we must overcome to ensure that federal information sharing efforts for homeland security result in meaningful exchanges of data that will protect the Nation from future threats.

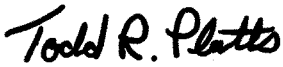
Accordingly, I would like GAO to examine the major challenges related to information sharing including: (1) identifying all of the different types of homeland security related

information classifications and the various handling protocols; (2) reviewing current policies and efforts for establishing government-wide processes for moving homeland security data between federal agencies and between federal, state, local, and private sector entities; (3) identifying who has the responsibility for establishing the overall systems design; and (4) providing an overview of the technologies and mechanisms that might facilitate such information sharing efforts.

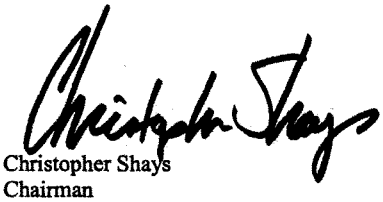
Thank you for your attention to this matter. Time frames for this review should be discussed and agreed upon with Committee staff as GAO conducts its work. Please contact Victoria Proctor or Jaime Hjort at (202) 225-5074 if you need additional information regarding this request.

Sincerely,

Tom Davis
Chairman



Todd Platts
Chairman
Subcommittee on Government
Management, Finance and
Accountability



Christopher Shays
Chairman
Subcommittee on National Security,
Emerging Threats, and International Relations

cc: The Honorable Henry A. Waxman
Ranking Minority Member

Mr. KUCINICH. I thank the Chair.

Good afternoon to all the witnesses and to members of the committee. Mr. Chairman, I believe in addition to the problem that this committee brings to light about the over-use and misuse in the classification of Federal documents, it could be said that the real problem before us goes beyond that. It's not the quantity of materials classified and declassified, it's not about which words are missing or about the implausible justifications based upon our national security. The real and growing problem we must address is the reflexive secrecy rampant through the administration.

The American people cannot get straight answers about the situation in Iraq, about the treatment of detainees at Abu Ghraib or at Guantanamo Bay, Cuba. The American people cannot get the intelligence budget of the United States, the American people cannot get the truth about Social Security. The American people have a right to know and to get the unbiased facts from their Government.

Congress also has a right to know, particularly this oversight committee, which is charged to find waste, fraud and abuse. Yet even before this committee we have heard a Department of Defense official tell us that last August she believed 50 percent of all materials are mis-classified at the Pentagon. Some believe the number is higher.

Instead of making information available or sharing information, the current administration has reversed the trend toward openness started under the Clinton administration. Instead of a presumption against classifying a document in case of doubt with the use of a lower level of classification when the appropriate level of classification was uncertain, this was used during the Clinton administration, the current administration's policy is simple: withhold the truth from the public through what you could call hyperclassification.

The Bush administration has dramatically increased the volume of Federal materials concealed from the American people. The President's Executive Order 13292, issued in March 2003, permitted officials to classify information when there was doubt whether or not to do so, and allowed officials to classify information at the more restrictive level when there was a question as to the appropriate level. We now have new and more levels of restricted access to information, such as the "sensitive but unclassified" and "critical infrastructure information" designations. Instead of utilizing the interagency security classification appeals panel established by President Clinton, where historical records were declassified at record rates and on a timely automated schedule, this administration's Executive order has delayed and weakened the system of automatic declassification and under-utilized the appeals panel.

Most tellingly, this administration didn't even include funds for the public interest declassification board in its fiscal year 2006 proposed budget. The administration's excessive use of classification restrictions on dissemination and release of documents delays in declassifying materials and disrespect toward open government is really a danger to our democracy.

It's a common assertion by this administration that we need to be secret to be safe. But the fact of the matter is, as has been stated by one of the witnesses we are going to hear from, we're losing

protection by too much secrecy. And this climate of secrecy is antithetical to a democratic society. This climate of secrecy takes us toward a type of government which is not democratic, which is profoundly undemocratic, which has that kind of a stale, garbage-like whiff of fascism to it.

So this is a serious matter that is up for discussion today. But we really need to go beyond it. Because while we're sitting here discussing this matter, the administration is moving ahead with policies, without the permission of the American people, spending money without the permission of the American people and cloaking it in a need for secrecy. And while they're doing it, they're tearing the Constitution to pieces.

[The prepared statement of Hon. Dennis J. Kucinich follows:]

Statement of Rep. Dennis J. Kucinich
Ranking Minority Member
House Subcommittee on National Security, Emerging Threats, and International Relations

Hearing on "Emerging Threats: Overclassification and Pseudo-classification"

March 2, 2005

Good afternoon. Mr. Chairman, the real problem before us today is not the overuse and misuse in the classification of federal documents. It is not the quantity of materials classified and declassified. It is not about which words are missing or about implausible justifications based on our national security. The real and growing problem we must address is the reflexive secrecy rampant throughout the current Administration.

The American people cannot get straight answers about the situation in Iraq, or about the treatment of detainees at Abu Gharib prison or at Guantanamo Bay, Cuba. The American people cannot get the intelligence budget of the United States. The American people cannot get the truth about Social Security. Mr. Chairman,

the American people have a right to know the truth, and to get the unbiased facts from their government.

Congress also has a right to know, and particularly this oversight committee, which is charged to find waste, fraud, and abuse. Yet, even before this committee, we heard an official from the Department of Defense tell us last August that she believed 50 percent of all materials are misclassified at the Pentagon. I believe the number is much higher.

Instead of making information available or sharing information, the current Administration has reversed the trend towards openness started under the Clinton Administration. Instead of a presumption against classifying a document in cases of doubt, or the use of a lower level of classification when the appropriate level of classification was uncertain, such as was used during the Clinton White House, the current Administration's policy is simple - withhold the truth from the public through hyper-classification.

The Bush Administration has dramatically increased the volume of federal materials concealed from the American people. Bush executive order 13292 issued in March 2003 permitted officials to classify information when there was doubt whether or not to do so, and allowed officials to classify information at the more restrictive level when there was a question as to the appropriate level. We now have new and more levels of restricted access to information, such as the use of the 'Sensitive But Unclassified' and 'Critical Infrastructure Information' designations.

Instead of utilizing the interagency Security Classification Appeals Panel established by President Clinton, where historical records were declassified at record rates and on a timely, automated schedule, the Bush executive order also delayed and weakened the system of automatic declassification and underutilized the appeals panel. Most tellingly, the Bush Adminsitration didn't even include funds for the Public Interest Declassification Board in its FY06 proposed budget.

The Bush Administration's excessive use of classification, restrictions on dissemination and release of documents, delays in declassifying materials, and disrespect towards open government is beyond comparison. We must not sit idly by and allow our right to know to continue to be suppressed.

Mr. SHAYS. I thank the gentleman. I agree with many of his comments.

Mr. Marchant, our new vice chairman of the subcommittee, is recognized, if he has an opening statement.

Mr. MARCHANT. Mr. Chairman, it's a privilege for me to be on this subcommittee with you and be a vice chairman. As a freshman, I'm employing the practice of listening and learning and will have some questions later.

Mr. SHAYS. Hopefully we all will practice that. Thank you. It's wonderful to have you on the committee and as vice chairman.

Mr. Turner—I'm sorry, we did have a statement, so I'm sorry, Mr. Waxman.

Mrs. Maloney, wonderful to have you on the committee and the Chair would recognize you.

Mrs. MALONEY. I yield to Mr. Waxman.

Mr. SHAYS. Mrs. Maloney defers and yields to Mr. Waxman, the ranking member of the full committee. I guess that was an anticipation of that, Mr. Waxman.

Mr. WAXMAN. Thank you, Mr. Chairman, for holding this hearing and for your leadership in addressing the issue of government secrecy. Incredibly, it seems to necessary to state the obvious today: the Government belongs to the people. The American people understand that some information must be kept secret to protect the public safety. But when the Government systematically hides information from the public, Government stops belonging to the people.

Unfortunately, there have been times in our Nation's history when this fundamental principle of openness has come under attack. The Watergate era of the Nixon administration was one of those times. We are now living through another.

Over the last 4 years, the executive branch has engaged in a systematic effort to limit the application of the laws that promote open government and accountability. Key open government laws, such as the Freedom of Information Act, the Presidential Records Act and the Federal Advisory Committee Act, have been narrowed and misconstrued. At the same time, the administration has greatly expanded its authority to classify documents, to conduct secret investigations and to curtail Congress' access to information.

Last fall, I released a report entitled Secrecy in the Bush administration. This detailed many of these threats to the principle of open government. And Mr. Chairman, I would like to ask unanimous consent to put this report into the hearing record for today.

Mr. SHAYS. Without objection, this report will be put into the record.

[NOTE.—The minority report entitled, "Secrecy in the Bush Administration," may be found in subcommittee files.]

Mr. WAXMAN. Yesterday, I wrote a letter to Chairman Shays that described a new threat to openness in government, the administration's mis-use of rapidly proliferating designations, such as sensitive but classified, and for official use only, to block the release of important information. I would also ask unanimous consent that

this letter be made a part of today's hearing as well, Mr. Chairman, unanimous consent to make my letter to you part of the record.

Mr. SHAYS. Yes, thank you, your letter will be part of the record.

[The information referred to follows:]

TOM DAVIS, VIRGINIA,
CHAIRMAN

CHRISTOPHER SHAYS, CONNECTICUT
DAN BURTON, INDIANA
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
JOHN L. MICA, FLORIDA
GIL GUTKNECHT, MINNESOTA
MARK E. SOUDER, INDIANA
STEVEN C. LaTOURETTE, OHIO
TODD RUSSELL PLATTS, PENNSYLVANIA
CHRIS CANNON, UTAH
JOHN J. DUNCAN, JR., TENNESSEE
CANDICE MILLER, MICHIGAN
MICHAEL R. TURNER, OHIO
DARRELL ISSA, CALIFORNIA
VIRGINIA BROWN-WAITE, FLORIDA
JON C. PORTER, NEVADA
KENNY MARCHANT, TEXAS
LYNN A. WESTMORELAND, GEORGIA
PATRICK T. McHENRY, NORTH CAROLINA
CHARLES W. DENT, PENNSYLVANIA
VIRGINIA FOXX, NORTH CAROLINA

ONE HUNDRED NINTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
FACSIMILE (202) 225–3974
MINORITY (202) 225–5051
TTY (202) 225–6852

http://reform.house.gov

HENRY A. WAXMAN, CALIFORNIA,
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
DANNY K. DAVIS, ILLINOIS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
CHRIS VAN HOLLEN, MARYLAND
LINDA T. SANCHEZ, CALIFORNIA
C.A. DUTCH RUPPERSBERGER, MARYLAND
BRIAN HIGGINS, NEW YORK
ELEANOR HOLMES NORTON, DISTRICT OF COLUMBIA

BERNARD SANDERS, VERMONT,
INDEPENDENT

March 1, 2005

The Honorable Christopher Shays
Chairman
Subcommittee on National Security, Emerging
Threats, and International Relations
Committee on Government Reform
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

In its final report on the attacks of September 11, 2001, the 9/11 Commission observed that the government keeps too many secrets. To address this problem, the Commission recommended that the "culture of agencies feeling they own the information they gathered at taxpayer expense must be replaced by a culture in which the agencies instead feel they have a duty … to repay the taxpayers' investment by making that information available."[1]

Unfortunately, there is growing evidence that the executive branch has increased the amount of information withheld from the American public and misused rapidly proliferating designations such as "sensitive but unclassified," "for official use only," "sensitive homeland security information," and "sensitive security information" to block the release of important government records.

My staff has investigated several examples of the use of these burgeoning designations. We have found that they are being invoked improperly to block the release of information that is not classified. Some of the examples we reviewed involve absurd overreactions to vague security concerns. In other examples, the Administration appears to have invoked the designations to cover up potentially embarrassing facts, rather than to protect legitimate security interests. The examples include the following:

---

[1] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (July 22, 2004).

- The State Department withheld unclassified conclusions by the agency's Inspector General that the CIA was involved in preparing a grossly inaccurate global terrorism report;

- The State Department concealed unclassified information about the role of John Bolton, Under Secretary of State for Arms Control, in the creation of a fact sheet that falsely claimed that Iraq sought uranium from Niger;

- The Department of Homeland Security concealed the unclassified identity and contact information of a newly appointed TSA ombudsman whose responsibility it was to interact daily with members of the public regarding airport security measures;

- Over the objections of chief U.S. weapons inspector Charles A. Duelfer, the CIA Mr. Duelfer to conceal the unclassified names of U.S. companies that conducted business with Saddam Hussein under the Oil for Food program; and

- The Nuclear Regulatory Commission sought to prevent a nongovernmental watchdog group from making public criticisms of its nuclear power plant security efforts based on unclassified sources.

In order to investigate more fully the scope of this problem, I request that the Subcommittee conduct a systematic analysis of information that the Administration has withheld from the American public through the use of these unclassified designations. In particular, I propose that the Subcommittee obtain from multiple federal agencies, including the Departments of Defense, State, and Homeland Security, copies of documents that exist in both a restricted but unclassified version and a public version. After obtaining these documents, the Subcommittee would be able to assess which specific pieces of information were removed and determine whether those redactions were appropriate.

I understand that the Subcommittee will be holding a hearing tomorrow on precisely this type of "pseudo-classification" of information by the Administration, and I commend you for taking this step. I hope we will have the opportunity at that time to discuss this proposal in more detail. The rest of this letter sets forth additional information on the examples described above.

Background

The Administration treats restricted unclassified information differently than traditional classified information. Classified information is governed by relatively uniform rules across federal agencies, and only a limited number of authorized personnel are permitted to designate information as classified. In addition, there are guidelines on how information must be declassified.

In contrast, restricted but unclassified information lacks even minimal controls or monitoring. It is governed by a rapidly evolving patchwork of disparate agency regulations and directives. Generally, any federal employee has authority to designate documents as "sensitive but unclassified," there are no uniform rules about when or how to remove these designations, and there are few checks in place to control the abuse of such designations. To the contrary, these designations appear to be used as automatic or default markings on many federal documents that government officials have not sufficiently reviewed.

In many cases, these unclassified designations have questionable legal pedigrees. For example, the designation "sensitive but unclassified" is not defined by statute or even by executive order. And unlike the criteria for categories of classified information, the criteria for many of the sensitive but unclassified designations are wholly the executive branch's invention.

For classified information, there is a single office charged with overseeing the classification process. This office, the Information Security Oversight Office (ISOO) at the National Archives and Records Administration, reported that in fiscal years 2001 to 2003, the average number of original classifications per year increased 50% over the average for the previous five fiscal years.[2] ISOO also reported that during this time, the average number of derivative classifications increased to 19.37 million per year, a 95% increase over the period from fiscal years 1996 to 2000.[3]

Unfortunately, there is no office comparable to the ISOO that monitors trends in the use of sensitive but unclassified information. And watchdog groups are severely hampered in their efforts to collect information about the propriety of the Administration's use of these restricted unclassified designations.

In order to investigate this issue, my staff examined several documents issued by the Administration in both public and restricted but unclassified formats. Instances in which the Administration appears to have inappropriately withheld information from the public are described below. To be clear, none of these examples involved classified information. Instead, the relevant information was withheld by federal agencies using various other rationales or, in some cases, no stated rationale at all.

---

[2] National Archives and Records Administration, Information Security Oversight Office, *Report to the President 2003* (Mar. 31, 2004). *See also White House Takes Secrecy to New Levels, Coalition Reports,* San Francisco Chronicle (Aug. 27, 2004).

[3] *Id. See also* OpenTheGovernment.org, *Secrecy Report Card: Quantitative Indicators of Secrecy in the Federal Government* (Aug. 26, 2004) (online at www.openthegovernment.org/otg/secrecy_reportcard.pdf) (reporting that the Administration spent $6.5 billion last year creating and maintaining classified documents, more than it spent during the entire decade previously).

Concealment of the CIA's Role in a Faulty Annual Terrorism Report

In September 2004, the State Department withheld from the public unclassified conclusions by its Inspector General that the CIA was involved in preparing a grossly inaccurate report on global terrorism. The report in question falsely claimed that terrorist events fell to a record low in 2003, when in fact significant terrorist attacks reached a record high.

Each year, the State Department produces the authoritative *Patterns of Global Terrorism* report on the total number of terrorist attacks throughout the world. The 2003 report claimed "the lowest annual total of international terrorist attacks since 1969."[4] After the report was issued, however, I joined two independent experts in questioning the report's data and conclusions. As we pointed out, the State Department made obvious errors in undercounting the number of terrorist events and failed to report that significant terrorist attacks actually reached a 20-year high in 2003.[5] Secretary of State Powell ultimately conceded that the "fact-checking, the methodology and at times even the math were flawed."[6]

In September 2004, the State Department Inspector General's office completed an unclassified analysis of the flawed *Patterns* report. The IG issued two versions of its final assessment: one to government officials marked "sensitive but unclassified,"[7] and another to the general public via the Department's website.[8] The second version was altered from the original and redacted in several places.

---

[4] U.S. Department of State, *Patterns of Global Terrorism — 2003* (Apr. 2004). *See also* U.S. Department of State, *Release of the 2003 "Patterns of Global Terrorism" Annual Report* (Apr. 29, 2003) (online at www.state.gov/s/d/rm/31961.htm) (quoting Deputy Secretary of State Richard Armitage stating that the data in the report provided "clear evidence that we are prevailing in the fight"); Letter from Paul V. Kelly, Assistant Secretary of State for Legislative Affairs, to Members of Congress (Apr. 29, 2004) (stating that the data was "an indication of the great progress that has been made in fighting terrorism").

[5] Letter from Rep. Henry A. Waxman to Secretary of State Colin L. Powell (May 17, 2004). *See also* Professors Alan B. Krueger and David Laitin, *Faulty Terror Report Card,* Washington Post (May 17, 2004).

[6] Letter from Secretary of State Colin L. Powell to Rep. Henry A. Waxman (June 28, 2004).

[7] U.S. Department of State, Office of the Inspector General, *Review of the Department's Patterns of Global Terrorism — 2003 Report* (Sept. 2004) (Report Number SIO-S-04-18) ("sensitive but unclassified" version).

[8] U.S. Department of State, Office of the Inspector General, *Review of the Department's Patterns of Global Terrorism — 2003 Report* (Sept. 2004) (online at http://oig.state.gov/documents/organization/41085.pdf) (Report Number SIO-S-04-18) (publicly released version).

"chronology" on how the fact sheet was developed.[14] This chronology described a meeting on December 18, 2002, between Secretary Powell, Mr. Bolton, and Richard Boucher, the Assistant Secretary for the Bureau of Public Affairs. According to this chronology, Mr. Boucher specifically asked Mr. Bolton "for help developing a response to Iraq's Dec 7 Declaration to the United Nations Security Council that could be used with the press." According to the chronology, which is phrased in the present tense, Mr. Bolton "agrees and tasks the Bureau of Nonproliferation," a subordinate office that reports directly to Mr. Bolton, to conduct the work.

This unclassified chronology also stated that on the next day, December 19, 2003, the Bureau of Nonproliferation "sends email with the fact sheet, 'Fact Sheet Iraq Declaration.doc,'" to Mr. Bolton's office (emphasis in original). A second e-mail was sent a few minutes later, and a third e-mail was sent about an hour after that. According to the chronology, each version "still includes Niger reference." Although Mr. Bolton may not have personally drafted the document, the chronology appears to indicate that he ordered its creation and received updates on its development.

The Inspector General's chronology was marked "sensitive but unclassified." In addition, the letter transmitting the chronology stated that it "contains sensitive information, which may be protected from public release under the Freedom of Information Act," and requested that no "public release of this information" be made.[15] In fact, however, the chronology consisted of nothing more than a factual recitation of information on meetings, e-mails, and documents.

Concealment of TSA Ombudsman's Identity

In February 2002, the Department of Homeland Security concealed the unclassified identity of a newly appointed ombudsman for the Transportation Security Administration (TSA) whose responsibility it was to interact daily with members of the public regarding airport security measures.

On February 14, 2002, TSA Director John W. Magaw appointed an ombudsman "to listen to a variety of concerns from passengers" and others regarding security screening methods and other issues related to the relatively new agency.[16] In making his announcement, Mr.

---

[14] Letter from Rep. Henry A. Waxman et. al to Anne W. Patterson, Deputy Inspector General, U.S. Department of State (Apr. 6, 2004) (this request was made under 5 U.S.C. §2954, the "Seven-Member Rule," which requires an executive agency to "submit any information requested of it" when sought by seven members of the House Government Reform Committee).

[15] Letter from Anne W. Patterson, Deputy Inspector General, Department of State, to Rep. Henry A. Waxman (Apr. 15, 2004).

[16] *Official to Check Screening Complaints*, Washington Post (Feb. 15, 2002).

Magaw stated, "We want to have a very simple but very complete passenger-complaint system so that we can look at them and, if feasible, make changes." He also stated that the ombudsman would sit "right off my office" and serve as a sounding board for passengers.

Despite this stated goal of interacting with members of the public, the identity of the ombudsman was withheld from the public. At the press conference in which the announcement was made, Mr. Magaw "declined to name the appointee."[17] In addition, at a subsequent briefing to Congress in January 2004, TSA officials provided a slide marked "sensitive security information" that stated: "How to contact the Ombudsman — Phone: 1-571-227-2383 or 1-877-266-2837 (toll-free)."[18]

Ironically, a cursory Google search reveals that both the identity of the ombudsman, Kimberly Hubbard Walton, and her contact information had been posted as part of a release on the TSA management team on the TSA's own website.[19]

There have been similar accounts relating to other federal government employees. According to the publication *Government Executive,* for example, the Defense Department telephone book has now been designated "for official use only," even though it was formerly publicly available at the Government Printing Office.[20]

Concealment of U.S. Companies Involved in the Oil for Food Program

In September 2004, the CIA intervened to block the chief U.S. weapons inspector, Charles A. Duelfer, from revealing the unclassified identities of U.S. companies that conducted business with Saddam Hussein under the Oil for Food program.

On September 30, 2004, Mr. Duelfer issued an unclassified report regarding the absence of weapons of mass destruction in Iraq.[21] As part of this report, Mr. Duelfer implicated a number of oil and energy services companies in schemes to assist Saddam Hussein in diverting funds away from legitimate humanitarian purposes under the Oil for Food program. Although the

---

[17] *Id.*

[18] Briefing to House Committee on Homeland Security, *Transportation Security Intelligence Service* (Jan. 8, 2004).

[19] TSA, *TSA Announces New Additions to the TSA Management Team* (Jan. 24, 2003) (online www.tsa.gov/public/display?content=090005198000f2e2).

[20] *Groups Raise Concerns about Increased Classification of Documents,* Government Executive (Oct. 27, 2004).

[21] Iraq Survey Group, *Comprehensive Report of the Special Advisor to the DCI on Iraq's WMD* (Sept. 30, 2004).

report named all foreign companies that received vouchers for the purchase of Iraqi oil, the names of U.S. corporations were redacted, even though they had received 20 contracts to procure over 71 million barrels of oil from Iraq. The U.S. companies listed in the restricted report include:

Companies	Barrels of Oil
Coastal Petroleum	36.0 million
Chevron	9.5 million
Mobil Export	9.3 million
Phoenix International	9.1 million
Bay Oil	5.6 million
Texaco	1.8 million

In addition to these six companies, Halliburton was also doing business in Iraq, apparently under the Oil for Food program.[22] Halliburton's contracts came to light after Vice President Cheney claimed he had instituted "a firm policy that we wouldn't do anything in Iraq, even — even arrangements that were supposedly legal."[23]

The public version of Mr. Duelfer's report removed the names of the American corporations and replaced them with the generic term "U.S. Company." In addition, the report stated: "The names of US citizens and business entities have been redacted from this report in accordance with provisions of the Privacy Act, 5 U.S.C. 552a, and other applicable law."[24]

When asked why the Bush Administration concealed this information, Mr. Duelfer testified to the Senate that he had wanted to identify the U.S. companies, but was overruled. According to Mr. Duelfer, "it was my view to put forward all the data ... because I felt it was important." But "with respect to the American names," Mr. Duelfer said, the Administration would not allow it.[25] According to Mr. Duelfer, CIA officials warned him that "the Privacy Act, you know, prohibits the public — putting out publicly American names." The CIA told Mr.

---

[22] *Firm's Iraq Deals Greater Than Cheney Has Said,* Washington Post (June 23, 2001) (stating that Halliburton held stakes in two firms, Dresser-Rand and the Ingersoll Dresser Pump Company, that signed contracts to sell more than $73 million in oil production equipment and spare parts to Iraq while Vice President Cheney was chairman and chief executive officer).

[23] *This Week,* ABC News (July 30, 2000) (when pressed further, the Vice President stated: "we've not done any business in Iraq since the sanctions are imposed, and I had a standing policy that I wouldn't do that").

[24] Iraq Survey Group, *Comprehensive Report of the Special Advisor to the DCI on Iraq's WMD* (Sept. 30, 2004) (online at www.cia.gov/cia/reports/iraq_wmd_2004).

[25] *Hearing of the Senate Armed Services Committee: Duelfer Report on Iraqi Weapons of Mass Destruction Programs,* Federal News Service (Oct. 6, 2004).

Duelfer that the information was not classified, but that it should be withheld nonetheless. As Mr. Duelfer stated: "they said look, this is the law."

Contrary to the information provided to Mr. Duelfer, however, the Privacy Act does not apply to corporations, but rather to individuals. The U.S. Code defines the term "individual" in the context of the Privacy Act as "a citizen of the United States or an alien lawfully admitted for permanent residence."[26] Corporations are not "citizens" under the Privacy Act.

Concealment of a Report Criticizing Faulty Nuclear Security Exercises

On August 4, 2003, the Chairman of the Nuclear Regulatory Commission (NRC) asserted in a letter to Congress that mock attack exercises with private security contractors at the Indian Point nuclear facility in New York demonstrated the strength of security measures there. In a letter to Senator Charles Schumer, the NRC Chairman stated that "force on force exercises at Indian Point indicates that the licensee has a strong defensive strategy and capability."[27] Another member of the NRC said: "Indian Point is our star; it did famously."[28]

In a highly critical letter on September 11, 2003, however, the nonprofit Project on Government Oversight (POGO) took issue with these statements, detailing numerous flaws with the exercises.[29] POGO based its findings on unclassified interviews with participants and observers of the exercises.

In particular, POGO highlighted that the exercises "used an inadequate and unrealistically low number of attackers," did not allow mock attackers to use "basic, readily-available weapons," conducted all exercises "during the daylight," and required mock attackers to use "only one entry point." The letter also condemned the NRC's "unacceptably poor planning" in failing to inform the Coast Guard about the exercise, resulting in Coast Guard personnel threatening to use "live ammo against the mock attackers." As POGO concluded, these exercises "should not in any way reassure you about the ability of the Indian Point security force to defend that facility against a credible terrorist attack."

In response to POGO's letter, the NRC directed the group not to make public its concerns and to remove its letter from its website. In a letter sent four days after receiving POGO's letter,

---

[26] 5 U.S.C. § 552a(a)(2).

[27] Letter from Niles J. Diaz, Chairman, Nuclear Regulatory Commission, to Senator Charles Schumer (Aug. 4, 2003).

[28] *Group Says Test of Nuclear Plant's Security Was Too Easy,* New York Times (Sept. 16, 2003) (quoting Commissioner Edward McGaffigan, Jr.).

[29] Letter from Danielle Brian, Executive Director, Project on Government Oversight, to Niles J. Diaz, Chairman, Nuclear Regulatory Commission (Sept. 11, 2003).

the NRC stated that it had identified both classified "Safeguards Information" and unclassified "sensitive homeland security information" that was for "official use only."[30] Yet the NRC informed POGO that it would not "identify what portions of your letter needed to be redacted so that you could put a redacted version of your letter on your website."[31]

Rather than identifying the passages of concern, according to POGO, the NRC "threatened us with criminal and civil sanctions were we to continue to make public either our letter or any of the sensitive material it allegedly contained."[32] Indeed, an October 8, 2003, letter from the NRC warned POGO "once again" that it would face "criminal penalties" if it did not "permanently remove from [its] website the entire letter."[33]

Since the NRC refused to identify any specific portions of the letter with classified or sensitive information, POGO could neither publish nor discuss any matter identified in the letter. As a result, POGO concluded that the NRC "took this position to stifle legitimate criticism of the agency."[34] POGO's concern was not with NRC efforts to protect classified information about the facility's defenses, but with NRC attempts to bar the publication of the entire report when it was based entirely on public sources critical of those defenses.

Rather than let the matter drop, POGO retained counsel to pursue legal action against the NRC for stifling its free speech. As a result, the NRC ultimately reversed its position, stating that "it has now become apparent that our general guidance was insufficient."[35] The NRC agreed to identify the specific information it believed should not be made public and informed POGO of these passages. None of the information ultimately identified by the NRC was classified or otherwise outside the public domain. After an impasse of three months, POGO issued a redraft of its original letter on December 9, 2003, with only minor changes to the text.[36]

---

[30] Letter from Annette L. Vietti-Cook, Secretary, Nuclear Regulatory Commission, to Danielle Brian, Executive Director, Project on Government Oversight (Sept. 15, 2003).

[31] Letter from Roy P. Zimmerman, Director, Office of Nuclear Security and Incident Response, Nuclear Regulatory Commission, to Danielle Brian, Executive Director, Project on Government Oversight (Oct. 8, 2003).

[32] Letter from Danielle Brian, Executive Director, Project on Government Oversight, to Chairman Niles J. Diaz, Nuclear Regulatory Commission (Dec. 9, 2003).

[33] Letter from Roy P. Zimmerman, *supra* note 31.

[34] Letter from Danielle Brian, *supra* note 32.

[35] Letter from Roy P. Zimmerman, Director, Office of Nuclear Security and Incident Response, Nuclear Regulatory Commission, to David C. Vladeck and Richard McKewen, Institute for Public Representation (Oct. 28, 2003).

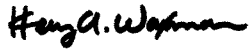
[36] Letter from Danielle Brian, *supra* note 32.

Conclusion

These examples are alarming. Democracies need openness and accountability to thrive. Yet under the Bush Administration, the executive branch is creating new categories of "sensitive but unclassified" information that are invoked to deny public access to important government information. These designations lack a statutory basis, and there is no federal entity monitoring their use. As a result, Congress and the American people have little idea how frequently the Administration is withholding information under these rapidly proliferating unclassified designations.

I know that you share my concern with this problem. Last year, you stated that "fewer people classifying fewer secrets would better protect national security by focusing safeguards on truly sensitive information while allowing far wider dissemination of the facts and analysis the 9/11 commission says must be shared."[37] In this spirit, I hope we can work together in bringing sunlight onto this issue. I look forward to speaking with you further.

Sincerely,



Henry A. Waxman
Ranking Minority Member

[37] *White House Takes Secrecy to New Levels, Coalition Reports*, San Francisco Chronicle (Aug. 27, 2004).

Mr. WAXMAN. Many of these new designations have been created out of thin air by the administration. They do not have a basis in Federal statute, and there are no criteria to guide their application. It appears that virtually any Federal employee can stamp a document "sensitive but unclassified" and there do not appear to be uniform procedures for removing these designations. The examples we discovered are alarming. The executive branch has been using these novel designations to withhold information that is potentially embarrassing, not to advance national security.

Last year I wrote a letter to Secretary Powell that revealed that the State Department's annual terrorism report was grossly inaccurate. This Government report claimed that terrorist attacks reached an all-time low in 2003. In fact, exactly the opposite was true. Significant attacks by terrorists actually reached an all-time high.

To his credit, Secretary Powell admitted that mistakes were made and required the issuance of a new report. Several months later, the inspector general prepared a report that examined what went wrong. The report was released to the public in one version. And another version, a "sensitive but unclassified" version, was sent to certain offices in Congress. My staff compared the two versions. They were identical except for one difference. The "sensitive but unclassified" version reported that the CIA played a significant role in preparing the erroneous report. This information was redacted in the public version.

I have a message for the administration. Admitting that the CIA made a mistake is not a national security secret. Another example involves the role that Under Secretary of State John Bolton played in preparing an infamous fact sheet that erroneously alleged that Iraq tried to import uranium from Niger. The State Department wrote me in September 2003 that Mr. Bolton "did not play a role in the creation of this document." But a "sensitive but unclassified" chronology, which has never been released to the public, shows that actually Mr. Bolton did direct the preparation of the fact sheet and received multiple copies of the draft.

Apparently, sensitive but unclassified is also a code word for embarrassing to senior officials. And here's an ironic example. The Department of Homeland Security used the sensitive but unclassified designation to withhold the identity of the ombudsman that the public is supposed to contact about airline security complaints. I suggested to Chairman Shays that this subcommittee should investigate the mis-use of these designations, and I am glad to report that he has agreed. In fact, we are signing letters today seeking information from several agencies about the way they use these new designations. With his support, I hope we can impose some restraints on this new form of government secrecy.

There are other issues I hope we can examine today. One involves the process that was used to declassify important 9/11 Commission documents. Last month, we learned about long delays in the declassification and release of key documents that called into question statements made by now-Secretary of State Condoleezza Rice and other senior administration officials. These embarrassing documents were not released until after the Presidential elections and 48 hours after Ms. Rice's confirmation as Secretary of State.

Today I hope we can learn more about the delay in the release of these documents and whether politics played any role.

Another important topic is the case of Sibel Edmonds, who will testify on the third panel. Ms. Edmonds joined the FBI in 2001 as a linguist. But she was fired just a few months later for warning her superiors about potential espionage occurring with the Bureau. Last month, the Justice Department Inspector General released an unclassified report that vindicated Ms. Edmonds, finding that her core allegations were clearly corroborated. Yet the Justice Department has repeatedly sought to prevent inquiries into her case by citing secrecy concerns. Indeed, government lawyers even argued that her legal efforts to obtain redress should be thrown out of court to avoid the risk of disclosing sensitive information.

Mr. Chairman, let me close by thanking you for holding this hearing, for investigating the problematic, sensitive but unclassified designation and for including Ms. Edmonds in the hearing. This hearing and your actions demonstrate that openness in government is not a partisan issue. The fact is, there is bipartisan concern in Congress that the pendulum is swinging too far toward secrecy. I look forward to the testimony of the witnesses today.

[The prepared statement of Hon. Henry A. Waxman follows:]

TOM DAVIS, VIRGINIA,
CHAIRMAN

CHRISTOPHER SHAYS, CONNECTICUT
DAN BURTON, INDIANA
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
JOHN L. MICA, FLORIDA
GIL GUTKNECHT, MINNESOTA
MARK E. SOUDER, INDIANA
STEVEN C. LATOURETTE, OHIO
TODD RUSSELL PLATTS, PENNSYLVANIA
CHRIS CANNON, UTAH
JOHN J. DUNCAN, JR., TENNESSEE
CANDICE MILLER, MICHIGAN
MICHAEL R. TURNER, OHIO
DARRELL ISSA, CALIFORNIA
VIRGINIA BROWN-WAITE, FLORIDA
JON C. PORTER, NEVADA
KENNY MARCHANT, TEXAS
LYNN A. WESTMORELAND, GEORGIA
PATRICK T. McHENRY, NORTH CAROLINA
CHARLES W. DENT, PENNSYLVANIA
VIRGINIA FOXX, NORTH CAROLINA

ONE HUNDRED NINTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
FACSIMILE (202) 225–3974
MINORITY (202) 225–5051
TTY (202) 225–6852

http://reform.house.gov

HENRY A. WAXMAN, CALIFORNIA,
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
DANNY K. DAVIS, ILLINOIS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
CHRIS VAN HOLLEN, MARYLAND
LINDA T. SANCHEZ, CALIFORNIA
C.A. DUTCH RUPPERSBERGER,
MARYLAND
BRIAN HIGGINS, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA

BERNARD SANDERS, VERMONT,
INDEPENDENT

Statement of Rep. Henry A. Waxman, Ranking Minority Member
Committee on Government Reform
Subcommittee on National Security, Emerging Threats, and International Relations
Hearing on
"Overclassification and Pseudo-classification"

March 2, 2005

Thank you, Mr. Chairman, for holding this hearing, and for your leadership in addressing the issue of government secrecy.

Incredibly, it seems necessary to state the obvious today — the government belongs to the people. The American people understand that some information must be kept secret to protect the public safety. But when the government systematically hides information from the public, government stops belonging to the people.

Unfortunately, there have been times in our nation's history when this fundamental principle of openness has come under direct attack. The Watergate era of the Nixon Administration was one of those times. We are now living through another.

Over the last four years, the executive branch has engaged in a systematic effort to limit the application of the laws that promote open government and accountability. Key open government laws such as the Freedom of Information Act, the Presidential Records Act, and the Federal Advisory Committee Act have been narrowed and misconstrued. At the same time, the Administration has greatly expanded its authority to classify documents, to conduct secret investigations, and to curtail Congress's access to information.

Last fall, I released a report entitled "Secrecy in the Bush Administration" that detailed many of these threats to the principle of open government. I ask unanimous consent that this report be made part of today's hearing record.

Yesterday, I wrote a letter to Chairman Shays that described a new threat to openness in government: the Administration's misuse of rapidly proliferating designations such as "sensitive but unclassified" and "for official use only" to block the release of important information. And I ask unanimous consent that this letter also be made part of today's hearing record.

Many of these new designations have been created out of thin air by the Administration. They do not have a basis in federal statute. And there are no criteria to guide their application. It appears that virtually any federal employee can stamp a document "sensitive but unclassified," and there do not appear to be uniform procedures for removing these designations.

The examples we discovered are alarming. The executive branch has been using these novel designations to withhold information that's potentially embarrassing, not to advance national security.

Last year, I wrote a letter to Secretary Powell that revealed that the State Department's annual terrorism report was grossly inaccurate. This government report claimed that terrorist attacks reached an all-time low in 2003. In fact, exactly the opposite was true: significant attacks by terrorists actually reached an all-time high.

To his credit, Secretary Powell admitted that mistakes were made and required the issuance of a new report.

Several months later, the Inspector General prepared a report that examined what went wrong. The report was released to the public in one version. And another version – a "sensitive but unclassified" version – was sent to certain offices in Congress.

My staff compared the two versions. They were identical except for one difference: the "sensitive but unclassified" version reported that the CIA played a significant role in preparing the erroneous report. This information was redacted in the public version.

I have a message for the Administration: admitting that the CIA made a mistake is not a national security secret.

Another example involves the role that Under Secretary of State John Bolton played in preparing an infamous fact sheet that erroneously alleged that Iraq tried to import uranium from Niger. The State Department wrote me in September 2003 that Mr. Bolton "did not play a role in the creation of this document." But a "sensitive but unclassified" chronology – which has never been released to the public – shows that actually Mr. Bolton did direct the preparation of the fact sheet and received multiple copies of the draft.

Apparently, "sensitive but unclassified" is also a codeword for "embarrassing to senior official."

And here's an ironic example: the Department of Homeland Security used the "sensitive but unclassified" designation to withhold the identity of the ombudsman that the public is supposed to contact about airline security complaints.

I suggested to Chairman Shays that the Subcommittee should investigate the misuse of these designations, and I am glad to report that he has agreed. In fact, we are signing letters today seeking information from several agencies about the way they use these new designations.

With his support, I hope that we can impose some restraints on this new form of government secrecy.

There are other issues I hope we can examine today. One involves the process that was used to declassify important 9/11 Commission documents. Last month, we learned about long delays in the declassification and release of key documents that called into question statements made by Secretary of State Condoleezza Rice and other senior Administration officials. These embarrassing documents were not released until after the presidential elections and after Ms. Rice's confirmation. Today, I hope we can learn more about the delay in the release of these documents and whether politics played any role.

Another important topic is the case of Sibel Edmonds, who will testify on the third panel. Ms. Edmonds joined the FBI in 2001 as a linguist, but she was fired just a few months later for warning her superiors about potential espionage occurring within the Bureau. Last month, the Justice Department Inspector General released an unclassified report that vindicated Ms. Edmonds, finding that her core allegations were "clearly corroborated."

Yet the Justice Department has repeatedly sought to prevent inquiries into her case by citing secrecy concerns. Indeed, government lawyers even argued that her legal efforts to obtain redress should be thrown out of court to avoid the risk of disclosing sensitive information.

Mr. Chairman, let me close by thanking you for holding this hearing, for investigating the problematic "sensitive but unclassified designation," and for including Ms. Edmonds in the hearing. This hearing – and your actions – demonstrate that openness in government is not a partisan issue. The fact is, there is bipartisan concern in Congress that the pendulum is swinging too far toward secrecy.

I look forward to the testimony of today's witnesses.

Mr. SHAYS. I thank the gentleman for his statement and for the work of his staff. You have done a lot of work that you have reason to be very concerned about.

At this time the Chair would recognize Mr. Turner, the former vice chairman of the committee, now chairman of?

Mr. TURNER. Federalism and Census. Thank you, Mr. Chairman, and thank you for your leadership on this issue, and for your assistance in my continuing on this subcommittee. This obviously is a very important issue. Just this week I believe we had a reminder of the issue of classification when we were all receiving information from our news media about the possible communication between Osama bin Ladin and Moussaoui, and looking to possible potential attacks on the United States. I think we all heard, as we looked at the news, and read the news accounts, that we were informed that the Homeland Security Department issued a classified bulletin to officials over the weekend about the intelligence, which spokesman Brian—I'm not even going to guess at that one—described as credible but not specific. The indulgence was obtained over the past several weeks, officials said.

Clearly, we've gotten to the point where we have become desensitized to what is either classified or not. One of the dangers of overclassification is that people no longer handle the information sensitively. In this instance, within I believe a day or two of it being issued, it's national news on CNN and all of our newspapers, which of course means that our adversaries, in addition to our friends, are reading it.

This is an important hearing that you are holding, in that it will assist us in identifying what really is important and needs to be protected information and hopefully assist us in keeping it classified and confidential.

Thank you.

Mr. SHAYS. I thank the gentleman for his statement. At this time, the Chair would recognize the gentlelady from New York City.

Mrs. MALONEY. Clearly, for me, nothing highlights better the overclassification of government documents than the 9/11 Commission staff report dealing with civil aviation. The release of this report was delayed for months beyond all documents of the 9/11 Commission report, and is heavily redacted. It is the only document that the 9/11 Commission members received that had one word covered in ink. Every other document that they received in their investigation was not redacted, just the civil aviation one.

Not only is it ironic that the underlying 9/11 Commission report spoke to the need to move from a need to know environment to a need to share environment. I think it is absolutely an outrage that large portions and parts of this report are being kept from the American people, including the September 11 families who fought so very, very hard to get answers on why September 11 happened, and how we could work to prevent it in the future, another future attack.

Although the 9/11 Commission staff completed its report on August 26, 2004, the Bush administration refused to declassify the findings until January 28, 2005, less than 48 hours after Condoleezza Rice was confirmed as Secretary of State. During the

period between August 26th and January 28th, the Commission was reportedly reviewing the Commission's report to determine whether it contained any information that should be classified in the interest of national security.

Problems with this process have been raised previously by the 9/11 Commission. On February 9th, the New York Times reported that the monograph had been turned over to the National Archives nearly 2 weeks before it had been heavily redacted. No notice was provided to me or any of the 25 Members of Congress who had written the Justice Department for its release. To say the least, the contents of the monograph were troubling. It states that,

> In the months before September 11, Federal aviation officials reviewed dozens of intelligence reports that warned about Osama bin Ladin and Al-Qaeda, some of which specifically discussed airline hijackings and suicide operations.
>
> Fifty-two intelligence reports from the FAA mentioned bin Ladin or Al-Qaeda from April to September 10, 2001. Five of the intelligence reports specifically mentioned Al-Qaeda's training or capability to conduct hijackings. And two mentioned suicide operations, although not connected to aviation. Despite these warnings, the FAA, lulled into a false sense of security and intelligence that indicated a real and growing threat leading up to 9/11, did not stimulate significant increase in security procedures.

This is what we know from public parts of the report. That day Chairman Shays and I called on the Justice Department to release the full, unredacted report, just like all previous documents of the 9/11 Commission. The delayed release, the ultimate timing of the release, the contents and the heavy redactions raise very serious concerns to me. That is why I was so pleased to join with the full committee ranking member, Henry Waxman, calling for hearings on this matter. I look very much forward to hearing from 9/11 Commissioner Richard Ben-Veniste, who will be testifying on this, along with the other witnesses.

In our letter, we raise concerns on whether the administration mis-used the classification process to withhold, possibly for political reasons, and it questions the veracity of statements, briefings and testimony by then National Security Advisory Condoleezza Rice, regarding this issue. I have concerns that the administration abused the classification process to improperly withhold the 9/11 Commission findings from Congress and the public, until after the November elections and the confirmation of Condoleezza Rice as Secretary of State.

I really want to learn today what were the specific rationales for each redaction in the report, and were these redactions appropriate. I have one example that is on display right now, where no one can argue that it is not over-classification. On this board you can clearly see the public testimony of Mike Canavan, a top FAA official before the 9/11 Commission on May 23, 2003. On this board is the same testimony partially redacted. The testimony that is blacked out reads, "We are hearing this, this, and this from this organization. It was just a gain in the chatter piece, so to speak."

So I truly do not understand why public testimony that is released to the public could ever end up covered by black ink and officially redacted.

With regard to our questions surrounding Secretary Rice, during her tenure as President Bush's national security advisor, she made several categorical statements asserting that there were never any

warnings that terrorists might use airplanes and suicide attacks. One possibility is that Secretary Rice was unaware of the extensive FAA warnings when she appeared before the press and testified before the 9/11 Commission. This would raise serious questions about her preparation.

Another possibility is that Secretary Rice knew about the FAA warnings but provided misleading information to the Commission. Neither of these possibilities would reflect well on Secretary Rice. Perhaps there are other, more innocent explanations for these seeming inconsistencies.

I look forward to the testimony of our witnesses, and I hope to find out how, when and why this document was classified. Finally, I would like to thank Chairman Shays, in accommodating our request for including Sibel Edmonds as a witness. I would like to welcome her. She will be testifying publicly for the first time ever before Congress, despite the fact that she was wrongly fired by the FBI 3 years ago for trying to do her patriotic duty by raising concerns with possible espionage within the FBI.

Even though the Justice Department Inspector General found that her claims had merit, the administration to this day has not fully investigated these serious issues, and amazingly, has still not made Ms. Edmonds whole. I hope that this situation will change, and I look forward to understanding how new designations that have no basis in Federal law or statute came into existence. Secrecy in government, particularly on public policy issues, ones from which we want to learn in order to prevent such actions in the future, are very, very serious, and I welcome the chairman and the ranking member's efforts. I'm glad to join them in this effort.

Thank you.

[The prepared statement of Hon. Carolyn B. Maloney follows:]

Statement of Congresswoman Maloney
March 2, 2005
Emerging Threats: Overclassification and Pseudo-classification
2154 Rayburn House Office Building
1 p.m.

For me nothing highlights better the
over-classification of government documents
than the 9/11 Commission staff report
dealing with civil aviation.

The release of this report was delayed for months
beyond all documents of the 9/11 Commission
and is heavily redacted.

It is the only document of the Commission to have
even one word covered in black ink.

Not only is it ironic that the underlying 9/11
Commission Report spoke to the need to move
from a "need to know" environment to a
"need to share" environment,
I think it is an outrage that large parts of this report
are being kept from the American public,
including the 9/11 Families
who fought so hard to get answers
on why 9/11 happened and

how we prevent future attacks.

Although the 9/11 Commission staff
completed its report on August 26, 2004,
the Bush Administration refused to declassify
the findings until January 28, 2005,
less than 48 hours after Condoleeza Rice was
confirmed as Secretary of State.

During the period between August 26 and
January 28, the Administration was reportedly
reviewing the Commission's report
to determine whether it contained any information
that should be classified in the interest of national
security.

Problems with this process had been raised
previously by the 9/11 Commission.

On February 9th the New York Times reported that
the Monograph had been turned over to the
National Achieves nearly two weeks before and
it had been heavily redacted.

No notice was provided to me or any of the 25 Members of Congress who had written the Justice Department for its release.

To say the least, the contents of the monograph were troubling.

It states that in the months before 9/11, federal aviation officials reviewed dozens of intelligence reports that warned about Osama bin Laden and Al Qaeda, some of which specifically discussed airline hijackings and suicide operations.

52 intelligence reports from the FAA mentioned Bin Laden or Al Qaeda from April to September 10, 2001.

Five of the intelligence reports specifically mentioned Al Qaeda's training or capability to conduct hijackings,
and two mentioned suicide operations, although not connected to aviation.

Despite these warnings the FAA was

"lulled into a false sense of security," and "intelligence that indicated a real and growing threat leading up to 9/11 did not stimulate significant increases in security procedures."

This is what we know from the public parts of the report.

That day Chairman Shays and I called on the Justice Department to release the full, unredacted report – just like all previous documents of the 9/11 Commission.

The delayed release,
the ultimate timing of the release,
the contents of the monograph
and the heavy redactions raise
serious concerns for me.

That is why I also joined with the
Full-Committee Ranking Member,
Henry Waxman calling for hearings on this matter
and I look forward to hearing from 9/11
Commissioner Richard Ben-Veniste

and our other witnesses on this later.

In our letter,
we raised concerns on whether
the Administration misused the classification
process to withhold, for political reasons
and question the veracity of statements, briefings,
and testimony by then-National Security Advisor
Condoleezza Rice regarding this issue.

I have concerns that the Bush Administration abused
the classification process to improperly withhold the
9/11 Commission findings from Congress and the
public until after the November elections and the
confirmation of Condoleezza Rice as Secretary of
State.

I want to know what were the specific rationales for
each redaction in the report?

Were these redactions appropriate?

I have one example right here were
no one can argue that it is not over-classification.

On this board you can clearly see the public testimony of Mike Canavan, a top FAA official, before the 9/11 Commission on May 23, 2003.

On this board is the same testimony partially redacted.

The testimony that is blacked-out reads "we are hearing, this, this, this, this and this from this organization. It was just again in the chatter piece, so to speak."

I just don't understand why public testimony could ever end up covered by this black ink.

With regards to our questions surrounding Secretary Rice, during her tenure as President Bush's National Security Advisor, she made several categorical statements asserting that there were never any warnings that terrorists might use airplanes in suicide attacks.

One possibility is that Secretary Rice was unaware of the extensive FAA warnings when she appeared

before the press and testified before the 9/11 Commission.

This would raise serious questions about her preparation and competency.

Another possibility is that Secretary Rice knew about the FAA warnings but provided misleading information to the public and the Commission.

Neither of these possibilities would reflect well on Secretary Rice. Perhaps there are other more innocent explanations for these seeming inconsistencies.

I look forward to the testimony of our witnesses and hope to find out how, when, and why this document was classified.

Finally, I would like to thank Chairman Shays in accommodating our requests for including Sibel Edmonds as a witness. I would like to welcome her, as she will be testifying publicly for the first time ever before Congress, despite the fact that she was

wrongly fired by the FBI three years ago for trying to do her patriotic duty by raising concerns with possible espionage within the FBI.

Even though the Justice Department Inspector General found that her claims had merit, the Administration to this day has not fully investigated these serious issues, and -- amazingly -- has still not made Ms. Edmonds whole.

To the contrary, the Administration is fighting her at every turn.

Mr. SHAYS. Before recognizing our other three members, who will have as much time as they would like, I do want to point out that Admiral McMahon has somewhat of a crisis meeting at the White House; in other words, this is not a typical meeting, you are being asked to be there for certain events that have happened today. And you will be leaving at 2:30. I just want the members to know that. I'm told that we will have votes at 2, which means they'll leave the machine open, so he'll probably get to leave at 2:15. So I'd just like the Members to be aware of that, but only because that should be information you might want to know.

Mr. Van Hollen, and then we'll go to Mr. Higgins and then to Mr. Ruppersberger.

Mr. VAN HOLLEN. Thank you, Mr. Chairman. I will be brief, just two things. First, with respect to classified information and use of classified information, abuse of classified information, there are two separate issues, and both identified by the 9/11 Commission report. One is the overcompartmentalization of legitimately classified information. They focus very much on the importance of sharing across agencies, because it doesn't do us any good in protecting our national security if one agency is sitting on a critical piece of the puzzle that when combined with another piece of the puzzle gives us a fuller picture.

Then of course there is the issue that we're looking at today, which is the overclassification of information in general. I want to thank the chairman for all his leadership on this issue and just say, it always amazes me to have briefings by Secretary Rumsfeld and others in this administration, and frankly in past administrations, in previous jobs as well, where they classified as secret or top secret, and you get into the room and you've heard what just happened had been reported on CNN or Fox News or whatever it may be, or you read it in the newspaper the next day.

It does breed a lot of cynicism about the abuse of classified information. I see it, it's just constant. Secret information is in the newspapers often before it's told to Members of Congress. I hope that we can develop a system that truly classifies the information that is critical to protect in our national security and not classify information that's an important part of the public debate in an exchange of views which is also essential to protecting our national security.

Thank you, Mr. Chairman.

Mr. SHAYS. I thank the gentleman for his statement.

Mr. Higgins, it's wonderful to have you as part of this committee.

Mr. HIGGINS. I have no questions at this time, Mr. Chairman, thank you.

[The prepared statement of Hon. Brian Higgins follows:]

Opening Statement
Representative Brian Higgins
Committee on Government Reform Subcommittee on National Security, Emerging Threats and International Relations
"Emerging Threats: Overclassification and Pseudo-classification"
March 2, 2005

One of the many lessons borne out of the tragedy of September 11, 2001 is that our nation can no longer afford any failures in bureaucracy that let crucial information fall through the cracks. As the 9/11 Commission found in its final report, agency must speak to agency and all information must be shared; that is the only way we can keep America's citizens safe from those who would do us harm. Today, we have an opportunity to tackle information sharing, or the lack thereof, by addressing two problems at the heart of this issue – the overclassification of documents by the executive branch and the hoarding of material by certain executive agencies unwilling to appropriately share the very information that could keep us safe. I thank Mr. Shays for organizing this hearing, and I thank all our panelists for sharing their experience and their expertise with us today.

To be clear, I believe the federal government, including its executive agencies, bears a responsibility to keep certain information and documents classified in order to protect the nation; few would argue otherwise. But the needless protection of information that is already public, that does not relate to national security, that does not put our country in harm's way or that is political in nature simply uses up manpower, confuses the public and actually hurts national security by watering down the very classification system the action abuses.

In addition, the withholding of information from the Congress, and from this Committee or the 9/11 Commission, as outlined by a recent report by Ranking Member Waxman, is unacceptable. It is the duty of the Committee on Government Reform to maintain proper oversight of the executive branch and its agencies and to request and receive information under the Seven Member Rule. It is not the Administration's job to

cover up information that might be politically embarrassing, by labeling it confidential or top secret.

There is another troubling aspect of document classification that I hope we will address today, regarding restrictions of access to unclassified information. Of late, there has been a promulgation of titles and restrictions on unclassified information. Executive agencies have created their own designations, their own rules and their own system in part to keep other agencies from having or understanding information that should be shared. No single agency in the executive branch can unilaterally protect us, and no single agency in the executive branch should routinely shut out another agency from the information it needs to keep us safe. The act of restricting information from another agency is unacceptable and we cannot allow such behavior to continue; as the 9/11 Commission made clear, information sharing is essential to homeland security.

President Bush recently nominated John D. Negroponte as the first Director of National Intelligence – a position created under the Intelligence Reform Act. The Director of National Intelligence (DNI) is required by law to establish a system that encourages information sharing, that sets government-wide standards, and that protects sources of information. The devil, of course, is in the details. The Senate-confirmed DNI must make information sharing a priority. In doing so, he must address the misuse of classification by this Administration to withhold information from elected officials and citizens alike. He must make declassification a main focus.

September 11, 2001 destroyed American naiveté in our belief that our government agencies were working together on our behalf. Instead, we discovered that too often, turf battles impede information sharing and put us in danger. Reforming what is and is not classified or restricted, allowing the Congress access to needlessly classified documents and setting across-agency standards that encourage rather than stifle information sharing are essential and long overdue steps we must take to ensure our safety. Thank you again, Mr. Shays, for recognizing the need for today's hearing, and thank you to our panelists for being here.

Mr. SHAYS. Thank you very much.

With that, I will announce our witnesses. I don't think Mr. Ruppersberger is here.

We have Mr. J. William Leonard, Director, Information Security Oversight Office, National Archives and Records Administration. We have Rear Admiral Christopher A. McMahon, Acting Director, Departmental Office of Intelligence, Security and Emergency Response, Department of Transportation; and Mr. Harold Relyea, Specialist in American National Government, Congressional Research Service, Library of Congress.

Gentlemen, if you will stand up, we will swear you in right away. As you know, we swear in all our witnesses.

Raising your right hand, do you solemnly swear or affirm that the testimony you will give before this subcommittee will be the truth, the whole truth and nothing but the truth?

[Witnesses sworn.]

Mr. SHAYS. Note for the record our three witnesses have responded in the affirmative. I ask unanimous consent that all members of the subcommittee be permitted to place an opening statement in the record and the record will remain open for a few days for that purpose. Without objection, so ordered.

I ask further unanimous consent that all witnesses be permitted to include their written statements in the record. Without objection, so ordered.

I thank the cooperation of the subcommittee, and Mr. Leonard, you have the floor.

STATEMENTS OF J. WILLIAM LEONARD, DIRECTOR, INFORMATION SECURITY OVERSIGHT OFFICE, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION; REAR ADMIRAL CHRISTOPHER A. McMAHON, U.S. MARITIME SERVICE, ACTING DIRECTOR, DEPARTMENTAL OFFICE OF INTELLIGENCE, SECURITY AND EMERGENCY RESPONSE, DEPARTMENT OF TRANSPORTATION; AND HAROLD C. RELYEA, SPECIALIST IN NATIONAL GOVERNMENT, CONGRESSIONAL RESEARCH SERVICE, LIBRARY OF CONGRESS

STATEMENT OF J. WILLIAM LEONARD

Mr. LEONARD. Thank you, Mr. Chairman, and I appreciate your holding this hearing today and for inviting me.

Our Nation and our Government, of course, are profoundly different in a post-September 11 world. Our citizens' sense of vulnerability has increased, as have their expectations of their Government to keep them safe. In each situation, information is crucial. On the one hand, Americans are concerned that information may be exploited by our country's adversaries to harm us. On the other hand, impediments to information sharing among Federal agencies and with State and local and private entities need to be continuously addressed in the interest of homeland security.

Even more so, the free flow of information is essential if citizens are to be informed, and if they are to hold their Government accountable. In many regards, our Government is confronted with the twin imperatives of information sharing and information protec-

tion, two responsibilities that are contained in her intention but are not incompatible.

I direct the Information Security Oversight Office under two Executive orders and applicable Presidential guidance, my office has substantial responsibilities with respect to classification of information by agencies within the executive branch. It is Executive Order 12958, as amended, that sets forth the basic framework and legal authority by which executive branch agencies classify national security information.

Pursuant to its Constitutional authority, in this order the President authorizes a limited number of officials to apply classification to certain national security related information. This authority is an essential and proven tool for defending our Nation. The ability to deceive and surprise the enemy can spell the difference between success and failure on the battlefield.

Similarly, it's nearly impossible for intelligence services to recruit human sources who often risk their lives aiding our country or to obtain assistance from other countries' intelligence services unless such sources can be assured of complete and total confidentiality. Likewise, certain intelligence methods can only work if the adversary is unaware of their existence.

Classification, of course, can be a double edged sword. Limitations on dissemination of information that are designed to deny information to the enemy on the battlefield can increase the risk of a lack of awareness on the part of our own forces, contributing to the potential for friendly fire incidents or other failures. Similarly, imposing strict compartmentalization of information obtained from human agents increases the risk that a Government official with access to other information that could cast doubt on the reliability of the agent would not know of the use of that agent's information elsewhere in the Government.

Simply put, secrecy comes at a price. I continuously encourage agencies to become more successful in factoring this reality into the overall risk equation when making classification decisions.

Classification is an important fundamental principle when it comes to national security. But it need not and it should not be an automatic first principle. In certain circumstances, even with respect to national security information, classification can run counter to our national interests. The decision to classify information or not is ultimately the prerogative of the agency original classification authorities. The exercise of agency prerogative to classify certain information has ripple effects throughout the entire executive branch. For example, it can serve as an impediment to sharing information with another agency, with State or local officials, or with the public, who generally need the information.

In delegating classification authority, the President has established clear parameters for its use and certain burdens that must be satisfied, which I have detailed in my prepared written testimony. As I testified the last time I appeared before this subcommittee, it is my view that Government classifies too much information. Primarily, I believe because classifieds often becomes an automatic decision rather than an informed, deliberate decision.

My official oversight responsibilities rest solely with classified national security information and do not extend to the various in-

formation access restrictions designations used by agencies to control some unclassified information. Nonetheless, as a minimum, I believe that proven effective attributes of the classification system can be used as benchmarks when evaluating any information protection framework. I have listed such attributes in my prepared written testimony.

Again, I want to thank you for inviting me here today, Mr. Chairman, and I would be happy to answer any questions that you or other Members may have.

[The prepared statement of Mr. Leonard follows:]

FORMAL STATEMENT

J. William Leonard

Director, Information Security Oversight Office

National Archives and Records Administration

before the

Committee on Government Reform

Subcommittee on National Security, Emerging Threats,

and International Relations

U.S. House of Representatives

March 2, 2005

Chairman Shays, Mr. Kucinich, and members of the subcommittee, I wish to thank you for holding this hearing on issues relating to information access restrictions as well as for inviting me to testify today.

Our Nation and its Government are, of course, profoundly different in a post-9/11 world. Our citizens' sense of vulnerability has increased, as have their expectations of their Government to keep them safe. In each situation, information is crucial. On the one hand, Americans are concerned that information may be exploited by our country's adversaries to harm us. On the other hand, impediments to information sharing among Federal agencies and with State, local and private entities need to be continuously addressed in the interests of homeland security. Even more so, the free flow of information is essential if citizens are to be informed and if they are to hold their

2

Government and its leaders accountable through informed participation in our electoral processes. In many regards, our Government is confronted with the twin imperatives of information sharing and information protection – two responsibilities that contain inherent tension but are not incompatible.

By section 5.2 of Executive Order 12958, as amended, "Classified National Security Information," the President established the organization I direct, the Information Security Oversight Office, often called "ISOO." We are within the National Archives and Records Administration and by law and Executive order (44 U.S.C. 2102 and sec. 5.2(b) of E.O. 12958) are supervised by the Archivist of the United States, who appoints the Director, ISOO with the approval of the President. Under Executive Orders 12958 and 12829 (which established the National Industrial Security Program) and applicable Presidential guidance, the ISOO has substantial responsibilities with respect to classification of information by agencies within the executive branch.

It is Executive Order 12958, as amended, that sets forth the basic framework and legal authority by which executive branch agencies classify national security information. Pursuant to his constitutional authority, in this Order the President authorizes a limited number of officials to apply classification to certain national security related information. This authority is an essential and proven tool for defending our nation. The ability to surprise and deceive the enemy can spell the difference between success and failure on the battlefield. Similarly, it is nearly impossible for our intelligence services to recruit human sources who often risk their lives aiding our country or to obtain assistance from

3

other countries' intelligence services, unless such sources can be assured complete and total confidentiality. Likewise, certain intelligence methods can work only if the adversary is unaware of their existence. Finally, the successful discourse between nations often depends upon constructive ambiguity and plausible deniability as the only way to balance competing and divergent national interests.

Classification, of course, can be a double-edged sword. Limitations on dissemination of information that are designed to deny information to the enemy on the battlefield can increase the risk of a lack of awareness on the part of our own forces, contributing to the potential for friendly fire incidents or other failures. Similarly, imposing strict compartmentalization of information obtained from human agents increases the risk that a Government official with access to other information that could cast doubt on the reliability of the agent would not know of the use of that agent's information elsewhere in the Government. Simply put, secrecy comes at a price. I have continuously encouraged agencies to become more successful in factoring this reality into the overall risk equation when making classification decisions.

Classification is an important fundamental principle when it comes to national security, but it need not and should not be an automatic first principle. In certain circumstances, even with respect to national security information, classification can run counter to our national interest. The decision to classify information or not is ultimately the prerogative of agency original classification authorities. The exercise of agency prerogative to classify certain information, of course, has ripple effects throughout the entire executive

branch. For example, it can serve as an impediment to sharing information with another agency, with State or local officials, or with the public, who genuinely need to know the information.

In delegating classification authority the President has established clear parameters for its use and certain burdens that must be satisfied. Specifically, every act of classifying information must be able to trace its origin to an explicit decision by a responsible official who has been expressly delegated original classification authority. In addition, the original classification authority must be able to identify or describe the damage to national security that would arise if the information were subject to unauthorized disclosure. Furthermore, the information must be owned by, produced by or for, or under the control of the U. S. Government; and finally, it must fall into one or more of the categories of information specifically provided for in the Order.[1]

As I testified the last time I appeared before this subcommittee, it is my view that the Government classifies too much information; primarily, I believe, because classification often becomes an automatic decision rather than an informed, deliberate decision. My conclusion that there is excessive classification is supported, in part, by agency input to

---

[1] Pursuant to § 1.4 of the Order, information shall not be considered for classification unless it concerns: (a) military plans, weapons systems, or operations; (b) foreign government information; (c) intelligence activities (including special activities), intelligence sources or methods, or cryptology; (d) foreign relations or foreign activities of the United States, including confidential sources; (e) scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism; (f) United States Government programs for safeguarding nuclear materials or facilities; (g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or (h) weapons of mass destruction.

my office that indicates that overall classification activity has risen steadily over the past several years. For example, based upon information furnished our office, the total number of classification decisions increased from 9 million in FY 2001 to 11 million in FY 2002, 14 million in FY 2003 and 16 million in FY 2004. For the sake of precision, I would note that, during the period from FY 2002 through FY 2004, the U.S. Government built a new structure for homeland security and engaged in wars in Afghanistan, Iraq and against al-Qaeda, so it cannot be said conclusively from these data that the increase during this period in the number of classification decisions was due solely or even substantially to the phenomenon of "over classification" as opposed to simply reflecting an increase in legitimate classification decisions as a result of the increase in the tempo of national security operations.

My official oversight responsibilities rest solely with classified national security information and do not extend to the various information access restriction designations used by agencies to control some unclassified information. Nonetheless, as a minimum, I believe the following are proven effective attributes of the classification system:

- Specificity with respect to what information is covered and what is not covered.
- Strict limitations as to who can designate information as falling under the system of controls.
- Built-in discretion that allows controls not to be applied even if the information is eligible.
- Built-in criteria that must be satisfied in order to place controls on dissemination.

- Clear designation of information requiring control to include information orally disseminated.
- Uniform standards with respect to how to handle and protect controlled information.
- A fixed duration of time for the application of controls.
- An appeal procedure whereby both authorized holders and outsiders can appeal the legitimate application of dissemination controls.
- An effective education and training program to maintain awareness.
- Built-in accountability, both for the improper application of controls and the failure to apply or follow legitimate controls.

Finally, we must avoid allowing the "need-to-know" principle to automatically override the "need-to-share" imperative.

Again, I thank you for inviting me here today, Mr. Chairman, and I would be happy to answer any questions that you or the subcommittee might have.

Mr. SHAYS. Thank you, Mr. Leonard. Admiral McMahon, you need to bring that mic a little closer, sir.

STATEMENT OF REAR ADMIRAL CHRISTOPHER A. McMAHON

Admiral MCMAHON. Thank you, Mr. Chairman, for your kindness in realizing I have to be in the White House in the next hour.

Mr. Chairman and members of the subcommittee, I'm Rear Admiral Christopher McMahon, U.S. Maritime Service, U.S. Department of Transportation. By way of introduction, I have just recently returned from Baghdad, where I have been serving as the transportation counselor and director of the Iraqi Reconstruction Management Office of Transportation at the American Embassy. In these positions, I have been responsible for Iraqi reconstruction in all modes of transportation.

I currently serve in DOT's Office of Intelligence, Security and Emergency Response, where in this capacity, among other things, I help advise the Secretary on the Department's contacts with the intelligence community, including the Department of Homeland Security and other Federal agencies involved with homeland security. I am honored to be here to discuss with you how the Department of Transportation is balancing the needs for secrecy necessary to ensure homeland security with the public's right to know its Government's activities.

At DOT, we adhere to the requirements of the Freedom of Information Act in making determinations about what information sought by the public may be disseminated and what may be lawfully withheld. We use FOIA not only to determine our responses to public information requests, but also to advise our employees on how they should treat the information they handle. In the context of protecting information vital to homeland security, our principal tool is the authority given to us and to DHS to designate information as security sensitive information [SSI].

At DOT, we use this designation only to refer to information that Congress has mandated that we protect. We also have an administrative safeguarding designation for sensitive information that is not necessarily security related that we label for official use only [FOUO], which I will discuss later in my testimony.

When Congress created the Department of Homeland Security under the Homeland Security Act of 2002, it not only transferred TSA from DOT to DHS, along with it the authority to establish SSI, but this same law gave similar authority to establish SSI within DOT. I wish to emphasize that SSI is not a security classification; hence, individuals need not have formal national security clearance to access SSI. What they must have is a need to know, and they must provide assurances that they understand and will comply with regulations related to the possession and permissible use of SSI.

In this way, we can share with other Federal agencies, State, local and tribal governments, industry and other persons with a need to know vital information related to homeland security without the fear that this information may be released to unvetted requestors.

When Secretary Mineta confronted the question of how SSI authority was to be handled within DOT, Secretary Mineta took five

very affirmative steps. First, he delegated the authority to designate information as SSI to the heads of all the operating entities within DOT, that is the administration, as it pertained to their own modes of transportation, but subject to the guidance and direction of the director of intelligence, security and emergency response, and from the Department of Transportation's general counsel's office, who is also the departmental officer for FOIA.

Second, the Secretary specifically directed that the Department not use this authority to evade its responsibilities under FOIA by stating, and I quote Secretary Mineta in part, "finding the right balance between protecting what needs to be protected and revealing what should be revealed is important. I expect all of us to give it the attention it deserves."

Third, Secretary Mineta further directed that we report to him regularly and review any case in which his authority is used to make a decision either to designate information as SSI or not to do so. Fourth, he asked the DOT Inspector General to review DOT's implementation of its SSI authority after 1 year to ensure that SSI designation process that we have in the Department is being used properly and is not being used to exempt information from public disclosure.

Finally, the Secretary directed that we coordinate with the Department of Homeland Security on how our two departments will use our parallel SSI authorities. My staff is learning day in and day out how truly challenging that charge from Secretary Mineta is, and that is to find the right balance between protecting what needs to be protected and revealing what should be revealed. However, as we use this authority to protect the American people, I have emphasized to the heads of our operating administrations that they keep in mind that our actions must always conform to the law and with the Secretary's admonition that we not use this authority to restrict unreasonably the public's right to know how we are carrying out our duties.

I want to discuss for a moment, and I've heard it mentioned in your statements, the designation, the administrative designation for sensitive information that we at DOT refer to—yes, sir?

Mr. SHAYS. Admiral, if you could try to finish up in a minute, because you will be leaving so quickly.

Admiral MCMAHON. Sure. I want to raise a final issue, and that is the Department's issue on the September 11 testimony. Questions have been raised as to the role, whether or not FAA used or the Department of Transportation used its authority to classify information in the interest of national security. The answer is no, we did not. In my testimony you will see the explanation for that.

I would also like to emphasize one last point, and that is, we have very limited SSI in place now at DOT. There are only two documents that are SSI that we have designated SSI, and in 2004 and 2005, there are no documents that we designated secret, which I think is important. So our use of SSI and secret has been extremely limited in the Department of Transportation.

I will be pleased to respond to any questions that the committee has.

[The prepared statement of Admiral McMahon follows:]

Statement of

Christopher J. McMahon, RADM, USMS

Departmental Office of Intelligence, Security, and Emergency Response

United States Department of Transportation

Before the

Subcommittee on National Security, Emerging Threats and International Relations

Committee on Government Reform

United States House of Representatives

March 2, 2005

Good afternoon, Mr. Chairman and Members of the Subcommittee, I am Rear Admiral Christopher J. McMahon, United States Maritime Service,[1] United States Department of Transportation (DOT). Recently, I returned from serving in Baghdad, where I was appointed by Secretary Mineta as Transportation Counselor and Senior Iraqi Reconstruction Management Office (IRMO) the Transportation Consultant at the American Embassy. In these positions, I was the principal representative responsible for overseeing transportation infrastructure reconstruction. Currently, I serve in DOT's Office of Intelligence, Security, and Emergency Response. In this capacity, I help oversee the Department of Transportation's contacts with the intelligence community including the Department of Homeland Security (DHS), and other Federal agencies involved with homeland security. I am honored to be here to discuss with you how the Department of Transportation is balancing the need for the secrecy necessary to ensure homeland security with the public's right to know how its Government is carrying out its duties.

At DOT, we adhere to the requirements of the Freedom of Information Act (FOIA) in making determinations about what information sought by the public may be disseminated, and what may be lawfully withheld. FOIA is a law with which we are all familiar – and yet we rely heavily on a large body of common law and commentary to interpret and explain it. We use FOIA not only to determine our responses to public information requests, but also to advise our employees on how they should treat the information that they handle. In the context of protecting information vital to homeland security, we are learning that our principle tool is the authority given to us – and given to DHS – to designate information as "Sensitive Security Information (SSI)." At DOT, we use the designation only to refer to information that Congress has mandated that we protect. We also have an administrative safeguarding designation for sensitive information that is not necessarily related to security that we label as, "For Official Use Only (FOUO)," which I will discuss later in my testimony.

[1] The United States Maritime Service is a voluntary organization established by an Act of Congress for the purpose of training United States civilians to serve on merchant vessels of the United States. Many members of the USMS serve at the United States Merchant Marine Academy, Kings Point, NY (my own normal duty station) and the five State maritime academies.

For many years, DOT's Federal Aviation Administration (FAA) had statutory authority to prevent disclosure of information related to aviation security, termed "Sensitive Security Information (SSI)." In a leading case on SSI, the court set forth three aspects of it:

- SSI may be withheld from public disclosure under FOIA.
- The information may be withheld from the public rulemaking record in an informal rulemaking.
- The information may be withheld from discovery in civil litigation.

In response to the attacks upon the United States on September 11, 2001, Congress enacted the Aviation and Transportation Security Act (ATSA) that created within DOT the new Transportation Security Administration (TSA). Under section 114(d) of ATSA, TSA, originally part of DOT, has "responsibility for security in all modes of transportation, including . . . security responsibilities over other modes of transportation that are exercised by DOT." (This authority transferred with TSA when TSA became part of the Department of Homeland Security.) ATSA also transferred from FAA to TSA the authority to designate information as SSI and expanded the scope of that authority to all modes of transportation. When Congress created DHS in the Homeland Security Act of 2002, it not only transferred TSA from DOT to DHS, but also transferred TSA's SSI authority, and gave similar authority to DOT.

Multiple sections of the U.S. Code require that the agency administering SSI authority promulgate regulations specifying the types of information qualifying for SSI treatment. FAA's regulations appeared at 14 CFR Part 191; TSA's appear at 49 CFR Part 1520, and DOT's at 49 CFR Part 15, both entitled "Protection of Sensitive Security Information."

I wish to emphasize that SSI is not a national security classification; hence, individuals need not have formal national security clearances to access SSI. What they must have is a clear "need to know," and they must provide assurances that they understand and will comply with regulations related to the possession and permissible use of SSI. In this way, we can share with other Federal agencies, State, local, and tribal governments, academia, industry, and other persons with a "need to know" information vital to homeland security without fear that we must release that same information to unvetted requestors.

When Secretary Mineta confronted the question of how SSI authority was to be handled within DOT, he took five affirmative steps:

1. He delegated the authority to designate information as SSI to the heads of all of DOT's constituent agencies as to their own modes of transportation, but subject to guidance and direction from the Director of Intelligence, Security, and Emergency Response and the Department's General Counsel (who is the Departmental officer in charge of FOIA). Before the Secretary did this, there was uncertainty about who in DOT could make an SSI determination, with the possibility that virtually anyone would be able to invoke SSI in the Secretary's name. The delegation provides clarity, structure, and accountability to the process, along with a mechanism to ensure consistency and actual security need.

2. The Secretary specifically directed that the Department not use this authority to evade its responsibilities under FOIA, saying that,

> [t]he authority to determine that information is SSI brings with it the responsibility not only to identify and protect qualifying information, but also not to reduce more than is truly needed the public's right to know how this part of its Government is carrying out its duties. Finding the right balance between protecting what needs to be protected and revealing what should be revealed is important. I expect all of us to give it the attention it deserves.

3. He further directed that we report to him regularly and review any case in which his authority is used to make a decision either to designate information as SSI or not to do so.

4. He is asking DOT's Inspector General to review DOT's implementation of its SSI authority after one year to ensure that the SSI designation process is not being used to improperly exempt information from public disclosure.

5. Finally, he directed that we coordinate with DHS on how our two departments will use their parallel SSI authorities.

My staff is learning day in and day out how truly challenging that charge from the Secretary – to find the right balance between protecting what needs to be protected and revealing what should be revealed -- can be. However, as we use this authority to protect the American people, I have emphasized to the heads of our operating administrations that they keep in mind that our actions must always conform to the law and, with the Secretary's admonition, that we not use this authority to restrict unreasonably the public's right to know how we are carrying out our duties.

As I mentioned, I want to discuss an administrative designation for sensitive information that we use at DOT—For Official Use Only (FOUO). FOUO identifies for our employees information that is sensitive and, therefore, before it is given to anyone outside the Federal Government, they are required to consult with FOIA staff. If the information does not qualify for withholding under FOIA, it must be released.[2]

As I stated earlier, this is not an easy area to understand and apply, particularly to the land modes of transportation, for which security concerns are relatively untested.

One final issue deserves attention. Questions have been raised over whether the Department

---

[2] The full warning that is to be used on such information is: "For Official Use Only. Public release to be determined under 5 USC 552." As provided in the relevant DOT directive (DOT Manual 1640.D, Classified Information Management Manual; Chapter 5, For Official Use Only Information (FOUO), 1997):

"For Official Use Only (FOUO) is not a classified information level. Information requiring FOUO marking is discussed in this document only to ensure knowledge of the requirements for unclassified marked documents. The marking FOUO shall be used only on unclassified information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA), Section 552, Title 5, U.S. Code."

of Transportation used its authority to classify information in the interest of national security to withhold from Congress and the public portions of a staff monograph of the 9.11 Commission. The answer is no, we did not. Let me explain.

In the Summer of 2004, the Department of Justice asked DOT and other agencies to review a draft of a 9.11 Commission staff monograph solely from the perspective of national security classification. The Federal Aviation Administration (FAA) made recommendations on classification of information relating to civil aviation security. (Since primary responsibility for civil aviation security had, by that time, been transferred to DHS, FAA recommended to Justice that DHS be consulted on FAA's recommendations.) FAA submitted its recommendations to Justice in mid-September 2004, within the period set by Justice. FAA had no further involvement with the issue of classifying any portion of a 9.11 Commission staff monograph.

In preparation for today's hearing, DOT's Office of Security reviewed how many original classification decisions DOT has made since 2001. This was not hard to do, since the authority to make original classification decisions is very tightly controlled at DOT; only seven people in all of DOT have original classification authority: The Secretary; Deputy Secretary; Assistant Secretary for Administration and the Assistant Secretary's Director of Security; the Departmental Director of Intelligence, Security, and Emergency Response; and the FAA Administrator and the Maritime Administrator. None of these can make an original classification higher than SECRET.

This was also not hard to do since a central accounting is kept at DOT of any decision originally to classify information. According to that accounting, in FY2001, FAA made one SECRET classification and the United States Coast Guard, now part of DHS, made one. In FY2002, FAA made six SECRET classifications and the Coast Guard made one. In FY 2003 DOT made no original security classifications. In FY2004, we also made no original security classifications.

Mr. Chairman, this concludes my prepared remarks. I would be pleased to respond to your questions.

Mr. SHAYS. Thank you. I'm going to go out of order. Mr. Relyea has graciously agreed to let questions be asked of you, primarily, Admiral, before you go. Candidly, since some of my Democratic colleagues have more questions to ask of you than we may have, we're going to start with them and keep that order, because we only have about 25 minutes for you.

At this time the Chair would recognize Mr. Waxman.

Mr. WAXMAN. Thank you very much, Mr. Chairman, for this courtesy, and Mr. Relyea, thank you also as well. The Admiral did indicate he has to leave, and I wanted to be able to ask him some questions.

I know it was short notice and you're new on the job, so I thank you for directly addressing the declassification of the 9/11 Commission staff report. As you know, the 9/11 Commission staff finished the report in August. Reviewing FAA warnings to airport security officials, the report found that "the FAA had indeed considered the possibility that terrorists would hijack a plane and use it as a weapon." Although this report was finished in August, the administration didn't release it until January 28, 2005. They said they were reviewing it for security classification issues.

This became an issue for two reasons. First, the Commission report undercut previous statements by Condoleezza Rice that nobody could have predicted that terrorists would use a hijacked airplane as a missile. Second, the report was withheld until 48 hours after she was confirmed as Secretary of State in January. This could have been a coincidence, or it could have been a mis-use of the classification system. We don't know.

But I have a list of short questions, so let me get right to them. First, you said the Justice Department asked the Transportation Department and the FAA to review the document. Who at the Justice Department was in charge of this declassification review process?

Admiral MCMAHON. Specifically, sir, I do not know the individual in charge. I would be happy to provide that information to you as appropriate.

Mr. WAXMAN. Thank you very much.

Who made the final decision on what to declassify and when?

Admiral MCMAHON. Similarly, I don't have the specific information, but we can certainly provide that for you.

Mr. WAXMAN. You said the FAA finished its review in September. Did the FAA recommend redacting any information?

Admiral MCMAHON. The FAA, under the, the FAA does not have the authority now to do that. What the FAA did, as indicated in my opening statement, it made some recommendations to the Department of Justice and that was it. It was actually the Department of Justice that took it from there, as I understand it.

Mr. WAXMAN. Do you know whether there were recommendations for redactions?

Admiral MCMAHON. I am not aware of that, sir.

Mr. WAXMAN. Are there any differences in the redactions the FAA recommended, if they did recommend some, and the final redactions in January?

Admiral MCMAHON. I am not aware of that, sir.

Mr. WAXMAN. The 9/11 Commission staff say they wrote this report so it could be fully declassified, like all the others, and that the Justice Department allowed them to retain their security clearances so they could address these classification issues. Did the FAA ever consult and negotiate with the staff of the 9/11 Commission who wrote the report?

Admiral MCMAHON. I am not aware of that, but I will say that, which I think is relevant, that the 9/11 Commission did note, "The Commission found no evidence that the FAA knew or possessed intelligence indicating that bin Ladin, Al-Qaeda or Al-Qaeda affiliates or any other group were planning to hijack commercial planes in the United States and use them as weapons." That was in the Commission report, as I understand it.

Mr. WAXMAN. Did the FAA or Justice Department ever suggest language changes that might have avoided classification?

Admiral MCMAHON. I am aware of none.

Mr. WAXMAN. During this time, did the Transportation Department or FAA have any contact with White House officials or National Security Council officials regarding this declassification process, and if so, can you please describe these contacts?

Admiral MCMAHON. I am aware of no such contact.

Mr. WAXMAN. You said FAA recommended that Justice consult the Department of Homeland Security. You also said that in the summer of 2004, Justice also asked several other agencies to do this review at the same time. Was Homeland Security left off the original list of agencies the Justice Department originally contact?

Admiral MCMAHON. I do not have that knowledge.

Mr. WAXMAN. Do you know whether the Justice Department ever contacted the Department of Homeland Security?

Admiral MCMAHON. No, I do not.

Mr. WAXMAN. Did the FAA have any interaction with the Department of Homeland Security?

Admiral MCMAHON. I do not believe so, sir. I'm not sure.

Mr. WAXMAN. OK. I appreciate your answers to the extent you are able to answer these questions. If you get other information, would you supply it to us for the record?

Admiral MCMAHON. I certainly will, sir.

Mr. WAXMAN. Thank you so much. Thank you, Mr. Chairman.

Mr. SHAYS. You have a very fine reputation, and it would be appreciated, in any of the questions that you do have knowledge of or gain knowledge of, that you would let our subcommittee know and we would definitely pass it on to Mr. Waxman.

Admiral MCMAHON. Yes, sir, we will certainly do that.

Mr. SHAYS. Thank you.

The Chair at this time would recognize Mr. Marchant.

Mr. MARCHANT. Admiral, how do you determine what information can be stamped SSI?

Admiral MCMAHON. There are a number of procedures and guidelines that are spelled out, that are quite specific. In the broadest terms, as I understand it, SSI information within the Department of Transportation pertains to information that could harm the transportation system. But it's not necessarily a threat to national security, per se. The next designation above that would be secret, and that's where it's a national security issue.

But more specifically, there are guidelines that we can provide you.

Mr. MARCHANT. You mentioned just a little earlier that there were only a couple of items now that are marked SSI or marked secret. Are there two categories there?

Admiral MCMAHON. There are. Since we have been given the authority in May 2004, and we implemented it in January, there have been two documents that we have designated SSI. They have gone through our vetting process, in other words, through the mode, through the Office of Intelligence Security and Emergency Response and through our general counsel's office, two documents.

Mr. MARCHANT. Does the DHS have the same criteria, same procedure?

Admiral MCMAHON. As I understand it, DHS has a similar authority. How they handle it within the Department of Homeland Security, I am not aware. Our Secretary has given us guidance on how he wants it done and the Secretary within the Department of Transportation.

Mr. MARCHANT. When you go up into the category of secret, are there are lot of those documents?

Admiral MCMAHON. The secret designation, again, how you designate something secret, there are only five individuals within the Department of Transportation that have that authority. They have to use designations which are much more, I think, rigid.

But we don't use that. Even though we have that authority, we don't really use it very often. In fact, in 2004 and 2005, there is no document that we have designated as secret. And by the way, one last thing on the secret, we report any secret document, as a check, we have an office that registers that and reports it to the National Archive Information Security Office. So there's a check on that as well.

Mr. MARCHANT. Do you think that DOT has reached the right balance between protecting what needs to be protected and revealing what should be revealed?

Admiral MCMAHON. Yes, sir, I do, and I think this issue that you mentioned is extremely important to Secretary Mineta. He has emphasized it, as you have seen in my opening testimony. The five parameters that he uses are extremely rigid. We are under pretty strict orders to do just that.

Mr. MARCHANT. Thank you, Mr. Chairman.

Mr. SHAYS. I thank the gentleman.

At this time the Chair would recognize for 5 minutes the gentlelady from New York, Mrs. Maloney.

Mrs. MALONEY. Thank you for your testimony. Doesn't the example that I showed earlier on the poster boards that showed the public testimony, testimony that was given publicly, was being redacted? I think that example alone casts very serious doubts as to the process used to redact the document in the first place, wouldn't you agree?

Admiral MCMAHON. Well, ma'am, I can't really speak to the document that you're referring to. I can only speak to what I'm familiar with within the Department of Transportation. As I just stated, our parameters and guidelines are extremely strict.

Mrs. MALONEY. I would assume that material that's already available to the public, testimony that's been given publicly and released to the public, I would assume there would be a guideline that public testimony that's released to the public, part of the public record, should not be redacted. That's just common sense.

Admiral MCMAHON. Yes, ma'am.

Mrs. MALONEY. And your very strict guidelines.

Admiral MCMAHON. And I can't really comment on it, except to say that again, restate what the 9/11 Commission stated that they found no evidence that FAA had done that or had withheld information, as you indicate.

Mrs. MALONEY. If you could go back and—all right, Mr. Shays.

Mr. SHAYS. What's helpful for us, Admiral, is you have experience in this area, so your opinion about the issue, whether it relates specifically to your own issue, would be helpful. So I mean, I realize you want to be somewhat cautious. But we have you here as a witness to give us your opinion about the concept.

So when I looked at that document that Mrs. Maloney had up, it did seem absurd times 10. I would think your opinion would have been somewhat similar, that you could qualify it. Was there anything in that language that would have suggested it needed to be redacted, any little thing?

Admiral MCMAHON. Mr. Chairman, I would have to—and I would be happy to offer that, but unfortunately I don't have enough knowledge of that particular document to really give you I think——

Mr. SHAYS. We were talking about that one sentence. I mean, if anything, it was just bad English, perhaps.

Admiral MCMAHON. Sir, I would have to look at it and study it more carefully to give you an opinion.

Mr. SHAYS. OK, well, we may have you back to do that.

At any rate, Mrs. Maloney.

Mrs. MALONEY. Here it is, right here, did the FAA redact this sentence? Did they?

Admiral MCMAHON. I'm not aware that the FAA did redact it, ma'am.

Mrs. MALONEY. Well, then, can you tell me who did redact it?

Admiral MCMAHON. I cannot provide that information.

Mrs. MALONEY. How can we find out?

Admiral MCMAHON. I will certainly ask our staff to look into that for you, ma'am.

Mrs. MALONEY. Would you find out who redacted it and why they redacted it?

Admiral MCMAHON. I would be very delighted to do that, ma'am.

Mrs. MALONEY. I don't see how saying, we're hearing this, this, this and this for this organization, it was just to gain a piece of chatter, I don't see how that endangers national security, do you?

Admiral MCMAHON. Not what you're highlighting, ma'am. We'll provide you that information.

Mrs. MALONEY. What defense could you or anyone possibly give for the civil aviation document to be so heavily redacted? And I repeat, it was the only document that was redacted. All the others going to the 9/11 Commission were not redacted.

And really what we need, Mr. Chairman, in looking at this, is we need a review board to look at the redactions. I thought the testimony of Mr. Leonard earlier, when he said the redactions had become almost "automatic," and people were automatically redacting things, it's just very, very troubling. I'd like it answered.

I see my time is up. But were you surprised at how long it took the civil aviation monograph to be released? Every other document had been released, and then of course, they couldn't release it until after the confirmation. Why did it take so long? Do you know why it took so much longer than all the other documents?

Admiral MCMAHON. No, ma'am, I cannot answer that.

Mrs. MALONEY. Were you surprised to see such large segments of the report redacted?

Admiral MCMAHON. I don't have enough specific information to answer the question. My staff will be in touch with yours to provide whatever information we can, ma'am.

Mr. SHAYS. Let me just thank the gentlelady for her questions and say, Admiral, you said you would come back with some information, which I know you will.

Admiral MCMAHON. Yes, Mr. Chairman.

Mr. SHAYS. I think that will be very helpful to the subcommittee.

Mr. Higgins, you have technically the floor. I technically have, but I recognize you if you would like to yield to Mr. Waxman or—would you like to do that?

Mr. WAXMAN. Thank you, Mr. Higgins. I wanted to ask some questions that Congressman Van Hollen wanted asked.

Admiral MCMAHON. Yes, sir.

Mr. WAXMAN. That's about the public statements made by Condoleezza Rice. On May 16, 2002, Ms. Rice held a press conference at the White House to address the question of what the Government knew before September 11th about the likelihood of a terrorist attack. She stated, "I don't think anybody could have predicted that these people would try to use an airplane as a missile, a hijacked airplane as a missile." This was a very significant statement coming from the President's National Security Advisor. Presumably she would not have made it without thoroughly researching the claim first.

Admiral McMahon, you were the head of intelligence and security for the Department of Transportation, which includes the Federal Aviation Administration. Your office would have been the logical first stop for Ms. Rice. Prior to holding her press conference, did Ms. Rice ever contact you or your predecessors to ask what the Department of Transportation, what the FAA knew about the possibility that terrorists might use hijacked airplanes and suicide attacks?

Admiral MCMAHON. No, sir, she did not.

Mr. WAXMAN. About 3 weeks later, on April 8, 2004, Ms. Rice testified before the 9/11 Commission, this was a rare event, a sitting National Security Advisor testifying under oath, and I'm sure Ms. Rice did a lot of preparation before that. Yet she still maintained that, "this kind of analysis about the use of airplanes as weapons actually was never briefed to us." Between the time she held her press conference at the White House and when she testi-

fied before the 9/11 Commission, did Ms. Rice ever consult with you, your predecessor or anyone else in your office?

Admiral MCMAHON. Certainly not with me, sir, and to my knowledge, no one at the Department of Transportation.

Mr. WAXMAN. Let me ask it more broadly, then. Did anyone at the National Security Council consult with anyone in your office before Ms. Rice made either of her public statements?

Admiral MCMAHON. To my knowledge, no.

Mr. WAXMAN. OK. Thank you very much. Thank you, Mr. Chairman.

Mr. SHAYS. Admiral, we learned in the last hearing we had, and I'll be happy to engage your other two colleagues in this question as well, that we, the estimate of overclassification was between 50 and 90 percent. I want each of you to tell me as succinctly as you can what is the negative of overclassification? I'll start with you, Mr. Leonard.

Mr. LEONARD. To me it's very clear, Mr. Chairman. The negative goes to the very integrity of the process itself. The thing that protects information is not the markings, it's not the safes, it's not the alarms on elaborate skiffs, it's people. We're dependent on people to exercise proper judgment and to be familiar with the rules and to understand them and to adhere to them.

Once individuals start losing faith in the integrity of the process, we have an uphill road in terms of having people comply.

Mr. SHAYS. Thank you. Admiral.

Admiral MCMAHON. Sir, I think this goes back to what the third parameter that Secretary Mineta gave us in determining security sensitive information, which was finding the right balance between protecting what we need to protect and enabling the public to know how its government functions. So the statement overclassifying, I think the Secretary is addressing just that concern, let's not overclassify, let's be secure but balanced.

Mr. SHAYS. Mr. Relyea, you've been doing this kind of work for how long?

Mr. RELYEA. Thirty-three years.

Mr. SHAYS. You're a real expert on this issue, and it's wonderful to have you here. We will look forward to your testimony when we get back from voting.

Can you just share with me the negative, the primary negative of overclassification?

Mr. RELYEA. Probably there's three things. I think Mr. Leonard struck on the first point, that's the integrity. Integrity, that's the first factor. If everything was classified, I think it was Potter Stewart who said it, then nothing is classified, so the system goes to smash.

There is the factor here of today, where the system is so embedded in cold war thinking that we never envisioned what the 9/11 Commission called for, not stepping over the need to know to a need to share. So we——

Mr. SHAYS. Can you define that difference?

Mr. RELYEA. Yes. I think it's a big change in culture. Those who are in the classification business, who use that as a tool, who manage it, who monitor it, this is a big change of thinking, I think, for

them. Because in the past it was to keep things compartmentalized, not necessarily let the information flow too widely.

The third factor is a very simple one which probably many of you on the subcommittee would be aware of in terms of your jurisdiction at full committee, and that's cost, efficiency and economy. This is costing a lot of money. You have to have the safes, you have to have the clearances, top secret secret clearance today is what, $2,500 I think, per person. It's very expensive. So you have costs of dollars, you have costs of integrity and you have ultimately cost of share.

Mr. SHAYS. Thank you. In the short time I have left, I want to know, what is, I know all the powers that want us to classify, in other words, all the pressures to classify from bad language, to not being embarrassed to real needs and so on. But what I want to know is, what is the pressure to not overclassify? I mean, it just seems to me we don't have a proper balance. There is everything stacked against just having a balance. I'd like, maybe I'll have you start, Mr. Relyea.

Mr. RELYEA. I think you're right, if you ingrain in a person that their whole job is to manage something that's classified, it's an available tool that you don't think too much about, because you lean on the side of protection, which was certainly there in the Reagan Executive order. There's not much of a break. You can talk about people challenging it, I don't think that happens very often in the system. You can have an oversight body, such as Mr. Leonard has, but it's limited in terms of its resources, I think, and how far it can get in terms of stopping this type of phenomenon and how you stop it.

Mr. SHAYS. Admiral.

Admiral MCMAHON. Sir, I think that we at the Department of Transportation are certainly cognizant of the fact that DHS is responsible for transportation security. But that said, transportation security is on our mind, too. So again, I think we need to strike a balance between trying to do what we can do to protect the security of the transportation system and enable the public to have the right to know how its Government is working. Again, I think Secretary Mineta has given us extremely strict parameters on doing just that. The fact that we don't classify a lot of documents, that we have none on the secret level in 2004–2005 and only two security sensitive documents in the last several months since we've had the authority I think speaks to that.

Mr. SHAYS. And the value of that is you certainly know how to protect the few that you do have.

Admiral MCMAHON. Yes, sir.

Mr. SHAYS. Mr. Leonard.

Mr. LEONARD. Part of the challenge is that I think the whole premise is set up on the basis of a false dichotomy, and that is, I need to protect this information, because its disclosure would damage national security. But there is the problem that often times, the withholding or the hoarding of the information can similarly damage the national interest. I don't like the word, but I'll use it anyhow, it's literally a cultural shift, a frame of mind that needs to occur in order to get that recognition that the act of withholding

can be just as damaging if not even sometimes more damaging than the disclosure of information.

Mr. SHAYS. Thank you. We have about 5 more minutes, Mr. Van Hollen, would someone check the TV? We're going to adjourn, Admiral, you're going to have a meeting at the White House, so you're not coming back. We'll start with Mr. Relyea, your statement, and we have some more questions.

Thank you very much. We stand adjourned.

[Recess.]

Mr. SHAYS. Mr. Relyea, we are now back in session and we would love to hear your statement. Thank you very much. Mr. Relyea, you have the floor for your statement and thank you for your patience.

STATEMENT OF HAROLD C. RELYEA

Mr. RELYEA. Mr. Chairman, members of the subcommittee, there can be little doubt at this late date that the terrorist attacks of September 11, 2001 have prompted rethinking and continuing concern about various aspects of the internal security, that is the homeland security, of the United States, not the least of which includes the public availability of information of potential value to terrorists for either the commission of their acts or for warning them of ways of their being detected.

Often times it has not been clear to what extent if any an attempt was made to weigh citizen needs for information vis-a-vis denying its availability to terrorists, or if thoughtful consideration was given to alternative limits short of total restriction. Recently, a December 2004 report from the Heritage Foundation observed, "at the very least, such wholesale withdrawal of information seems arbitrary and undermines important values of Government openness, the development of electronic Government to speed the delivery and lower the costs of Government services and public trust."

A primary tool for protecting information in the post-September 11 environment is security classification. One may not agree with all of its rules and requirements, but that is an expression of policy and procedure. Its attention to detail is commendable. The operative Presidential Directive, Executive Order 12958, as amended, for instance, defines its principal terms, exclusive categories of classifiable information are specified, as are the terms of the duration of classification as well as classification prohibitions and limitations. Classified information is required to be marked appropriately, along with the identity of the original classifier, the agency or office of origin, and a date or event for declassification.

Authorized holders of classified information who believe that its protected status is improper are encouraged and expected to challenge that status through prescribed arrangements. Mandatory declassification reviews are also authorized to determine if protected records merit continued classification at their present level, a lower level or at all. An information security oversight office provides central management and oversight of the security classification program.

Not long ago, in the closing days of January, GCN Update, the online electronic news service of Government Computer News, reported that dozens of classified Homeland Security Department documents had been accidentally made available on a public Inter-

net site for several days due to an apparent security glitch at the Department of Energy. Describing the contents to the compromised materials and the reactions to the breach, the account stated, "The documents were marked for official use only, the lowest secret level classification." The documents, of course, were not security classified, because the marking cited is not authorized by Executive Order 12958.

Interestingly, however, in view of the fact that this mis-interpretation appeared in a story to which three reporters contributed, perhaps it reflects to some extent the current state of confusion about the origin and status of various information control markings which have appeared of late. However, as my prepared remarks indicate, such markings are not new. Over three decades ago, another subcommittee of the Committee on Government Reform, known then as the Committee on Government Operations, explored these markings and the difficulties they created. Those difficulties are again with us today.

Analyses by the Jason Program office of the Mitre Corp., the Heritage Foundation and the Federal Research Division of the Library of Congress have decried the introduction of the undefined sensitive but unclassified marking and other such labels. Assessments of the variety and management of current information control markings, other than those prescribed for security classifications, are underway at CRS and the Government Accountability Office. Early indications are that very little of the attention to detail that attends the security classification program is to be found in other information control marking activities. Key terms often lack definition. Vagueness exists regarding who is authorized to apply markings, for what reasons and for how long. Uncertainty prevails concerning who is authorized to remove the markings and for what reasons.

Options to remedy the situation might include a circumscribed and particularized legislative authorization for some such marking or markings, or a legislative limitation or restriction of the use of such markings. These choices of course are open to discussion.

Thank you for your attention, and I welcome your questions.

[The prepared statement of Mr. Relyea follows:]

STATEMENT BY HAROLD C. RELYEA
CONGRESSIONAL RESEARCH SERVICE
BEFORE
HOUSE GOVERNMENT REFORM
SUBCOMMITTEE ON NATIONAL SECURITY,
EMERGING THREATS, AND INTERNATIONAL RELATIONS
MARCH 2, 2005
EMERGING THREATS: OVERCLASSIFICATION AND PSEUDO-CLASSIFICATION

Mr. Chairman and members of the Subcommittee, thank you for your invitation to appear here today to offer testimony regarding the subject matter of this hearing, the emerging threats posed by overclassification and pseudo-classification of information within the federal departments and agencies. I am Harold C. Relyea, a Specialist in American National Government with the Congressional Research Service of the Library of Congress.

There can be little doubt at this late date that the terrorist attacks of September 11, 2001, have prompted rethinking and continuing concern about various aspects of the internal security — or homeland security — of the United States, not the least of which includes the public availability of information of potential value to terrorists for either the commission of their acts or forewarning them of ways of their being detected. Oftentimes, it has not been clear to what extent, if any, an attempt was made to weigh citizen needs for information vis-a-vis denying its availability to terrorists, or if thoughtful consideration was given to alternative limits short of total restriction. "At the very least," a Heritage Foundation report observed not long ago, "such wholesale withdrawal of information seems arbitrary and undermines important values of government openness, the development of electronic government (e-gov) to speed the delivery and lower the costs of government services, and public trust."[1] The recent creation of privacy and civil liberties officers and institutions may ameliorate this and other information management concerns, including the collection, security, and scrutiny of vast amounts of personally identifiable information.

---

[1] James Jay Carafano and David Heyman, "DHS 2.0: Rethinking the Department of Homeland Security," *Heritage Special Report* (Washington: Dec. 13, 2004), p. 20.

Security Classification

A primary tool for protecting information in the post-9/11 environment is the classification of national security information.[2] Current security classification arrangements, prescribed by an executive order of the President, trace their origins to a March 1940 directive issued by President Franklin D. Roosevelt as E.O. 8381. This development was probably prompted somewhat by desires to clarify the authority of civilian personnel in the national defense community to classify information, to establish a broader basis for protecting military information in view of growing global hostilities, and to better manage a discretionary power seemingly of increasing importance to the entire executive branch. Prior to this 1940 order, information had been designated officially secret by armed forces personnel pursuant to Army and Navy general orders and regulations. The first systematic procedures for the protection of national defense information, devoid of special markings, were established by War Department General Orders No. 3 of February 1912. Records determined to be "confidential" were to be kept under lock, "accessible only to the officer to whom intrusted." Serial numbers were issued for all such "confidential" materials, with the numbers marked on the documents, and lists of same kept at the offices from which they emanated. With the enlargement of the armed forces after the entry of the United States into World War I, the registry system was abandoned and a tripartite system of classification markings was inaugurated in November 1917 with General Orders No. 64 of the General Headquarters of the American Expeditionary Force.

During World War II, in addition to the President's order and prevailing armed forces directives on marking and handling classified information, the Office of War Information, in September 1942,

---

[2] This historical overview derives from Harold C. Relyea, "The Evolution of Government Information Security Classification Policy: A Brief Overview (1775-1973)," in U.S. Congress, House Committee on Government Operations, *Security Classification Reform*, hearings, 93rd Cong., 2nd sess. (Washington: GPO, 1974), pp. 505-597; Harold C. Relyea, "Appendix II: Government Information Security Classification Policy," in U.S. Congress, Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, *Supplemental Reports on Intelligence Activities*, Book VI, S. Rept. 94-755, 94th Cong., 2nd sess. (Washington: GPO, 1976), pp. 313-352.

issued a government-wide regulation on creating and managing classified materials. Among other ad hoc arrangements of the era, personnel cleared to work on the Manhattan Project for the production of the atomic bomb, in committing themselves not to disclose protected information improperly, were "required to read and sign either the Espionage Act or a special secrecy agreement," establishing their awareness of their secrecy obligations and a fiduciary trust which, if breached, constituted a basis for their dismissal.[3]

A few years after the conclusion of World War II, President Harry S. Truman, in February 1950, issued E.O. 10104, which, while superseding E.O. 8381, basically reiterated its text, but added a fourth "Top Secret" classification designation, making American information security categories consistent with those of our allies. At the time of the promulgation of this order, however, plans were underway for a complete overhaul of the classification program, which would result in a dramatic change in policy.

E.O. 10290, issued in September 1951, introduced three sweeping innovations in security classification policy. First, the order indicated the Chief Executive was relying upon "the authority vested in me by the Constitution and statutes, and as President of the United States" in issuing the directive. This formula appeared to strengthen the President's discretion to make official secrecy policy: it intertwined his responsibility as Commander in Chief with the constitutional obligation to "take care that the laws be faithfully executed."[4] Second, information was now classified in the interest of "national security," a somewhat new, but nebulous, concept, which, in the view of some, conveyed more latitude for the creation of official secrets. It replaced the heretofore relied upon "national defense" standard for classification. Third, the order extended classification authority to

---

[3] Anthony Cave Brown and Charles B. MacDonald, eds., *The Secret History of the Atomic Bomb* (New York: Dial Press/James Wade, 1977), p. 201.

[4] In *Environmental Protection Agency* v. *Mink*, Supreme Court Associate Justice Byron White, delivering the majority opinion, proffered that "Congress could certainly have provided that the Executive Branch adopt new procedures" for the security classification of information, "or it could have established its own procedures — subject only to whatever limitations the Executive [or constitutional separation of powers] privilege may be held to impose upon such congressional ordering." 410 U.S. 73, 83 (1973).

nonmilitary entities, to be exercised by, presumably, but not explicitly limited to, those having some role in "national security" policy.

The broad discretion to create official secrets granted by E.O. 10290 engendered widespread criticism from the public and the press. In response, President Dwight D. Eisenhower, shortly after his election to office, instructed Attorney General Herbert Brownell to review the order with a view to revising or rescinding it. The subsequent recommendation was for a new directive, which was issued in November 1953 as E.O. 10501. It withdrew classification authority from 28 entities, limited this discretion in 17 other units to the agency head, returned to the "national defense" standard for applying secrecy, eliminated the "Restricted" category, which was the lowest level of protection, and explicitly defined the remaining three classification areas to prevent their indiscriminate use.

Thereafter, E.O. 10501, with slight amendment, prescribed operative security classification policy and procedure for the next two decades. Successor orders built on this reform. These included E.O. 11652, issued by President Richard M. Nixon in March 1972, followed by E.O. 12065, promulgated by President Jimmy Carter in June 1978. For 30 years, these classification directives narrowed the bases and discretion for assigning official secrecy to executive branch documents and materials. Then, in April 1982, this trend was reversed with E.O. 12356, issued by President Ronald Reagan. This order expanded the categories of classifiable information, mandated that information falling within these categories be classified, authorized the reclassification of previously declassified documents, admonished classifiers to err on the side of classification, and eliminated automatic declassification arrangements.[5]

President William Clinton returned security classification policy and procedure to the reform trend of the Eisenhower, Nixon, and Carter Administrations with E.O. 12958 in April 1995. Adding

---

[5] See Richard C. Ehlke and Harold C. Relyea, "The Reagan Administration Order on Security Classification: A Critical Assessment," *Federal Bar News & Journal*, vol. 30, Feb. 1983, pp. 91-97.

impetus to the development and issuance of the new order were changing world conditions: the democratization of many eastern European countries, the demise of the Soviet Union, and the end of the Cold War. Accountability and cost considerations were also significant influences. In 1985, the temporary Department of Defense (DOD) Security Review Commission, chaired by retired General Richard G. Stilwell, declared that there were "no verifiable figures as to the amount of classified material produced in DOD and in defense industry each year." Nonetheless, it concluded that "too much information appears to be classified and much at higher levels than is warranted."[6] In October 1993, the cost of the security classification program became clearer when the General Accounting Office (GAO) reported that it was "able to identify government-wide costs directly applicable to national security information totaling over $350 million for 1992." After breaking this figure down — it included only $6 million for declassification work — the report added that "the U.S. government also spends additional billions of dollars annually to safeguard information, personnel, and property."[7] E.O. 12958 set limits for the duration of classification, prohibited the reclassification of properly declassified records, authorized government employees to challenge the classification status of records, reestablished the balancing test of E.O. 12065 weighing the need to protect information vis-a-vis the public interest in its disclosure, and created two review panels — one on classification and declassification actions and one to advise on policy and procedure.

Recently, in March 2003, President George W. Bush issued E.O. 13292 amending E.O. 12958. Among the changes made by this directive were adding infrastructure vulnerabilities or capabilities, protection services relating to national security, and weapons of mass destruction to the categories of classifiable information; easing the reclassification of declassified records; postponing the automatic declassification of protected records 25 or more years old, beginning in mid-April 2003

---

[6] U.S. Department of Defense, Department of Defense Security Review Commission, *Keeping the Nation's Secrets* (Washington: GPO, 1985), pp. 48-49.

[7] U.S. General Accounting Office, *Classified Information: Costs of Protection Are Integrated with Other Security Costs*, GAO Report GAO/NSIAD-94-55 (Washington: Oct. 1993), p. 1.

to the end of December 2006; eliminating the requirement that agencies prepare plans for declassifying records; and permitting the Director of Central Intelligence to block declassification actions of the Interagency Security Classification Appeals Panel, unless overruled by the President.

The security classification program has evolved over 65 years. One may not agree with all of its rules and requirements, but, as an expression of policy and procedure, its attention to detail is commendable. The operative presidential directive, as amended, defines its principal terms. Those who are authorized to exercise original classification authority are identified. Exclusive categories of classifiable information are specified, as are the terms of the duration of classification, as well as classification prohibitions and limitations. Classified information is required to be marked appropriately along with the identity of the original classifier, the agency or office of origin, and a date or event for declassification. Authorized holders of classified information who believe that its protected status is improper are "encouraged and expected" to challenge that status through prescribed arrangements. Mandatory declassification reviews are also authorized to determine if protected records merit continued classification at their present level, a lower level, or at all. Unsuccessful classification challenges and mandatory declassification reviews are subject to review by the Interagency Security Classification Appeals Panel. General restrictions on access to classified information are prescribed, as are distribution controls for classified information. An entity — the Information Security Oversight Office within the National Archives and Records Administration — is mandated to provide central management and oversight of the security classification program. If the director of this entity finds that a violation of the order or its implementing directives has occurred, it must be reported to the head of the agency or to the appropriate senior agency official so that corrective steps, if appropriate, may be taken.

Pseudo-Classification

Not long ago, in the closing days of January, *GCN Update*, the online, electronic news service of *Government Computer News*, reported that "dozens of classified Homeland Security Department

documents" had been accidently made available on a public Internet site for several days due to an apparent security glitch at the Department of Energy. Describing the contents of the compromised materials and reactions to the breach, the account stated the "documents were marked 'for official use only,' the lowest secret-level classification." The documents, of course, were not security classified, because the marking cited is not authorized by E.O. 12958. Interestingly, however, in view of the fact that this misinterpretation appeared in a story to which three reporters contributed, perhaps it reflects, to some extent, the current state of confusion about the origin and status of various new information control markings which have appeared of late.[8]

Moreover, the situation is not unprecedented. In March 1972, a subcommittee of the House Committee on Government Operations, now the House Committee on Government Reform, launched the first oversight hearings on the administration and operation of the Freedom of Information (FOI) Act. Enacted in 1966, the FOI Act had become operative in July 1967. In the early months of 1972, the Nixon Administration was developing new security classification policy and procedure, which would be prescribed in E.O. 11652, issued in early March. The subcommittee's strong interest in this directive is reflected in its unsuccessful attempt to receive testimony from one of the directive's principal architects, David Young, Special Assistant to the National Security Council. The subcommittee sought his testimony as it examined the way in which the new order "will affect the economic and efficient operation of our security classification system, the rationale behind its various provisions, and alternatives to the present approach."[9] Although Young, through White House Counsel John Dean III, declined the invitation to testify, the subcommittee was more successful in obtaining department and agency responses to its August 1971

---

[8] Patience Wait, "DHS Classified Briefings Leaked Through Energy System," *GCN Update*, Jan. 27, 2005, available at [http://www.gcn.com/vol1_no1/daily-updates/34907-1.html]; credited as contributing to this story were GCN staff writers Susan M. Menke and Mary Mosquera.

[9] Letter to David Young, Apr. 24, 1972, appearing in U.S. Congress, House Committee on Government Operations, *U.S. Government Information Policies and Practices — Security Classification Problems Involving Subsection (b)(1) of the Freedom of Information Act (Part 7)*, hearings, 92nd Cong., 2nd sess. (Washington: GPO, 1972), pp. 2452-2453.

questionnaire, which, among other questions, asked: "What legend is used by your agency to identify records which are *not* classifiable under Executive Order 10501 [the operative order at the time] but which are not to be made available outside the government?"[10] Of 58 information control markings identified in response to this question, the most common were "For Official Use Only" (11 agencies); "Limited Official Use" (nine agencies); "Official Use Only" (eight agencies); "Restricted Data" (five agencies); "Administratively Restricted" (four agencies); "Formerly Restricted Data" (four agencies); and "Nodis," or no dissemination (four agencies). Seven other markings were used by two agencies in each case.[11] A CRS review of the agency responses to the control markings question prompted the following observation.

> Often no authority is cited for the establishment or origin of these labels; even when some reference is provided it is a handbook, manual, administrative order, or a circular but not statutory authority. Exceptions to this are the Atomic Energy Commission, the Defense Department and the Arms Control and Disarmament Agency. These agencies cite the Atomic Energy Act, N.A.T.O. related laws, and international agreements as a basis for certain additional labels. The Arms Control and Disarmament Agency acknowledged it honored and adopted State and Defense Department labels.[12]

At a May 1, 1972, hearing on the relationship of the FOI Act to the security classification system, Chairman William S. Moorhead of the Foreign Operations and Government Information Subcommittee wondered aloud how the act's nine exemptions to the rule of disclosure could be expanded to the multiple information control markings which the departments and agencies had indicated they were using.[13] The following day, when the hearing continued, William D. Blair, Jr., Deputy Assistant Secretary for Public Affairs at the Department of State, explained that some

---

[10] Ibid., p. 2930 (emphasis in original).

[11] See Ibid., pp. 2933-2934.

[12] Ibid., p. 2932.

[13] Ibid., p. 2284.

information control markings were used to route otherwise classified information to a limited group of recipients, "those people who have responsibility for the subject matter concerned." He then addressed the relationship question raised by Chairman Moorhead, saying:

> But if a question came in under the Freedom of Information Act or from the Congress or other representative of the public for that given document, the fact that it is marked, let's say, NODIS, is not relevant. What is relevant to the making available of that document to the public is whether or not it was properly classified under the Executive order and whether or not the Freedom of Information Act, for example, once we have reviewed the document, still pertains, whether we feel that the need for the classification still pertains and whether, in fact, we are authorized under the act to withhold it.[14]

A moment thereafter, he explained another marking, which was not applied to route classified information, but apparently had the same effect as a security classification protective marking.

> "Limited official use" is not a fixed distribution channel, such as some of these other terms you have mentioned. It simply is an administrative red flag put on that document which means that the document should be given the same degree of protection, physical protection as a classified document even though it is not, under the Executive order, classifiable.[15]

However, when asked if, in applying this particular marking, "you mean to exclude all individuals outside the Department, subject to the Freedom of Information Act, where they can go to court to obtain it," Blair's response indicated that the use of the marking was somewhat more complicated than functioning as a parallel security label, when he said:

> Not necessarily sir. That may be the case. For instance, one set of files on which we use "Limited official use" quite commonly is personnel files. Well, we would be very likely to deny those personnel files if they were requested by a member of the public, on quite different grounds from classification — on grounds of invasion of privacy. But on the other hand we may use a

---

[14] Ibid., pp. 2477-2478.

[15] Ibid., p. 2478.

term like "Limited official use" on an internal advisory document which we may be authorized under the Freedom of Information Act to withhold if it were requested; but we might decide not to claim that authority.[16]

Although an attempt was made to obtain further explanation of how information control markings were used, the questioner, a subcommittee staff member, concluded "that all you have convinced me of is to reinforce my belief that a distribution marking is merely a more restrictive or stricter type of classification marking."[17]

Later in the hearing, in an exchange with the subcommittee's staff director, DOD General Counsel J. Fred Buzhardt made another attempt to clarify the use of control markings.

In the first place, you have a determination as to whether the material is to be classified. Once the decision is made that the information should be classified, then the limitation of access has to do with the protection of that which is classified. We also have the responsibility to control the dissemination. That is what these access limitations are for, to control dissemination, to confine access to the people who have a need to know to work with the information. It is a protection device. We must use protective devices of some sort.[18]

Asked if the control markings, such as "eyes only," were applied to material that was not classified, Buzhardt said:

I presume you wouldn't find "eyes only" in an authorized way upon any document that was not classified by one of the classifiers. Once it is classified you can use limitations on distribution to protect it. That is a protective device.[19]

To this response, Blair added:

The purpose of classification is to determine what information is or is not available to the public outside of the government. These labels that you are referring to have nothing to do with that.

---

[16] Ibid.

[17] Ibid., p. 2479.

[18] Ibid., p. 2497.

[19] Ibid.

> They have absolutely no value for determining what information or what document may be given to a member of the public. They are simply a mailing device, if you like, a means by which a superior determines which of his subordinates he wishes to deal with this particular matter and be aware of this particular information.[20]

These explanations of information control markings being used as devices to limit the distribution of classified information within DOD and the State Department, however, did not appear to extend to all such markings. Blair, for instance, had testified that the "Limited official use" marking was applied, in his words, "quite commonly" to personnel files, which, for the most part, were not security classifiable materials at that time. Several entities indicating they used information control markings had no original classification authority. These included, among others, the American Revolution Bicentennial Commission (ARBC), the Department of Housing and Urban Development, and the Federal Trade Commission (FTC).[21] Does this situation mean that the control markings of these entities were applied only to limit the distribution of classified information received from other agencies? That is possible, but seems unlikely. The ARBC control marking, "Administratively confidential," appears to have been designed for information of a different character from national security classified materials, while the FTC label, "For staff use only," does not appear to have provided much limitation on the distribution of classified information.

Before this phase of the oversight hearings on the FOI Act concluded, the subcommittee received testimony from Assistant Attorney General Ralph E. Erickson of the Office of Legal Counsel, Department of Justice, on May 11, 1972. During the course of his appearance before the subcommittee to discuss E.O. 11652, the use of control markings to limit the distribution of classified information was raised with the following question from the subcommittee's staff director.

> Can you assure us today that these kinds of distribution access stamps will not be used on unclassified material in any Executive agency or department? If you can guarantee that, then I

---

[20] Ibid., pp. 2497-2498.

[21] See Ibid., p. 2935.

will go along and say [Section] 4(a) is a big improvement. But I do not think that is going to be the case from other testimony we have had. I think people are going to substitute LIMDIS, NODIS, and all these other stamps for the stamps authorized under the Executive order and we are going to proliferate more and more and more.[22]

Erickson offered a two part response.

First, it is our hope within the Department of Justice and I think in other agencies, too, that the use of this sort of a restricted distribution will be severely limited or removed. But, more importantly, it [Section 4(a)] specifically limits the use of such designations to the point where they must conform with the provision of this order and would have no effect in terms of classification. It will not prevent the information from otherwise being made available. It may in part restrict the distribution within the department but certainly if a request were made under the Freedom of Information Act it has no applicability.[23]

He assured his questioner that control markings used to limit the distribution of classified information "will not have any effect on disclosure" under the FOI Act, and would not, in themselves, be a bar to disclosure.

Later, in May 1973, when reviewing this phase of the subcommittee's oversight hearings, a report by the parent Committee on Government Operations commented:

One of the difficult problems related to the effective operation of the security classification system has been the widespread use of dozens of special access, distribution, or control labels, stamps, or markings on both classified and unclassified documents. Such control markings were not specifically authorized in Executive Order 10501, but have been utilized for many years by many executive agencies having classification authority and dozens of other agencies who do not

---

[22] Ibid., pp. 2705-2706.

[23] Ibid., p. 2706.

possess such authority. The use of such stamps has, in effect, been legitimized in section 9 of the new Executive Order 11652.[24]

On this matter, the report concluded that, "while there is a clear rationale for the use of such access or control markings, the basic problem is the effect of the proliferation of their use on the effective operation of the classification system. This problem," it continued, "fully explored with executive branch witnesses during the hearings, is one that this committee believes should be carefully monitored by the [newly created] Interagency Classification Review Committee and by department heads to assure that it does not interfere with the overall effectiveness and integrity of the classification system."[25]

That such interference with the security classification program by these types of information control markings — in terms of both their confusion and presumed coequal authority with classification markings — has occurred in the post-9/11 environment may be discerned in the recent *GCN Update* story cited earlier. In some instances, the phraseology of the markings is new, and, in at least one case, the asserted authority for the label is, unlike most of those of the past, statutory. Among the problems they generate, however, the one identified over three decades ago by the House Committee on Government Operations endures.

Broadly considering the contemporary situation regarding information control markings, a recent information security report by the JASON Program Office of the MITRE Corporation proffered the following assessment.

> The status of sensitive information outside of the present classification system is murkier than ever. ... "Sensitive but unclassified" data is increasingly defined by the eye of the beholder.

---

[24] U.S. Congress, House Committee on Government Operations, *Executive Classification of Information — Security Classification Problems Involving Exemption (b)(1) of the Freedom of Information Act (5 U.S.C. 552)*, H. Rept. 93-221, 93rd Cong., 2nd sess. (Washington: GPO, 1973), p. 75.

[25] Ibid., p. 78.

Lacking in definition, it is correspondingly lacking in policies and procedures for protecting (or not protecting) it, and regarding how and by whom it is generated and used.[26]

A contemporaneous Heritage Foundation report appeared to agree with this appraisal, saying:

> The process for classifying secret information in the federal government is disciplined and explicit. The same cannot be said for unclassified but security-related information for which there is no usable definition, no common understanding about how to control it, no agreement on what significance it has for U.S. national security, and no means for adjudicating concerns regarding appropriate levels of protection.[27]

Concerning the current "Sensitive But Unclassified" (SBU) marking, a recent report by the Federal Research Division of the Library of Congress commented that guidelines for its use are needed, and noted that "a uniform legal definition or set of procedures applicable to all Federal government agencies does not now exist." Indeed, the report indicates that SBU has been utilized in different contexts with little precision as to its scope or meaning, and, to add a bit of chaos to an already confusing situation, is "often referred to as Sensitive Homeland Security Information."[28]

Assessments of the variety and management of information control markings, other than those prescribed for the classification of national security information, are underway at CRS and GAO. Early indications are that very little of the attention to detail that attends the security classification program is to be found in other information control marking activities. Key terms often lack definition. Vagueness exists regarding who is authorized to applying markings, for what reasons, and for how long. Uncertainty prevails concerning who is authorized to remove markings and for what reasons.

---

[26] MITRE Corporation, JASON Program Office, *Horizontal Integration: Broader Access Models for Realizing Information Dominance* (McLean, VA: Dec. 2004), p. 5.

[27] Carafano and Heyman, "DHS 2.0: Rethinking the Department of Homeland Security," p. 20.

[28] U.S. Library of Congress, Federal Research Division, *Laws and Regulations Governing the Protection of Sensitive But Unclassified Information*, by Alice R. Buchalter, John Gibbs, and Marieke Lewis (Washington: Sept. 2004), p. i.

One Congressional Response

Half a century ago, in November 1954, Secretary of Commerce Sinclair Weeks announced that, at the direction of the President and on the recommendation of the National Security Council, he was creating an Office of Strategic Information (OSI) within his department. The mission of this new entity, according to the Secretary, was to work with various private sector organizations "in voluntary efforts to prevent unclassified strategic data from being made available to those foreign nations which might use such data in a manner harmful to the defense interests of the United States."[29] The new office, however, was something of an anomaly. It had no legislative charter, and its activities, in many regards, appeared to overlap with, and duplicate, certain more clearly stated functions of other agencies. Because the concept of "strategic information" was not precisely defined, its regulatory application was seen as potentially sweeping more broadly than the protections established for the classification of national security information. Nonetheless, the OSI was created to detect any imbalance favoring the Communist bloc in exchanges of scientific, technical, and economic information, and to alert federal agencies, as well as scientists, businesses, and the press to the indiscriminate publication of unclassified information of possible benefit to an enemy nation.

Journalists and scientists took their objections to the OSI to a House subcommittee studying government information policy and practice.[30] Having serious reservations about the OSI, the subcommittee urged its abolition, a recommendation endorsed by the parent Committee on Government Operations (now known as the Committee on Government Reform).[31] In April 1957,

---

[29] U.S. Department of Commerce, Office of the Secretary, *Press release (G-520)* (Washington: Nov. 5, 1954); James Russell Wiggins, *Freedom or Secrecy*, Revised edition (New York: Oxford University Press, 1964), pp. 102-103.

[30] U.S. Congress, House Committee on Government Operations, *Availability of Information from Federal Departments and Agencies*, hearings, 84th Cong., 2nd sess. (Washington: GPO, 1956), pp. 1123-1187, 1233-1286, 1447-1521, 1639-1711.

[31] U.S. Congress, House Committee on Government Operations, *Availability of Information from Federal*

(continued...)

the House eliminated all funds for the OSI and prohibited the transfer of any money from other sources for its continuation.[32] When the Senate agreed to this action, Secretary Weeks was forced to abolish the OSI.[33] With the demise of the office went a vague concept of information control which had strong potential, in its application, for sweeping beyond carefully crafted security classification protections and otherwise complicating their comprehension and legitimacy.

While current department and agency use of vaguely defined information control marking with weak and, in some regards, nebulous management regimes, would seemingly not warrant the drastic action taken in the case of OSI, other options are available. These might include a circumscribed and particularized legislative authorization for some such marking(s), or a legislative limitation or restriction of the use of such markings.

Thank you for your attention. I welcome your questions.

---

[31] (...continued)
Departments and Agencies, H. Rept. 2947, 84th Cong., 2nd sess. (Washington: GPO, 1956), p. 91.

[32] *Congressional Record*, vol. 103, Apr. 9, 1957, p. 5376; also see U.S. Congress, House Committee on Government Operations, *Availability of Information from Federal Departments and Agencies*, H. Rept. 2578, 85th Cong., 2nd sess. (Washington: GPO, 1958), pp. 13-14.

[33] *Federal Register*, vol. 22, July 24, 1957, p. 5876.

Mr. SHAYS. Thank you very much.

We're just going to start over again, if any of the Members have questions for Mr. Leonard or Mr. Relyea. I would just ask, I am unclear, and I want a little bit more explanation, I have heard your testimony which says we have a process in place to know when to classify and know when not to, we have rules and we have a process. But what I'm not hearing is, if it's balanced, and if it really can work well. Because I don't think it's working well now. So I guess my first question is, I made an assumption from your testimony that it is not working well. Is that a correct assumption, Mr. Leonard?

Mr. LEONARD. Yes, sir.

Mr. SHAYS. Mr. Relyea.

Mr. RELYEA. I think so, too.

Mr. SHAYS. So the issue, I want to know, one of the challenges, and I say this with no reluctance, I don't think the House of Representatives has done the proper job of oversight of the administration. I actually think it hurts the administration. I think had we been to Iraq more often, had someone been in Abu Ghraib, a Member, someone would have come to them and said, you know, bad things are happening here, you need to check it out, questions would have been asked, there would have been a lot more focus and we could have nipped it in the bud. That's what I think.

So I think that information that is needed by someone is never going to be seen by them. I also think that when you have so much information, besides the cost that you point out, Mr. Relyea, you end up with just so much to keep track of that it's just a waste of time as well as money. So I want to know what you think could bring balance to the system.

Mr. RELYEA. One consideration that I would offer, and Mr. Leonard may not appreciate my offering this, I think his office, his oversight unit is understaffed. I think a model that might be looked at, or an arrangement that might be looked at is not unlike the budget officers that OMB has. Perhaps ISOO, his unit, would benefit from having in their employ as their arm into the agencies some type of classification officer who would be more the arm of ISOO than it would be an employee of the agency.

Mr. SHAYS. Mr. Leonard.

Mr. LEONARD. As I mentioned in my testimony, Mr. Chairman, fundamentally, as the current framework is set up, the decision to classify is an act of judgment. Like so many other things in life, when it comes to judgment, people sometimes do not exercise good judgment or don't take the time to be discerning.

Mr. SHAYS. I think it goes more than that, from your testimony, that there's actually incentives to classify that may be logical based on those incentives.

Mr. LEONARD. Quite frankly, very few incentives not to classify. Two comments that I continually get in this area is, Leonard, don't you know we're at war, and we don't have time for your administrative niceties. The other statement that always drives me up a wall is, well, you know, we always want to error on the side of caution. I'm always dumbfounded by the very notion of somehow, somebody having error as part of an implementation strategy. It just strikes me as bizarre.

But yet, and I understand where people are coming from. In Homeland Security, folks are working at absolutely, unbelievable ops tempos. It's been for years. I can really sympathize with the pressures that they're under and that sometimes, you know, maybe I don't have the time or the inclination to step back and do it right. But on the other hand, my reply always is, if we're ever going to get it right, I would like to think when we're at war is when we're going to get it right.

Mr. SHAYS. That's a good point, but I would love to know what the incentives are to have it be more balanced. So just think about it a little longer and just let me finish by asking, what is the status of the Public Interest Declassification Board, Mr. Relyea?

Mr. RELYEA. If memory serves me correctly——

Mr. SHAYS. Excuse me. It should be Mr. Leonard I should start with. I apologize.

Mr. LEONARD. Yes, sir. We have the Public Interest Declassification Board, and as you are aware, iy was extended by the Intel Reform Act last December. It provides for nine members, five appointed by the President, four by the congressional leadership. The President appointed his five members last August-September. There is one congressional representative appointed, the House Minority Leader appointed her a member. My understanding is other appointments are under consideration.

The board has yet to meet. The biggest obstacle we are encountering right now is the board was a victim of I guess unfortunate timing, in that it was scheduled to sunset in December of last year, and therefore, there were no provisions for it in either the 2005 or the 2006 budget. It was literally extended at the last minute, December of last year.

Mr. SHAYS. So there's no money for them?

Mr. LEONARD. There's no money for it, but I am confident there are ongoing efforts right now to identify money in both 2005 and 2006 to fund this.

Mr. SHAYS. What impact can the Public Interest Declassification Board have on classification and declassification policies and practices?

Mr. LEONARD. Profound. One of the most profound is one of the provisions that was added as a result of the Intel Reform Act, and that is that the board can now hear appeals from committees of the Congress when there are concerns or disputes about the appropriateness of classification, and they can make a recommendation to the President as to the continued appropriateness of classification. I think that's a very profound addition to the provision.

Mr. SHAYS. OK. Thank you.

Mr. Waxman.

Mr. WAXMAN. Thank you, Mr. Chairman.

Mr. Leonard, I know you specialize in classified information, but I would like to get your impressions about the withholding of unclassified, confidential business information. Let's just use a hypothetical. Suppose a Government agency conducts an audit of a Government contract and suppose those auditors issue a report concluding that the contractor has grossly overcharged the Government for goods or services. In your experience, have you ever seen a case in which the administration has withheld as proprietary

business information the actual amount a company has overcharged?

Mr. LEONARD. First of all, Mr. Waxman, you are right, this is beyond my area of expertise. But to answer your specific question, no, I have never encountered that.

Mr. WAXMAN. Would such a withholding be appropriate, in your opinion?

Mr. LEONARD. I would be hard pressed to readily come up with a rationale.

Mr. WAXMAN. Let me turn to a slightly different issue. Under Executive Order 12600, when there is a request for a document under the Freedom of Information Act, the Government must allow contractors to designate information in that document as confidential commercial information. Would you agree that regardless of what information a contractor believes should be withheld, a Government agency has an independent duty to make its own determination?

Mr. LEONARD. Again, beyond my area of expertise, but yes, my understanding would be it should be more than just an assertion.

Mr. WAXMAN. So it would be inappropriate, in your view, for an agency to simply abdicate its responsibility to make its own assessment?

Mr. LEONARD. Yes, I do.

Mr. WAXMAN. One last question, Mr. Leonard. If a contractor merely disagrees with the Government auditor's conclusion, that alone wouldn't be a valid reason to redact the auditor's findings, would it?

Mr. LEONARD. Not from my experience.

Mr. WAXMAN. Mr. Relyea, do you agree with Mr. Leonard's answers to my questions?

Mr. RELYEA. Yes, I would tend to agree, particularly where, your next to last question, it strikes me that where an agency is just accepting what a contractor is saying is proprietary, it's going to create difficulties for the ultimate defense of that type of case, if it's an FOIA case and it is going to court. What does the agency say, this guy told me this is the answer? It's a terrible abrogation of responsibility.

Mr. WAXMAN. About that first question, about not——

Mr. RELYEA. The dollar amount?

Mr. WAXMAN. Yes, not giving a dollar amount where there is a question of overcharging. Do you think that is proprietary?

Mr. RELYEA. It's hardly proprietary information. It's disclosable, it seems to me.

Mr. WAXMAN. OK. And you've had knowledge of this whole area?

Mr. RELYEA. Of the FOIA Act, yes, I've worked with it extensively over the years.

Mr. WAXMAN. Thank you, thank you both.

Mr. SHAYS. They are both qualified experts in this issue.

Mr. WAXMAN. Mr. Leonard was a little modest.

Mr. SHAYS. They are both.

Mrs. Maloney.

Mrs. MALONEY. In the interest of time, I can call them later or talk to them. Other people, Richard Ben-Veniste told me he has to leave, too.

Mr. SHAYS. Sure. Are there any closing comments either of you would like to make?

Mr. RELYEA. I have one comment I'd like to make. As I mentioned in my statement, somewhere with these pseudo-classification markings we probably are looking for some type of legislative solution. One I would ask you to think about is creating legislatively the situation where the implementation or use of these labels could not be accomplished using appropriated funds unless authorized. So you turn the situation around to the agencies and you say, if you're going to use these labels, you have to get our approval.

Mr. SHAYS. These labels being?

Mr. RELYEA. Any of these pseudo markings.

Mr. SHAYS. Sensitive but unclassified? Sensitive homeland security information, for official use only?

Mr. RELYEA. Correct. So as they come back to try to get an authorization to use appropriated funds to use these things, then you put a management platform under them. You get a common term, you get an understanding of how they will be used, who will use them, how long. It may be a way of working this problem through.

Mr. SHAYS. Thank you very much. Mr. Leonard.

Mr. LEONARD. Yes, sir. On that point, I would make two observations. No. 1, both dealing with the plethora of sensitive but unclassified regimes, I may not be the brightest person around, especially if you listen to my wife, that's an accurate description. [Laughter.]

But even I, of average intellect, have a hard time keeping track and understanding and knowing all the ins and outs of all the various regimes out there. It's just literally impossible to understand all the rules and the nuances and the difference. When I think of the operators out there who have to take all this information and compile it and assemble it and do something with it and disseminate it, my heart really goes out to them in terms of, how do they understand or how do they know what's right and what's wrong. My concern is that people always default then in uncertainty to withhold.

The second thing is the tremendous impact this has on our ability to leverage information technology. The ability to assemble and collate and analyze and data mine and disseminate information and to use technology to do that is severely restricted by these again plethora of caveats in terms of how different information is handled and identified. I think that impact is very significant in terms of our efficiency in this area.

Mr. SHAYS. Great. Thank you both very much. We appreciate your patience with the subcommittee and obviously appreciate your testimony in response to our questions. Thank you.

At this time, the Chair would welcome our second panelist, Mr. Richard Ben-Veniste, and thank him for his patience in waiting to testify. You might stay standing, because as you know, we swear in our witnesses.

Please raise your right hand.

[Witness sworn.]

Mr. SHAYS. Thank you. It's wonderful to have you once again before our subcommittee, especially since we have taken care of some of your recommendations on the 9/11 Commission. Thank you for all your good work.

Mr. WAXMAN. Mr. Chairman, I think modesty is not appropriate when we talk about the exemplary service that Mr. Ben-Veniste gave to the 9/11 Commission, and the role that you and Mrs. Maloney played in pushing that legislation forward to a good conclusion. It's something that those of us who supported your efforts are quite proud of.

Mr. SHAYS. Thank you very much, Mr. Waxman. It was a team effort, and it's nice to be part of a good team.

I would say that any time I link up with Mrs. Maloney, I seem to get things done. So Mr. Ben-Veniste, nice to have you here.

STATEMENT OF RICHARD BEN-VENISTE, COMMISSIONER, NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES

Mr. BEN-VENISTE. Chairman Shays, members of the Subcommittee on National Security, thank you for the privilege of appearing before you today to testify on the subject of emerging threats, overclassification and pseudo-classification.

I would like to address my remarks to three separate topics. First, the recommendations of the 9/11 Commission as they relate to the question of overclassification; second, the experience of the 9/11 Commission with respect to declassification of its final report; and third, the experience of the Commission, now former Commission, with respect to the staff report submitted to the administration for declassification. That report, entitled, "The Four Flights and Civil Aviation Security," was submitted to the administration on the last day of the Commission's existence, August 21, 2004.

Let me start with the recommendations of the 9/11 Commission with respect to classification. All Commissioners understand the need to know principle and its importance. That principle exists for good reason: the need to protect sources and methods of intelligence. The Commission found, however, that the failure to share information was the single most important reason why the U.S. Government failed to detect and disrupt the September 11 plot.

There were bits and pieces of critical information available in different parts of the Government, in the CIA, the FBI, and the NSA. Some of the bits were bigger than others. But pieces of the information were never shared and never put together in time to understand the September 11 plot.

We cannot say for certain that the sharing of information would have succeeded in disrupting the plot. No one can. But we can know for certain that the failure to share information contributed to the Government's failure to interrupt the plot. The failure to share information may have cost lives. We paid a terrible price on September 11th because too much information was kept secret or otherwise not shared.

Within the intelligence community, there are two basic reasons why information is not shared. First, the intelligence community is a collection of fiefdoms, 15 separate agencies. They have separate cultures. They desire to protect their own turf. They distrust the ability of their counterparts to protect information and they design their computers so that they cannot transmit data easily from one agency to another.

Second, information is not shared because of the need to know principle. I want to underscore again, all Commissioners understood the importance of protecting sources and methods. But the need to know principle also results in too much classification and too much compartmentalization of information. Not only do we end up keeping secrets from the enemy, but we end up keeping secrets from ourselves. Timely information does not get to the analyst and to the policymaker. Important information is denied the American people.

Mr. Chairman, the chief reason the 9/11 Commission recommended the creation of a director of national intelligence was so that someone could smash the stovepipes in order to demand the sharing of information and force cooperation across the intelligence community. We want one individual in charge of information technology to unclog the arteries of information sharing across the intelligence community. We want one individual in charge of security rules and one set of rules for security, so that as much information as possible flows to analysts, policymakers and those on the front lines with security responsibilities.

We want to make sure that the President gets the information he needs to do the job, and so does the border inspector and so does the cop on the beat. Information has to flow more freely. Much more information needs to be declassified. A great deal of information should never be classified at all.

Mr. Chairman, my personal view is that an unconscionable culture of secrecy has grown up in our Nation since the cold war. Secrecy has often acted as the handmaiden of complacency, arrogance and incompetence. Senator Pat Moynihan, a passionate opponent of unnecessary secrecy in Government, called for the creation of a counter-culture of openness, a climate which simply assumes that secrecy is not the starting place. It is time we heeded that call.

The Nazi War Crimes Disclosure Act, signed by President Clinton in 1998, created an interagency working group to implement the act's mandate of declassifying documents relating to World War II war crimes and their perpetrators, still kept secret by our Government. As one of three non-governmental members of the IWG appointed by President Clinton, I have had direct experience with the difficulties of getting public release of records stamped secret. So far, over 8 million pages of previously classified documents have been released. National security has not been jeopardized. Yet but for this act, these records would still be secret.

Recently, despite the fact that relevant records are in some cases more than 50 years old, the CIA balked at full compliance with the act, causing a delay of more than a year in the IWG's work. Finally, to break the impasse, the IWG had to seek congressional intervention. The act's authors, Senator Mike DeWine and Representative Carolyn Maloney, rejected the CIA's argument for withholding important documents in a meeting with CIA and IWG officials. Ultimately the CIA abandoned its opposition and has now promised to comply.

The Senate recently passed a bill authorizing a 2-year extension of the IWG, which is scheduled to expire at the end of this month. The House has not yet acted.

Let me return to the Commission's experience with declassification. Mr. Chairman, the 9/11 Commission, had many challenges in gaining access to highly classified and sensitive material it needed to conduct its investigation and complete its work. We had a number of differences with the executive branch on questions of access. You are familiar with many of them, and I will not recount them in detail. Suffice it to say, with strong support from the American public, and from many Members of Congress, the Commission eventually gained access to documents and witnesses it needed to conduct its work.

The Commission has had similar challenges in the declassification review process. We saw it as our obligation to make as much information available to the American public in as timely a fashion as possible. Within the administration, there are different voices. Clearly, some individuals and agencies wanted to block the release of material. Because our bipartisan Commission spoke with a consistently unanimous voice on the issue of transparency, we were able to overcome those objections and move forward.

Beginning with the Commission staff statements, we developed a process where a White House designated point of contact coordinated the review and declassification of the Commission's written product. Eventually, our point of contact became Dan Levin, then at the Justice Department, who did an exemplary job. He kept the agencies on tight deadlines, and worked with us to solve problems and keep the process on track. Lawyers from the White House Counsel's office also worked hard to solve issues in the pre-publication review process. Solving problems in most cases meant modest word changes and minor massaging of the text.

The staff statements were in large measure the building blocks for the final report. The process we established for declassification of the staff statements helped us immensely in the declassification review of the Commission's final report.

We are very proud to say that the final report of the Commission was issued without a single redaction. There was not a single paragraph, not a single sentence blacked out from what we believed we needed to say to tell the full story of September 11 to the American public. We commend the administration for recognizing that a critical component for enhancing national security was to tell the story of September 11 completely and credibly. The 9/11 Commission report without redactions helped to win the public's interest and the public's confidence. The integrity of the report helped our Government and Nation move forward with the reform bill signed into law by the President last December.

Let me address the staff report on the four flights and the civil aviation issue of civil aviation security. The Commission also had good experience with the administration in the completion of two staff reports on terrorist finance and terrorist travel that were issued without redactions on the last day of the Commission's existence, August 21, 2004. On the last day of its existence, the Commission also submitted its third and final staff report to the administration for declassification review. That staff report was entitled, "The Four Flights and Civil Aviation Security."

As in the case of the other two reports, it provides a wealth of additional detail in support of the facts and conclusions in the

Commission's final report. As the Commission's general counsel made clear to the administration at the time of the staff report's submission, he and several staff retained their security clearances even after the end of the life of the Commission. Thus, in our view, staff still should have been able to work with the administration to address any concerns about classification in a mutually satisfactory manner, so that this staff report, like the two previous staff reports, could be issued without redactions.

As this process had worked so well previously, we did not anticipate that it would not be utilized with respect to the final report. We cannot say with certainty why the declassification review of this last staff report took so long and why the outcome was so unsatisfactory. Part of the answer is that the administration decided it could no longer negotiate with former Commission staff, including the office of the staff report, because they became private citizens after August 21st. The administration refused to engage former Commission staff or commissioners in dialog about the declassification process. In the absence of a dialog and pressure from an existing commission, the declassification process took an inordinate amount of time and produced an unsatisfactory result.

What we find especially troubling about the redactions in this last staff report is that most of them relate to material known as sensitive security information [SSI], under the control of the Federal Aviation Administration before September 11 and under the control of the Transportation Security Administration today. There is little material in this last staff report from the intelligence community. So we have the remarkable situation that the Nation's most highly classified secrets, those that relate to NSA intercepts and covert action, and those that go into the President's daily brief, got declassified and put in a public report, read now by millions of people.

In contrast, far less sensitive material in this last staff report got blacked out or replaced with blank pages. Indeed, one redaction deletes a sentence from public testimony in a hearing before the 9/11 Commission. Some of the redactions, that's at page 56, if you care to check that monograph. Some of the redactions relate to the performance of airport security checkpoints and equipment before September 11. We believe that the public needs to know what the Commission staff wrote about checkpoint performance. Some of the redactions relate to security warnings associated with FAA notices to the airlines leading up to September 11. We believe the public needs to know the nature of those warnings.

Some of the redactions relate to a description of the FAA's no-fly list and criticism of how it was administered. We believe the public needs to know the nature of that criticism. We do not believe these redactions are justified, because they concern a civil aviation system that no longer exists. That system is gone forever. We see no public purpose served in keeping its flaws hidden. Those flaws certainly were apparent to the hijackers. The American people should know them in full as well.

These redactions are a disservice to the September 11 families, to the Commission and to the Nation. They deprive the public of the information it deserves. They stoke the fires of public cynicism. Redactions feed conspiracy theories and undermine confidence.

This is the very reason why we employed our open hearings, that we were transparent not only in our staff reports, but in talking about what was in them publicly. We wanted to avoid the mistakes of past commissions, where conspiracy theories grew up and still persist.

So we tried to be as transparent as possible in doing our work. Redactions inevitably lead to questions. What won't our leaders tell us? What won't they allow us to know? Redactions serve neither the public interest nor the cause of truth.

Mr. Chairman, let me conclude by saying that the Public Discourse Project, the not-for-profit organization of which of the September 11 commissioners is a member, has offered a simple and constructive proposal with respect to this last staff report. If the administration were willing to meet with former Commission staff, including those who drafted this report, we're confident that a report without redactions could be reproduced in short order. Such a proposal was made to the White House in writing, and to date it has not been accepted.

Such a report with integrity and credibility is exactly the kind of report that the American Government should produce and the kind of report that the American public deserves.

Thank you very much, and thank you for your kind remarks. I would be pleased to answer any questions you may have.

[The prepared statement of Mr. Ben-Veniste follows:]

Prepared Statement of
Richard Ben-Veniste, former Commissioner,
National Commission on Terrorist Attacks Upon the United States
before the Subcommittee on National Security,
Emerging Threats and International Relations
Committee on Government Reform
U.S. House of Representatives
March 2, 2005

Chairman Shays, Ranking Member Kucinich, Members of the Subcommittee on National Security: Thank you for the privilege of appearing before you today to testify on the topic of "Emerging Threats: Overclassification and Pseudoclassification."

I would like to address my remarks to three separate topics:

-- First, the recommendations of the 9/11 Commission as they relate to the question of overclassification;

-- Second, the experience of the 9/11 Commission with respect to declassification of its final report; and

-- Third, the experience of the Commission – now former Commission – with respect to the last staff report submitted to the Administration for declassification. That report, entitled "The Four Flights and Civil Aviation Security," was submitted to the Administration on the last day of the Commission's existence -- August, 21, 2004.

Recommendations of the 9/11 Commission

Let me start with the recommendations of the 9/11 Commission with respect to classification. All Commissioners understand the "need to know" principle and its importance. That principle exists for a good reason: the need to protect sources and methods of intelligence.

The Commission found, however, that the failure to share information was the single most important reason why the United States government failed to detect and disrupt the 9/11 plot. There were bits and pieces of critical information available in different parts of the government – in the CIA, the FBI, and NSA – but the pieces of information were never shared, and never put together in time to understand the 9/11 plot.

We cannot say for certain that the sharing of information would have succeeded in disrupting the plot. No one can. But we know for certain that the failure to share information contributed to the government's failure to interrupt the plot. The failure to share information may have cost lives. We paid a terrible price on September 11 because too much information was kept secret or otherwise not shared.

Within the intelligence community, there are two basic reasons why information is not shared:

First, the intelligence community is a collection of fiefdoms, fifteen separate agencies.

-- They have separate cultures;

-- They desire to protect their own turf;

-- They distrust the ability of counterparts to protect their information; and

-- They designed their computers so that they cannot transmit data easily from one agency to another;

Second, information is not shared because of the "need to know" principle. I want to underscore again: All Commissioners understand the importance of protecting sources and methods.

-- But the "need to know" principle also results in too much classification and too much compartmentation of information.

-- Not only do we end up keeping secrets from the enemy, but we end up keeping secrets from ourselves.

-- Timely information does not get to the analyst and to the policymaker.

-- Important information is denied to the American people.

Mr. Chairman, the chief reason the 9/11 Commission recommended the creation of a Director of National Intelligence was so that someone could "smash the stovepipes," order the sharing of information and force cooperation across the Intelligence Community.

-- We want one individual in charge of information technology, to

unclog the arteries of information sharing across the intelligence community.

-- We want one individual in charge of security rules, and one set of rules for security, so that as much information as possible flows to analysts, policymakers, and those on the front lines with security responsibilities.

-- We want to make sure that the President gets the information he needs to do his job -- and so does the border inspector and the cop on the beat.

Information has to flow more freely. Much more information needs to be declassified. A great deal of information should never be classified at all.

Mr. Chairman, my personal view is that an unconscionable culture of secrecy has grown up in our nation since the cold War. Secrecy has often acted as the handmaiden of complacency, arrogance and incompetence. Sen. Pat Moynihan, a passionate opponent of unnecessary secrecy in government, called for a "counter culture of openness, a climate which simply assumes that secrecy is not the starting place." It is time we heeded that call.

The Nazi War Crimes Disclosure Act signed by President Clinton in 1998, created an Interagency Working Group to implement the Act's mandate of declassifying documents relating to WWII war crimes and their perpetrators still kept secret by the government. As one of three non-government members of the IWG appointed by President Clinton, I have had direct experience with the difficulties of getting public release of records stamped "secret." So far, over 8 million pages of previously

classified documents have been released. National security has not been jeopardized. Yet, but for the Act, these records would still be secret.

Recently, despite the fact that relevant records are in some cases more than 50 years old, the CIA balked at full compliance, causing a delay of more than a year in the IWG's work. Finally, to break the impasse, the IWG had to seek Congressional intervention. The Act's authors, Sen. Mike DeWine and Rep. Carolyn Maloney, rejected the CIA's argument for withholding important documents in a meeting with IWG and CIA officials. Ultimately, the CIA abandoned its opposition and has promised to comply.

The Commission Experience with Declassification

Mr. Chairman, the Commission had many challenges in gaining access to the highly-classified and sensitive material it needed to conduct its investigation and complete its work. We had a number of differences with the Executive branch on questions of access. You are familiar with many of them, and I will not recount them in detail.

Suffice it to say, with strong support from the American public and from many Members of Congress, the Commission eventually gained access to the documents and witnesses it needed to conduct its work.

The Commission had similar challenges in the declassification review process. We saw it as our obligation to make as much information available to the American public in as timely a fashion as possible. Within the Administration, there were different voices. Clearly, some individuals and agencies wanted to block the release of material. Because our bi-partisan Commission spoke with a consistently unanimous voice on the issue of transparency, we were able to overcome

the objections and move forward.

Beginning with Commission staff statements, we developed a process where a White House-designated point of contact coordinated the review and declassification of the Commission's written product. Our point of contact, Dan Levin, then at the Justice Department, did an exemplary job. He kept the agencies on tight deadlines, and worked with us to solve problems and keep the process on track. Lawyers from the White House Counsel's office also worked hard to solve issues in the pre-publication review process. Solving problems, in most cases, meant modest word changes and minor massaging of the text.

The staff statements were in large measure the building blocks for the final Report. The process we established for declassification of the staff statements helped us immensely in the declassification review of the Commission's final Report.

We are very proud to say that the final Report of the Commission was issued without a single redaction. There was not a single paragraph, not a single sentence, blacked out from what we believe we needed to say to tell the full story of 9/11 of the American public. We commend the Administration for recognizing that a critical component for enhancing national security was to tell the story of 9/11 completely and credibly.

The 9/11 Commission Report – without redactions – helped to win the public's interest and the public's confidence. The integrity of the report helped our government and nation move forward with the reform bill signed into law by the President in December.

Staff Report on the Four Flights and Civil Aviation Security

The Commission also had a good experience with the Administration in the completion of two staff reports -- on Terrorist Finance and Terrorist Travel -- that were issued, without redactions, on the last day of the Commission's existence, August 21, 2004.

On the last day of its existence the Commission also submitted its final staff report to the Administration for declassification review. That staff report was entitled "The Four Flights and Civil Aviation Security." As in the case of the other two staff reports, it provides a wealth of additional detail in support of the facts and conclusions in the Commission's final Report.

As the Commission's General Counsel made clear to the Administration at the time of this staff report's submission, he and several staff retained their security clearances even after the end of the life of the Commission. Thus, in our view, staff still should have been able to work with the Administration to address concerns about classification in a mutually satisfactory manner, so that this staff report – like the two previous staff reports – could be issued without redactions. As this process had worked so well previously, we did not anticipate that it would not be utilized with respect to the final staff report.

We cannot say with certainty why the declassification review of this last staff report took so long, and why the outcome was so unsatisfactory. Part of the answer is that the Administration decided it could no longer negotiate with former Commission staff – including the authors of the report – because they became private citizens after August 21st. The Administration refused to engage former Commission staff in a dialogue about the declassification process. In the absence of dialogue and pressure from an existing Commission, the declassification process took an inordinate amount of time and produced an unsatisfactory result.

What we find especially troubling about the redactions in this last staff report is that most of them relate to material known as "Sensitive Security Information," or SSI, information under the control of the Federal Aviation Administration before 9/11, and under the control of the Transportation Security Administration today. There is little material in this last staff report from the Intelligence Community. So we have the remarkable situation that the nation's most highly classified secrets – those that relate to NSA intercepts and covert action, and those that go into the President's Daily Brief – got declassified and put in a public report read by millions of citizens. In contrast, far less sensitive material in this last staff report got blacked out or replaced with blank pages. Indeed, one redaction deletes a sentence from public testimony before the Commission.

Some of the redactions relate to the performance of airport security checkpoints and equipment before 9/11. We believe the public needs to know what the Commission staff wrote about checkpoint performance.

Some of the redactions relate to security warnings associated with FAA notices to the airlines leading up to 9/11. We believe the public needs to know the nature of those warnings.

Some of the redactions relate to a description of the FAA's "No-Fly" List and criticism of how it was administered. We believe the public needs to know the nature of that criticism.

We do not believe these redactions are justified, because they concern *a civil aviation security system that no longer exists*. That system is gone forever, and we see no public purpose served in keeping its flaws hidden. Those flaws certainly were apparent to the hijackers; the American people should know about them in full as well.

These redactions are a disservice to the 9/11 families, to the Commission, and to the nation. They deprive the public of the information it deserves. They stoke the fires of public cynicism. Redactions feed conspiracy theories and undermine confidence. Redactions inevitably lead to questions: What won't our leaders tell us? What won't they allow us to know? Redactions serve neither the public interest nor the cause of truth.

Conclusions

Mr. Chairman, the Public Discourse Project, a not for profit organization of which each former 9-11 Commissioner is a member, offers a simple and constructive proposal: If the Administration is willing to meet with former Commission staff, including those who drafted this report, we are confident that a report without redactions can be produced in short order.

Such a report, with integrity and credibility, is exactly the kind of report that the American government should produce -- and the kind of report that the American people deserve.

Thank you. I will be pleased to try to answer your questions. # # #

Richard Ben-Veniste, a former member of the 9/11 Commission, is a partner in the Washington, D.C. office of Mayer Brown Rowe and Maw, 1909 K St., N.W., Washington, DC 20006, Tel: (202)263-3000.

Mr. SHAYS. Mr. Ben-Veniste, thank you very much. We are going to start out with Mr. Waxman.

Mr. WAXMAN. Mr. Ben-Veniste, thank you for your excellent statement here today and again, for your exemplary service on the 9/11 Commission.

I would like to start with the process the administration went through to declassify the final 9/11 Commission staff report. Your testimony is that the administration refused to consult with 9/11 Commission staff about the redactions, that it took an inordinate amount of time and that it produced an unsatisfactory result.

Let me start with the failure to work with the September 11 staff. The administration allowed September 11 staff to keep their security clearance, isn't that correct?

Mr. BEN-VENISTE. Yes, some of those clearances are kept for other reasons and had been in existence prior to the creation of the Commission.

Mr. WAXMAN. So let me get a clarification. If the administration permitted them to retain their security clearances, why does it matter whether they were employees or not? Why did the administration refuse to consult them about these redactions?

Mr. BEN-VENISTE. In my view, there is no rationale in that regard.

Mr. WAXMAN. Well, that's pretty straight-forward.

Mr. BEN-VENISTE. I try to be, Mr. Waxman.

Mr. WAXMAN. On the timing question, you may have heard Admiral McMahon in our first panel, the head of security and intelligence for the Transportation Department, say that the FAA actually completed its review in September. Did that surprise you?

Mr. BEN-VENISTE. Yes, it did, sir.

Mr. WAXMAN. Do you have any information about why the report was delayed from September until January?

Mr. BEN-VENISTE. I do not.

Mr. WAXMAN. Although this hearing has produced some information, we now have more new questions than answers. I think we will have to pursue this issue further. Who do you recommend the committee talk to for additional information about this declassification process? Officials at the White House and the Justice Department?

Mr. BEN-VENISTE. Yes, Mr. Waxman, I think the three areas are the TSA, the Justice Department and White House counsel's office.

Mr. WAXMAN. Are there any specific documents you believe the committee should specifically request?

Mr. BEN-VENISTE. There are memoranda discussing why this material has been redacted, why it has taken so long. Clearly there has been substantial public interest, by the New York Times and other important publications. And of course, through a hearing like this, which generates appropriate additional public interest. There should be some traffic among the agencies to ask the logical question of what the heck took so long and why.

Mr. WAXMAN. Mr. Chairman, I think what Mr. Ben-Veniste suggests makes a lot of sense. I would like to propose that the subcommittee interview these people and request these documents. We can discuss this further.

Mr. SHAYS. The committee would be happy to do that, and we would be happy to work with your staff to have that happen.

Mr. WAXMAN. Thank you.

Commissioner Ben-Veniste, Condoleezza Rice testified before the 9/11 Commission on April 8, 2004.

Mr. BEN-VENISTE. I remember that.

Mr. WAXMAN. I would like to ask you about the circumstances surrounding her testimony. First, I remember that the White House did not want to allow her to testify. They were very opposed to her appearing before the Commission under oath. If I remember correctly, the Commission's time with Ms. Rice was very truncated. I wonder if you would be able to describe for us the background on that, what was happening behind the scenes?

Mr. BEN-VENISTE. Well, I can only talk about what was happening behind our scene. Obviously we felt that Dr. Rice's testimony would be very important. You may recall that Dr. Rice had characterized certain elements of what became her testimony in public statements in various venues prior to the time that she testified. We felt that it was more than appropriate that Dr. Rice provide her insights and recommendations to us in a public forum, since this was the purpose of the 9/11 Commission and she was an integral part of the history of what occurred prior to September 11. So I believe it was on the basis of the unanimous demand by this bipartisan commission that Dr. Rice appeared publicly before us, under oath, as other witnesses had appeared, to provide an answer to those questions.

Now, as it turned out, her testimony was scheduled for the morning of the same day during which we had already committed to question President Clinton. So when you say truncated, I suppose that's what you mean. I had all of 16 minutes to question. I would have appreciated more time, but we made do with what we had.

Mr. WAXMAN. So you didn't feel that you had a satisfactory amount of time to pursue all the issues you wanted to raise with her?

Mr. BEN-VENISTE. I would have had more questions. And I probably would have been more considerate of the length of her answers, had there been more time.

Mr. WAXMAN. Good point. Her testimony came 3 weeks after she held a press conference at the White House. There she said, "I don't think anybody could have predicted that these people would try to use an airplane as a missile, a hijacked airplane as a missile." But the 9/11 Commission staff report stated that the FAA had indeed considered the possibility that terrorists would hijack a plane and use it as a weapon.

Given the Commission's findings, were you concerned that perhaps her statements were not based on a thorough review of the subject?

Mr. BEN-VENISTE. Well, it's not just the FAA, Mr. Waxman, but within the intelligence community as we had pointed out repeatedly in public hearings and certainly in our final report in various portions of the report, the intelligence community was aware that on perhaps 10 separate occasions involving various plots, some of them interrupted in various stages of preparation, that terrorists were planning to use planes as weapons. One such plot involved

crashing a plane into CIA headquarters. Another plot involved crashing a plane into the Eiffel Tower. We know that someone crashed a plane onto the White House lawn.

This was not something which required anybody to do a great deal of research on. It seemed to us at the time, particularly one familiar with the intelligence apparatus of the United States. I can point to the fact that just prior to September 11, in an overseas conference in Italy we took measures to protect against the use of suicide aircraft flying into buildings at that conference, which of course President Bush attended.

Mr. WAXMAN. When she testified before your Commission, however, she sort of backed off her previous statement and said, this kind of analysis about the use of airplanes as weapons actually was never briefed to us. Were you surprised that she still hadn't been briefed on these FAA warnings by April 2004, 2½ years after the September 11th attacks?

Mr. BEN-VENISTE. I was disappointed, Mr. Waxman. I have a very high threshold for surprise, having operated here in the Nation's Capital for many decades now.

Mr. WAXMAN. She was a National Security Advisor, it was her job to get all the information so she could present it to the President. She had others telling her there was a great deal of urgency, particularly Richard Clarke, that there was a great deal of urgency about Al-Qaeda. You said all these CIA reports and FAA reports were being issued. Yet she wasn't being briefed on it.

Mr. BEN-VENISTE. In our report, we point out that Dr. Rice viewed her function as National Security Advisor in a way somewhat differently than her predecessor, Sandy Berger, in terms of her responsibility for the domestic threats posed by terrorists. Perhaps the next time you have the opportunity to question Dr. Rice, you might ask her about that.

Mr. WAXMAN. She may have viewed her role differently, but she made all the public statements on behalf of the administration, pretty much suggesting that she had this very clear role of developing the policy.

I thank you for your answers to these questions. Thank you, Mr. Chairman.

Mr. SHAYS. I thank the gentleman for his questions and for your responses.

I think one of the important points of the 9/11 Commission was a very clear finding that there were breakdowns in the previous administration, there were breakdowns in the present administration. Had either administration done better or Congress, or had the intelligence community done its better job, any one of those doing better might have changed the outcome. Do you think that's an unfair analysis?

Mr. BEN-VENISTE. I think that there is a mistake in apportioning responsibility in that sort of equivalence. The agencies and individuals who had greater responsibilities, certainly for protecting the homeland. Obviously when you make a generalization, it does a disservice to some and is more generous to others.

Mr. SHAYS. When Mr. Clarke appeared before our subcommittee behind closed doors, it was one of the most shocking experiences I had had. It was before September 11th, and we had by then had

I think about 10 hearings on the terrorist threat, and we were now meeting with the terrorist czar. We asked him what our strategy was to deal with the terrorist threat and he said, we don't have any strategy.

We were so dumbfounded, his basic response was, we know who the bad guys are and we go after them. We were so surprised by it that the subcommittee wrote him a letter, with his response. And we were so surprised by it that we wrote Condoleezza Rice a letter and said, don't hire the guy, when she took over. But we also told Condoleezza Rice that there was a terrorist threat out there that she needed to deal with, and we don't think they responded to that, either.

I would like to know what you think gives us a culture, a counterculture of openness. What do you think does that? It obviously starts with the White House. But what are things that——

Mr. BEN-VENISTE. It doesn't seem to be coming from the White House, so when we say, where does it start, I think first you identify what the problem is and the problem is that for decades this culture has existed. But for exceptions like the Nazi War Crimes Disclosure Act, which mandates specific declassification, there is no consequence, essentially, to those who unnecessarily withhold and classify materials that are withheld from public inspection.

So the result of that is more and more classification, more and more secrecy, less and less openness. Unless that trend is reversed, if the leadership is not coming from the administration then it's got to come from the Congress. The press is very happy to support, I'm quite sure, efforts toward openness. The spirit that Senator Pat Moynihan was talking about has not yet taken hold. I think legislation is necessary, the creation of ombudsmen or classification authorities within each of the agencies that classifies material would be a step in the right direction.

There are consequences for making mistakes and releasing information. There don't seem to be any consequences to withholding information that should be available to the public.

Mr. SHAYS. What department did you find the most reluctant or the most secretive and what did you find, well, which had the best culture for openness and which had the worst?

Mr. BEN-VENISTE. You know, I don't know—do you mean with respect to the 9/11 Commission?

Mr. SHAYS. Yes, I guess so. In other words, when my staff has looked at the Transportation Department, for the most part they think they have a pretty good policy and practice, for the most part.

Mr. BEN-VENISTE. Part of that depends on making the distinction between who talks the talk and who walks the walk, Mr. Chairman. People may make very soothing noises about cooperation and releasing material and providing them. But until you get down in the weeds and see what's actually produced——

Mr. SHAYS. Well, are you capable of answering the question of, did you have enough interaction with enough agencies to find out anything? Usually you would say, you know, these guys are being a lot more cooperative than this group.

Mr. BEN-VENISTE. We found that the FBI was particularly cooperative, that FBI Director Mueller's leadership was much appre-

ciated. And other places we had to employ a blowtorch and a pair of pliers.

Mr. SHAYS. Thank you. That's helpful.

Mrs. Maloney.

Mrs. MALONEY. I just would like to join with my colleagues in congratulating you on the extraordinary job you and the other commissioners did with the 9/11 Commission report. Really one of my happiest days was the day the President signed the intelligence bill into law. It would not have happened without your dedicated commitment. Also your work on the Nazi War Crimes Disclosure Act, which is continuing, as we are pushing to get an extension to compete the work. So we thank you for your work.

Mr. BEN-VENISTE. Thank you.

Mrs. MALONEY. What defense could you possibly give for the civil aviation document to be so heavily redacted? Do you have any understanding? As I understand, it was the only document that was redacted. Is that true? That's what I read.

Mr. BEN-VENISTE. Substantially yes. There were discussions but there were minor revisions made, and our staff reports, the two other ones that were released, what we call the staff monographs, which are far more detailed expositions of facts that are contained in more summary fashion in some cases than our final report. But that is correct. So if you are asking me to put on my hat as a defense lawyer rather than an observer and an advocate for openness, I would have to plead ignorance on that point.

I went through, in my prepared remarks, a recitation of where we feel that these redactions occurred and why we feel that they were unwarranted in each case, including redacting a statement of Michael Canavan in open testimony before the Commission.

Mrs. MALONEY. Exactly. Ridiculous.

Mr. BEN-VENISTE. Governor Kean and Congressman Hamilton wrote the White House counsel, essentially pointing out the deficiencies, on February 11th, stating basically our disappointment with the classification review process of this last staff statement and offering again to work together with them with our staff. White House counsel responded on March 1st, saying essentially that they had sent the report back to the DOJ——

Mr. SHAYS. We will put that letter into the record.

Mr. BEN-VENISTE. We can do that. We can make both the February 11 and March 1 letters available.

Mr. SHAYS. We will put them both into the record.

[The information referred to follows:]

9/11

Public Discourse Project

Thomas H. Kean
CHAIR

Lee H. Hamilton
VICE CHAIR

BOARD MEMBERS

Richard Ben-Veniste

Fred F. Fielding

Jamie S. Gorelick

Slade Gorton

Bob Kerrey

John F. Lehman

Timothy J. Roemer

James R. Thompson

Christopher A. Kojm
President

February 11, 2005

The Honorable Harriet Miers
Counsel to the President
The White House
Washington, DC 20500

Dear Ms. Miers,

We write with respect to the Administration's classification review of the 9/11 Commission's staff report, "The Four Flights and Civil Aviation Security."

At the expiration of the life of the Commission last August, we had requested the expeditious completion of a classification review of this document.

During the life of the Commission, we had developed an excellent relationship with Judge Gonzales that led to the successful classification review of 17 staff statements, two staff reports and the final report of the Commission. This process involved the review of highly classified, compartmented materials. Through the hard work of the White House Counsel's office, Dan Levin, and others in the Executive branch, the final report of the Commission was completed and submitted to the public without a single redaction. This was a significant accomplishment for the American people, allowing the story of 9/11 to be told in full.

We were disappointed, therefore, that a classification review of this last staff report could not be completed without redactions. This came as a surprise to us, as nearly all of material included in this staff report was of a lower level of sensitivity than material that had previously been placed in the public record.

We respectfully request that another effort be made to release this staff report without redactions. Several members of the former Commission staff retain security clearances and would be willing to cooperate in any way with you and your office to achieve this desirable outcome.

Finally, we wish you every success in your new and important assignment in service to our nation.

With best regards,

Tom Kean

Lee Hamilton

One Dupont Circle, NW, Suite 700, Washington, DC 20036
202 776-0302 www.9-11pdp.org fax 202 776-9087

THE WHITE HOUSE
WASHINGTON
March 1, 2005

The Honorable Thomas H. Kean
The Honorable Lee H. Hamilton
9/11 Public Discourse Project
One Dupont Circle, N.W., Suite 700
Washington, D.C. 20036

Dear Governor Kean and Mr. Hamilton:

Thank you for your February 11 letter regarding the 9/11 Commission staff monograph, "The Four Flights and Civil Aviation Security" ("monograph"). This letter responds to the issue you raise.

My understanding is that the then-General Counsel of the Commission submitted to the Department of Justice ("DOJ") this 120-page monograph on the last day of the Commission's existence (August 21, 2004). I also understand the Commission had in its possession the information underlying the monograph when the Commission drafted its final report, and presumably included in that report the key information it wished to make public. Because this monograph was not submitted by the July 26, 2004 deadline and was not "agreed to by a majority of Commissioners," it does not fit within the legal requirements imposed by Congress for Commission reports. However, as an accommodation to the Commission, DOJ spearheaded a pre-publication review of the monograph to determine whether it could be publicly released consistent with the constitutional and statutory obligation to protect classified and other sensitive national security information. I am advised this exercise resulted in certain redactions to protect detailed descriptions of aviation security measures from disclosure to those who might attempt attacks on aircraft in America in the future.

As you note, throughout the Commission's existence, because of the cooperative relationship between the Executive Branch and the Commission, all Commission reports, staff monographs, and staff statements were released without redaction. [illegible] this was often accomplished by agreeing to certain textual changes in the Commission's drafts. However, because the Commission ceased to exist hours after this monograph was submitted, DOJ concluded that – unlike with prior Commission reports – no legal representative of the former Commission was properly empowered to revise the monograph or negotiate with DOJ on the Commission's behalf regarding classification issues.

I am pleased that the White House Counsel's Office and General Gonzales were able to work with you and the Commission cooperatively, and I look forward to continuing those good relationships with you. I have asked for further review of your request as to whether the monograph can be released responsibly without redactions.

Sincerely,

Harriet Miers
Counsel to the President

Mrs. MALONEY. Thank you.

I would like to ask you about Sibel Edmonds. As you know, the former FBI translator, Ms. Edmonds, is going to be testifying today. The Commission also had a chance to interview her, as well as to raise her case before FBI Director Mueller, when you met with him. The Justice Department Inspector General recently released its report on her allegations, finding that they were credible and supported by other witnesses and evidence.

I would like to ask you, Mr. Ben-Veniste, did the Commission also find her to be credible?

Mr. BEN-VENISTE. Well, I can't speak for the Commission on that, Mrs. Maloney, because that was something where the Commission made a determination that her assertions were under active investigation by the IG's office. I think Mr. Fein has done extraordinary service to this country in the work he has performed over time as Inspector General of the Department of Justice and I have no reason to think that his report is anything but credible and accurate with respect to Ms. Edmonds.

Mr. SHAYS. We have 5 minutes to vote.

Mrs. MALONEY. We have to run and vote. It's always a great pleasure to see you and thank you again for your great service.

Mr. SHAYS. So we will close this panel, and thank you for your testimony, Mr. Ben-Veniste. Thank you very much. We will start with the third panel when we get back, and we are recessed.

[Recess.]

Mr. SHAYS. The Subcommittee on National Security, Emerging Threats, International Relations is now reconvened for our hearing on Emerging Threats, Overclassification and Pseudo-Classification.

I will introduce our three panelists. Mr. Thomas Blanton, executive director, National Security Archive, George Washington University; Mr. Harry A. Hammitt, editor and publisher, Access Reports: Freedom of Information, Lynchburg, VA; and Ms. Sibel Edmonds, former contract linguist, Federal Bureau of Investigation. Welcome.

If you would stand, I will swear you all in, as we do in our subcommittee. Please raise your right hands.

[Witnesses sworn.]

Mr. SHAYS. Note for the record all three witnesses have responded in the affirmative. We appreciate your patience as we begin this third panel at 4 p.m.

We'll just start with you, Mr. Blanton, and we'll go from there.

STATEMENTS OF THOMAS BLANTON, EXECUTIVE DIRECTOR, NATIONAL SECURITY ARCHIVE, GEORGE WASHINGTON UNIVERSITY; HARRY A. HAMMITT, EDITOR AND PUBLISHER, ACCESS REPORTS: FREEDOM OF INFORMATION; SIBEL EDMONDS, FORMER CONTRACT LINGUIST, FEDERAL BUREAU OF INVESTIGATION

STATEMENT OF THOMAS BLANTON

Mr. BLANTON. Thank you very much, Mr. Chairman. It is a privilege to be here with you today, also to be here in the Rayburn Building, because Sam Rayburn is quite famous in my family for having broken up a fist fight on the floor of the House of Rep-

resentatives that was started by a relative of mine, a Congressman named Thomas Blanton of Texas. He broke up the fist fight by picking up Tom by the scruff of the neck and pulling him away. I just suggest, Mr. Chairman, that your subcommittee has the secrecy and the pseudo-secrecy system by the scruff of the neck. It's up to you to pull it away so it stops doing damage to our security.

Mr. SHAYS. Will we get a building named after us? [Laughter.]

Mr. BLANTON. I would hope so.

What I want to do today, very briefly, Mr. Chairman, is try to diagnose the problem and offer a couple of solutions. Up on the screen, you see this wonderful little graphic that just takes all the data that Bill Leonard's wonderful audit office has amassed since its start in 1980, that's the first time that we started counting the number of national security secrets, the number of secrecy decisions. You can see that last year, in 2003, the number of new national security secrecy decisions broke the previous record at the height of the cold war. What I just found out today, from your hearing, Mr. Chairman, from Mr. Leonard, is that his new report out at the end of the month says the new number will actually go off this chart. Secrecy is off the charts. It will be 16.1 million, is the latest data from 2004.

Now, two things to remember about each one of these decisions. One is they create a stream of secrets, because through the magic of e-mail, computers, xeroxing, copying attachments, referencing, they actually generate far more documents than just the 14 or 16 million that are stamped. Second, they create a stream of costs out into the future, direct costs to taxpayers. The 2003 estimate was $6.5 billion, and that's the unclassified number, we don't know what it costs from the CIA. And a stream of indirect costs in ignorance and inefficiency and inaction, like in the September 11 example.

So the question to ask is the one you asked at your August 24th hearing. You asked how much overclassification exists. What I did is just put into one page some of the great answers that you got. From 50 percent, said the Pentagon's Deputy Under Secretary of Defense for Counter-Intelligence and Security, beyond 50 percent is what Mr. Leonard said. Sixty percent is what the Interagency Security Classification Appeals has done, ruled for the requestor. Seventy-five percent is what Tom Kean, the chair of the 9/11 Commission said. Ninety percent was the estimate of President Reagan's own National Security Council Executive Secretary in quotes to the Moynihan Commission. That's how much overclassification, 50 to 90 percent.

Bottom line, you can sum it up, Houston, we have a problem. The antidote to secrecy is this slide, the rise and fall of declassification. Again, these are based on the ISOO numbers, they're based on sampling of all the agencies that classify information or declassify. What you see here is during the cold war we had a relatively low level of declassification running along for quite a while. In the mid-1990's, boom, with the reforms that were in President Clinton's Executive order, continued by President Bush, the threat of automatic declassification really clarifies the agency's mind. You had a boom, and in this period more historical national security secrets came out than from all previous Presidents put together.

It has now plummeted. The level is still a little bit higher than it was in the cold war, and that's a positive sign.

The scary stuff is the stuff we can't count. The new forms of pseudo-classification like sensitive but unclassified, for official use only. This is a fun little response to a Freedom of Information Act request. It was a meeting between the Homeland Security Secretary Tom Ridge and the Pakistani Foreign Minister. This was a briefing memo given to Secretary Ridge. It says what your purposes are in assuming that we're going to work with the Pakistanis and not treat Pakistanis too badly when they come into our country.

The entire background section is cut out. They could not find an identifiable harm under national security to withhold this information. So instead, they called it sensitive but unclassified and have used the fifth exemption to the Freedom of Information Act, the one about deliberative process, to withhold the whole thing. This kind of labeling is what's proliferating inside the bureaucracy. You see dozens of examples we're already getting from people like the Transportation Security Administration.

For example, this next slide is just one example from our Freedom of Information request about a circular, one of those aviation warnings that Congresswoman Maloney and others were talking about that are mentioned in the September 11 report. One of the warnings before September 11, it's an unclassified circular but it's withheld under SBU, withheld under sensitive information, even though the exact quote from it was printed in the No. 1 best selling 9/11 Commission Report and in the congressional inquiry.

So the problem here is that the proliferation, which is uncounted, unchecked, they have no rules, they have no real standards, they have no audit agency like Mr. Leonard's, they have no independent review boards like Richard Ben-Veniste's review board on the Nazi war crimes. There's none of the kinds of checks and balances. Our framers were trying to change a culture in 1776. There's a culture of monarchy.

How do you change a culture? You set up competing centers of power and checks and balances on all that power. If you have an intelligence czar, you probably need a declassification czar. If you have an agency that's creating new labels like SBU, you need an independent review board in that agency to look at those decisions and push them out. That's the only way that we're going to get our hands around this problem, because frankly, the bottom line, and this is the one place in the 9/11 Commission report where they say the attacks could have been prevented, it's the only finding in the entire report where they say with any amount of certainty, we could have prevented it.

And what do they say? According to the interrogation of Ramzi Binalshibh, the pay master of the hijackers, if the planners had known that Moussaoui, the Minnesota flyboy, the one who only wanted to learn to fly, not to take off or land, had been arrested, then they would have canceled the September 11 attacks. Why is that? Because that FBI agent out in Phoenix would have read about in the paper, oh, another Islamic extremist arrested at the flight schools. Let's dig that memo I sent to Washington out of the vault and get it around to all the field offices. Maybe the two guys

that they had already identified being in the United States might have shown up on the 10 most wanted list.

I mean, this is the only moment the Commission said publicity about the arrest might have derailed the plot. Publicity. Now, publicity is not a program like the SHARE Network that you heard described in the August hearing, the Markle Foundation Report that the 9/11 Commission bought into. I say basically that SHARE concept is not publicity, and it's not really a challenge to the need to know culture. It's an expansion of the need to know culture to cover more people. Mr. Crowell, your witness, said last summer, he said that the network would include "the relevant players."

Who decides who the relevant players are? Is it the epidemiologist but not the general practitioners? Is it the power plant owners? What about the workers? If it doesn't include the public, if it doesn't push the secrets out, then it's a system that's not going to work. Then we're right back to this obsolete notion of need to know.

I have to say that I think because of this finding, the Deputy Under Secretary of Defense was wrong when she testified before your subcommittee last summer as well, because she said the tension here, "How much risk is the Nation willing to endure in the quest to balance protection against the public's desire to know?" That's absolutely the wrong formulation. The lesson of September 11 is that secrecy was the problem. Secrecy destroyed our protection. Too much secrecy was the core of the unconnecting of the dots.

The teaching is between a natural bureaucratic imperative that spans every administration, that goes back to the dawn of bureaucracy, ancient Iraq under Hammarabi, probably. To control information, because information is power and turf and resources. Versus how do we actually protect ourselves? Will this information if it's released damage us or help protect us?

The core rule of computer security in the computer security world is, if the bug is secret, then the only people who know are the vendor and the hacker. The larger community of users can neither protect themselves, nor offer fixes. That to me should be the principle that we proceed with looking at all of these labels. Does this information withholding make us safer or not? I think most of these new labels would fail abjectly.

The question is, how do you make them fail? That's my final point. It's just simply, you have to build in an independent review board at every agency with a small staff with people like Richard Ben-Veniste on it, asking those questions inside the agency. You might just want to start with a pretty simple measure, ask Admiral McMahon to count the number of sensitive but unclassified or for official use only items created in his agency last year. He can tell you that he created six actual national security secrets. He has to report that number to Mr. Leonard's office. There is a limited number of people in his agency who even have the authority to list something as secret. Ask him to do that about the SBU and FUOU and SSI and all these other labels, and you've got a start.

If you can count them, you can restrain them. If you can put a cost on them, you can restrain them. If you can set up an independ-

ent power structure to push against them, you can restrain them. If you limit the number of officials who can label them, who can create secrets, who can create these labels and you expand the number of officials who are releasing information, then you'll win.

[The prepared statement of Mr. Blanton follows:]

Statement by **Thomas S. Blanton**, National Security Archive, George Washington University
March 2, 2005

Hearing on "Emerging Threats: Overclassification and Pseudo-classification"

2154 Rayburn House Office Building
Subcommittee on National Security, Emerging Threats, and International Relations
Committee on Government Reform
U.S. House of Representatives

Rising Tide of Secrecy

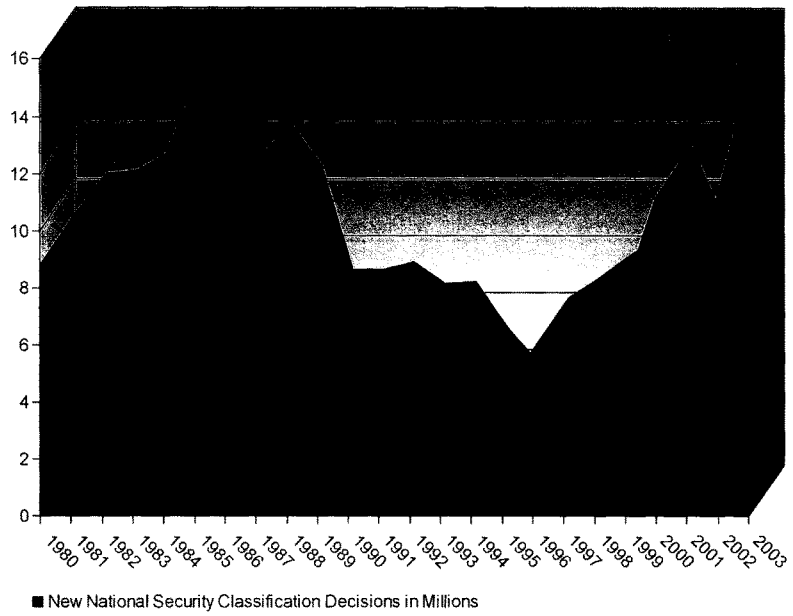


Chart by Jamie Noguchi, National Security Archive
Data from Information Security Oversight Office at the National Archives

Statement by **Thomas S. Blanton**, National Security Archive, George Washington University
March 2, 2005

Hearing on "Emerging Threats: Overclassification and Pseudo-classification"

2154 Rayburn House Office Building
Subcommittee on National Security, Emerging Threats, and International Relations
Committee on Government Reform
U.S. House of Representatives

How Much Overclassification?

"Massive" – Erwin Griswold, Former Solicitor General of the United States (who prosecuted the Pentagon Papers case in 1971), quoted in the *Washington Post*, February 15, 1989.

"50-50" – Carol A. Haave, Deputy Undersecretary of Defense for Counterintelligence and Security, August 24, 2004 hearing of this Subcommittee.

"Even beyond 50%" – J. William Leonard, Director of the Information Security Oversight Office, National Archives and Records Administration, August 24, 2004 hearing of this Subcommittee.

60% -- Information Security Classification Appeals Panel rulings for declassification against agency claims of secrecy, according to J. William Leonard testimony, August 24, 2004 ("60-some-odd percent of the time the panel will override an agency's determination in whole or in part").

75% -- Thomas H. Kean, Chair of the 9/11 Commission and former Governor of New Jersey, quoted in Cox News Service, July 21, 2004 ("Three-quarters of what I read that was classified shouldn't have been").

90% -- Rodney B. McDaniel, executive secretary of the National Security Council under President Reagan, quoted in Moynihan Commission report (1997), p. 36, saying only 10% of classification was for "legitimate protection of secrets."

"Laughable if it wasn't so insulting" – Senator Trent Lott (R-Mississippi), on the CIA's redaction of the Senate Intelligence Committee report on Iraq weapons of mass destruction, quoted in Cox News Service, July 21, 2004.

Statement by **Thomas S. Blanton**, National Security Archive, George Washington University
March 2, 2005

Hearing on "Emerging Threats: Overclassification and Pseudo-classification"

2154 Rayburn House Office Building
Subcommittee on National Security, Emerging Threats, and International Relations
Committee on Government Reform
U.S. House of Representatives

Rise and Fall of Declassification

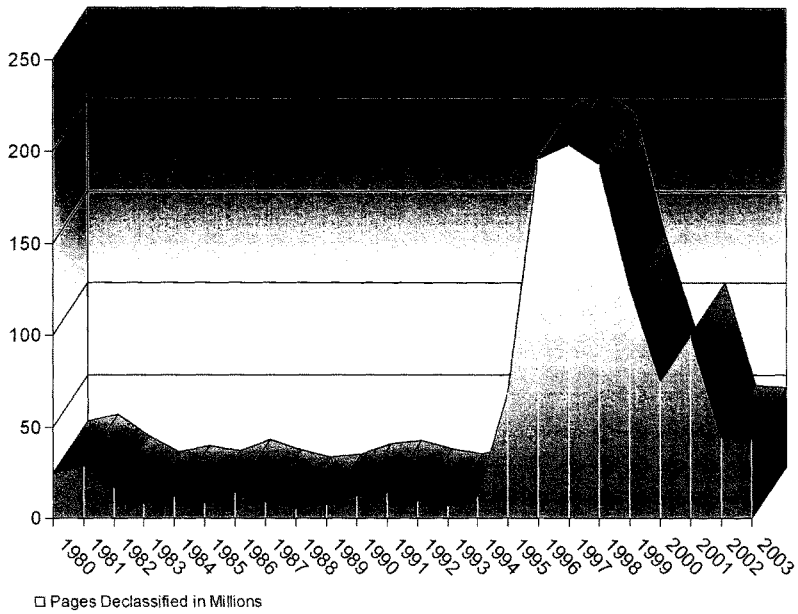


Chart by Jamie Noguchi, National Security Archive
Data from Information Security Oversight Office at the National Archives

Statement by **Thomas S. Blanton**, National Security Archive, George Washington University
March 2, 2005

Hearing on "Emerging Threats: Overclassification and Pseudo-classification"

2154 Rayburn House Office Building
Subcommittee on National Security, Emerging Threats, and International Relations
Committee on Government Reform
U.S. House of Representatives

The New Pseudo-classification

SENSITIVE BUT UNCLASSIFIED

INFORMATION

MEMORANDUM FOR SECRETARY RIDGE

Subject: Your meeting with Mian Khurshid Mahmood KASURI, Minister of Foreign Affairs, Law, Justice, and Human Rights, Pakistan, Friday, January 31, 10:00 10:30 am

Purpose

- Underscore the U.S. Government's appreciation of Pakistan's continued help in the war on terrorism.
- Explain the Department of Homeland Security's mission and organization.
- Emphasize that NSEERS is an important component of our ability to combat the threat of domestic terrorism and that we will strive to minimize its impact on law-abiding visitors to the United States.

Participants in the meeting

U.S.
Secretary Ridge
Pamela Kinney
(Note taker)

Pakistan
Foreign Minister Kasuri
Ambassador Ashraf Jehangir Qazi
Akbar Zaib, Director General (Americas)
Mohammad Sadiq, DCM
Farukh Amil, Counselor
Syed Zulfiqar Gardezi
(note taker)

Background

[redacted]

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED
-2-

[redacted]

SENSITIVE BUT UNCLASSIFIED

Statement by **Thomas S. Blanton**, National Security Archive, George Washington University
March 2, 2005

Hearing on "Emerging Threats: Overclassification and Pseudo-classification"

2154 Rayburn House Office Building
Subcommittee on National Security, Emerging Threats, and International Relations
Committee on Government Reform
U.S. House of Representatives

Pseudo-classification and FOIA

TSA 9-29-04 FOIA Release

Log Entry Date: 06/22/2001
Log Entry Time: 1454
Shift: 2ND Shift (Day)
Entry Classification: UNCLASSIFIED
Watch Officer: [redacted]
IC#s Referenced: [redacted]
Info Circular Referenced: [redacted]

Entry: IMMINENT THREAT: NATIONAL MEDIA REPORTING THREAT ALERT AND MILITARY REACTION IN MIDDLE EAST. ADDITIONALLY, CNN REPORTS ON WORLDWIDE CAUTION IN PROCESS AT STATE. BEGIN DRAFTING [redacted]

Report of the Joint Inquiry Into the Terrorist Attacks of September 11, 2001

- An FAA Circular on June 22, 2001, referring to a possible hijacking plot by Islamic terrorists to secure the release of fourteen persons incarcerated in the United States in connection with the 1996 bombing of Khobar Towers.

[Page 217]

9-11 Commission Report Chapter 8 p. 256

blow up sites in New York City. The reporting noted that operatives might opt to hijack an aircraft or storm a U.S. embassy. This report led to a Federal Aviation Administration (FAA) information circular to airlines noting the potential for "an airline hijacking to free terrorists incarcerated in the United States." Other reporting mentioned that Abu Zubaydah was planning an attack, possibly against Israel, and expected to carry out several more if things went well. On May 24 alone, counterterrorism officials grappled with reports alleging plots in Yemen and Italy, as well as a report about a cell in Canada that an anonymous caller had claimed might be planning an attack against the United States.[10]

9-11 Commission Report Chapter 8 Notes p. 533

10. See CIA, SEIB, "Terrorist Groups Said Cooperating on US Hostage Plot," May 23, 2001; FAA information circular, "Possible Terrorist Threat Against American Citizens, [redacted] June 22, 2001 (this IC expired on August 22, 2001); CIA, SEIB, "Bin Ladin Network's Plans Advancing," May 26, 2001; NSC email, Clarke to Rice and Hadley, "A day in the life of Terrorism Intelligence," May 24, 2001.

Statement by **Thomas S. Blanton**, National Security Archive, George Washington University
March 2, 2005

Hearing on "Emerging Threats: Overclassification and Pseudo-classification"

2154 Rayburn House Office Building
Subcommittee on National Security, Emerging Threats, and International Relations
Committee on Government Reform
U.S. House of Representatives

Openness Equals Security

THE

9/11

However, publicity about Moussaoui's arrest and a possible hijacking threat might have derailed the plot.[107]

[page 276]

COMMISSION

REPORT

107. According to Ramzi Binalshibh, had KSM known that Moussaoui had been arrested, he would have cancelled the 9/11 attacks. Intelligence report, interrogation of Ramzi Binalshibh, Feb. 14, 2003.

[page 541]

FINAL REPORT OF THE NATIONAL COMMISSION ON
TERRORIST ATTACKS UPON THE UNITED STATES

AUTHORIZED EDITION

Statement by **Thomas S. Blanton**, National Security Archive, George Washington University
March 2, 2005

Hearing on "Emerging Threats: Overclassification and Pseudo-classification"

2154 Rayburn House Office Building
Subcommittee on National Security, Emerging Threats, and International Relations
Committee on Government Reform
U.S. House of Representatives

Mr. Chairman, and members of the Committee, thank you for this opportunity to speak with you about the growing problem of **government secrecy and the danger it poses to our security**. This Subcommittee has become a model for the Congress as a whole in its diligent oversight of a difficult problem, and I applaud your commitment to air diverse views and to question conventional thinking.

I have reviewed in detail the record of your hearing on August 24, 2004, to which my own organization, the National Security Archive, contributed a reader of declassified documents entitled "Dubious Secrets," featuring General Pinochet's drink preferences (scotch and pisco sours) and a joke terrorist attack on Santa Claus (the secret was that the CIA occasionally has a sense of humor). Mr. Chairman, you asked the question whether overclassification was a 10% problem or a 90% problem, and your witnesses provided some remarkable yardsticks. The deputy undersecretary of defense for counterintelligence and security confessed that **50% of the Pentagon's information was overclassified.** The head of the Information Security Oversight Office said it was even worse, "even beyond 50%." The former official who participated in the Markle Foundation study cited by the 9/11 Commission on information sharing stated that 80-90% (at least in the area of intelligence and technology) was appropriately classified at first, but over time that dwindled down to the 10-20% range.

My own experience is in the realm of declassified national security information. The National Security Archive ranks as probably the most active and successful non-profit user of the Freedom of Information Act: We have filed more than **30,000 Freedom of Information and declassification requests** in our nearly 20 years of operations, resulting in more than six million pages of released documents that might otherwise be secret today (some of them have in fact been reclassified, but the government won't tell us which ones). We have published more than half a million pages on the Web and other formats, along with more than 40 books by our staff and fellows, including the Pulitzer Prize winner in 1996 on Eastern Europe after Communism. We won the George Polk Award in April 2000 for "piercing self-serving veils of government secrecy." We have partners in 35 countries around the world doing the same kind of work today, opening the files of secret police, Politburos, military dictatorships, and the Warsaw Pact, and leveraging openness in both directions.

My own estimate of overclassification in the United States today tends towards the high end of your 90% range, Mr. Chairman. Let me put on the record here several expert assessments to support this view. For example, the distinguished former Solicitor General of the United States who prosecuted the Pentagon Papers case, Dean Erwin Griswold, wrote in the *Washington Post* (15 February 1989) that: *"It quickly becomes apparent to any person who has considerable experience with classified material that there is* ***massive overclassification*** *and that the principal concern of the classifiers is not with national security, but with governmental embarrassment of one sort or another. There may be some basis for short-term classification while plans are being made, or negotiations are going on, but apart from details of weapons systems, there is very rarely any real risk to current national security from the publication of facts relating to transactions in the past, even the fairly recent past."*

Senator Daniel P. Moynihan's commission on reducing and protecting government secrecy quoted Rodney B. McDaniel, a career Navy officer and executive secretary of President Reagan's National Security Council, who estimated in 1991 that **only 10% of classification was for *"legitimate protection of secrets."*** The Moynihan report contrasted this view with that of the then-head of the Information Security Oversight Office, Steven Garfinkel, who stated that overclassification was only a 10% problem. (1997 Report, p. 36) As this Subcommittee heard in August, Mr. Garfinkel's successor has now moved the official estimate above 50%.

A Cox News Service report last summer (21 July 2004) headlined "Lawmakers Frustrated By Delays In Declassifying Documents," quoted the Republican former governor of New Jersey and then-chair of the 9/11 Commission, Thomas H. Kean, as saying, ***"Three-quarters of what I read that was classified shouldn't have been"*** – a 75% judgment. The material Mr. Kean was reviewing included the most recent and sensitive terrorism-related intelligence and counterterrorism information. The same Cox article quoted Senator Trent Lott (R-Miss.) on his frustration with the Senate Intelligence Committee report on Iraq, as reviewed by the CIA: *"The initial thing that came back was absolutely an insult and would be* ***laughable if it wasn't so insulting****, because they redacted half of what we had. A lot of it was to redact a word that revealed nothing."*

I agree with Senator Lott and Governor Kean: national security secrecy is skyrocketing, but like the ballistic missile defense system, it cannot tell the real threat from the decoys. Let's start with the core statistics, or least the most recent ones available, provided by the Information Security Oversight Office in last year's report to the President. New classification decisions are up from 9 million in 2001, to 11 million in 2002, to 14 million in 2003. If you look at that ISOO data all the way back to the first year in which it was collected – 1980 – you will discover that **the number of new secrecy decisions in 2003 is the highest ever recorded, higher even than the peak years of the Cold War in the mid-1980s.**

Tracking the same ISOO data since 1980, we can also see **the rise and fall of declassification in the 1990s**. The ISOO reports show many years of low levels (around 20 million pages per year) until the numbers leap in 1995, stay at the 200 million page

level for three years, and then plummet down under 50 million pages a year now. I think it's fair to say that President Clinton's executive order on secrecy produced the declassification of more historic national security secrets than all previous presidents put together. But now, the system is almost completely out of whack – a point that ISOO's director made at your August hearing.

At least the national security classification system has **formal checks and balances**. By all the evidence of overclassification, these checks do not work very well, but they do exist. They **desperately need strengthening**. I'm thinking not only of ISOO, that lean machine of a small, well-trained professional staff providing audits and oversight, within its limited means, of a vast and sprawling system. There is also the Interagency Security Classification Appeals Panel (ISCAP), which has ruled for openness in some 60% of its cases (there's another marker on the overclassification gauge), although the total number of cases is quite small and involves mostly historical rather than current information. There is also the Office of Management and Budget requirement, first included in appropriations bills in the 1990s, that agencies add up and report their classification costs (the CIA's are still classified, of course) – thus giving us a benchmark number and some sense of comparative expense to the taxpayer. These numbers, over $6.5 billion in fiscal 2003, remind us that every secrecy decision generates a stream of direct costs to the taxpayer, in addition to the indirect costs of inefficiency and information asymmetries.

Likewise, the executive orders governing classification have been around long enough that a cottage industry of insiders and outsiders have developed expertise on how the system works or ought to work. And at least since the 1974 amendments to the Freedom of Information Act, the courts have provided some guidance on classification. In general, the courts defer to the executive (to a fault, I would argue), but along the way, the extra levels of review during litigation almost always force out information that the agencies originally withheld. In other words, **we lose the final decision, but we get documents**.

What's most alarming is that the new forms of secrecy, the "pseudoclassifications" like Sensitive But Unclassified (SBU) or Sensitive Security Information (SSI) or Sensitive Homeland Security Information (SHSI), have **no such checks and balances**. Where is the **audit agency**, tracking the basic data on the number and extent of new restrictions? Where is the **appeals panel**, overriding the reflexive instincts of agencies? Where is the **cost reporting**, or do the agencies lack any clue as to how much the secrecy costs them? Where is the **cost-benefit analysis** inside agencies, or do they not see the double-edged sword inherent in secrecy? Where are the **bureaucratic centers of countervailing power**, pressing for declassification? Where are the court cases, or will judges continue blind deference to executive judgments? Where is the Congress, when the President's lawyers assert unilateral authority over secrecy, detentions, interrogations, and energy policy, among many other topics?

The National Security Archive's experience with pseudoclassification is not encouraging. Among our many projects, we are pursuing the public release of the actual primary sources cited and quoted by the 9/11 Commission, and we have been on the receiving end of an object lesson in reflexive pseudosecrecy at the Transportation Security

Administration. For example, last year we asked for the five Federal Aviation Administration warnings to airlines on terrorism in the months just prior to 9/11 – warnings that were quoted in the 9/11 Commission report and discussed at length in public testimony by high government officials. The TSA responded by denying the entire substance of the documents under five separate exemptions to the Freedom of Information Act, and even withheld the unclassified document titles and Information Circular numbers as "Sensitive Security Information." When we pointed out that the **titles, dates, and numbers were listed in the footnotes to the number one best-selling book in the United States**, the 9/11 Commission report, the TSA painstakingly restored those precise digits and letters in its second response to us, but kept the blackout over everything else.

We have heard from officials at the Department of Justice that these new pseudoclassifications are simply guidance for safeguarding information, and do not change the standards under the Freedom of Information Act. But such a claim turns out to be mere semantics: In every case, the new secrecy stamps tell government bureaucrats "don't risk it"; in every case, **the new labels signal "find a reason to withhold."** In another TSA response to an Archive FOIA request, the agency released a document labeled "Sensitive But Unclassified" across the top, and completely blacked out the full text, including the section labeled "background" – which by definition should have segregable factual information in it. The document briefed Homeland Security Secretary Tom Ridge on an upcoming meeting with the Pakistani Foreign Minister, but evidently officials could not identify any national security harm from release of the briefing, and fell back on the new tools of SBU, together with the much-abused "deliberative process" exemption to the Freedom of Information Act.

As William Leonard of ISOO pointed out at the GovSec Expo (July 29, 2004), SBU protection regimes still exist that date back to the Cold War, and none have been officially discarded. The government, instead, is adding regimes year after year, Mr. Leonard remarked, *"without any regard to what's been done before to a point where I'm concerned today that if you wanted to identify the person in the government or outside the government who understands all the various protection regimes, understands what all the requirements are, understands what all the standards are – that person doesn't exist."*

This dynamic is fundamentally what's wrong with the Markle Foundation recommendations for the SHARE network that were embraced by the 9/11 Commission and about which you heard from Mr. Bill Crowell at your August 2004 hearing. I read his testimony and the two editions of the Markle report with great interest, because the group seems to have begun with the assumption that you share, Mr. Chairman, that the "need to know" secrecy culture is working against our security. But **the group's recommendations do not actually challenge the "need to know" culture. Instead, they embrace the SBU attitude,** the official-use-only elitism. The language in Mr. Crowell's testimony and in the underlying reports gives a remarkable amount of attention to the ways that the SHARE system would help agencies control and track and audit

employees, preventing leaks and authenticating information, keeping the data in the hands of only the relevant players.

That's the key phrase. Mr. Crowell's direct quote before this Subcommittee was: *"While certain information, particularly about sources and methods, must be protected against unauthorized disclosure, the general mindset should be one that strives for broad sharing of information with all of* ***the relevant players*** *in the network."* Who exactly decides who are the relevant players? Where do we draw the line? Are firefighters included in but not health inspectors? Epidemiologists but not general practitioners? Power plant managers but not the plant's workers? First responders but not neighbors? **Aren't we right back where we started at the need to know?** What will stop the SHARE system from turning into the mother of all pseudoclassifications? The strength of our open society is the free flow of information but the SHARE concept looks more like the Soviet GOSPLAN.

We could spend billions of dollars implementing the computer networks necessary for SHARE, or we could invest a few million in real openness and government accountability. President Bush nominated members for the Public Interest Declassification Board but did not include the Board's $600,000 allowance in his budget. We could establish **an independent review board with a small staff like ISOO at every major federal agency for a million dollars each per year**, less than the cost of our excellent military marching bands.

The number one lesson of 9/11 is that the "relevant players" include the public, front and center. As the staff director of the Congressional Joint Inquiry on 9/11 found, *"The record suggests that, prior to September 11th, the U.S. intelligence and law enforcement communities were fighting a war against terrorism largely without the benefit of what some would call their most potent weapon in that effort:* ***an alert and informed American public.*** *One need look no further for proof of the latter point than the heroics of the passengers on Flight 93 or the quick action of the flight attendant who identified shoe bomber Richard Reid."* After all, the only part of our national security apparatus that actually prevented casualties on 9/11 was the citizenry – those brave passengers on Flight 93 who figured out what was going on before the Pentagon or the CIA did, and brought their plane down before it could take out the White House or the Capitol.

Look at the case of the Unabomber, the Harvard-educated terrorist who blew up random scientists with letter bombs. Years of secret investigation turned up nothing but rambling screeds against modernity and the machine, and only after the madman threatened more violence unless his words were published, did the FBI relent and give the **crank letter file to the newspapers**. The *Washington Post* and the *New York Times* went in together on a special section to carry the 35,000 words in 1995, but the key paper was the *Chicago Tribune*, read at the breakfast table in a Chicago suburb by the bomber's brother, who said, sounds like crazy Ted, guess I'd better call the cops.

How did we catch the Washington sniper? The police had been chasing a white van for weeks with no luck, and finally changed the description to a blue sedan based on an

eyewitness report. They refused to give out the license plate number (because the sniper would then change the plates, of course); but finally an unnamed police official took it upon herself to leak the license number at midnight, local radio and TV picked it up, and a trucker was listening who saw a blue sedan in a rest area in western Maryland. He checked the plate number, and bingo, **within three hours of the leak they arrested the sniper**. Openness empowers citizens.

The entire 9/11 Commission report includes only one finding that the attacks might have been prevented. This occurs on page 247 and is repeated on page 276 with the footnote on page 541, quoting the interrogation of the hijackers' paymaster, Ramzi Binalshibh. Binalshibh commented that if the organizers, particularly Khalid Sheikh Mohammed, had known that the so-called 20th hijacker, Zacarias Moussaoui, had been arrested at his Minnesota flight school (he only wanted to fly, not to take off or land) on immigration charges, then Bin Ladin and KSM would have called off the 9/11 attacks. And wisely so, because news of that arrest would have alerted the FBI agent in Phoenix who warned of Islamic militants in flight schools in a July 2001 memo that vanished into the FBI's vaults in Washington. The Commission's wording is important here: **only "publicity" could have derailed the attacks.**

This is why Ms. Carol Haave, the deputy undersecretary of defense, framed the problem wrongly at your August 24 hearing. She testified, *"In the end, this is a discussion about risk. How much risk is the nation willing to endure in the quest to **balance protection against the public's desire to know?** It's a complex question that requires thought and ultimately action."* She and the Pentagon have missed the point. We are not balancing protection against the public's desire to know. The tension is actually between bureaucratic imperatives of information control versus empowering the public and thus making us more safe. Yes, there are real secrets that must be protected, but the lesson of 9/11 is that we are losing protection by too much secrecy. The risk is that by keeping information secret, we make ourselves vulnerable. The risk is that when we keep our vulnerabilities secret, we avoid fixing them. In an open society, it is only by exposure that problems get fixed. In a distributed information networked world, secrecy creates risk – risk of inefficiency, ignorance, inaction, as in 9/11. As the saying goes in the computer security world, **when the bug is secret, then only the vendor and the hacker know – and the larger community can neither protect itself nor offer fixes**. Publicity is not a SHARE network limited to relevant players. Publicity is TV, the newspapers, the Internet, and the highly efficient information distribution system that is our open society. That is our strength, not our weakness.

So how do we put countervailing pressure on the secrecy system, and on the new SBU systems, to force publicity, to empower the public? We can start the way the framers did, with checks and balances. **If you create a power center for creating and holding secrets, like the new intelligence czar, then you need a counter center for declassifying secrets**. The Moynihan commission, for example, recommended setting up a formal Declassification Center based at the National Archives and staffed by an interagency group with delegated powers from their agencies. Their performance would be measured by their openness. Just such a group served the Congress well during the

Iran-contra investigations by reviewing and declassifying more than 30 thick volumes of testimony and documents in record time, with enormous benefits for government accountability and without damage to national security.

Another model is the Public Interest Declassification Board authorized in the intelligence reform bill last year. Not all the members have yet been named, so the jury is still out on whether this Board will meet the expectations of Senators Lott and Wyden, for example. But **every previous experience with a statutory independent review board has been a major success**, pushing out of the system the secrets that do not need keeping. These include the Assassination Records Review Board, the State Department's historical advisory committee, and the Interagency Working Group on Nazi and Japanese War Crimes. Every agency needs a review board like these, with authority in statute, with scholars and former officials doing the oversight, with regular reporting requirements and open meetings. The model we should not follow is that of the CIA, where the advisory committee has no statute behind it and, by allowing its recommendations to remain confidential, has voluntarily given up what little leverage it might have had.

One of William Leonard's recommendations is that the new secrecy systems have to be coordinated with the old ones. He makes the valid point that it would be a major reform and **potential restraint to have a common set of standards** across all agencies in place of the differentiated, culture-driven, idiosyncratic standards that have arisen in the multiple secrecy regimes. Such differences create huge uncertainties among officials about what behavior is expected and how much information to share.

Even part of the CIA agrees with this critique. For example, a 1977 study by the CIA of its own codeword compartments (declassified in 2002) found that the proliferation of compartments had deleterious psychological effects that "seem to diminish rather than enhance security," and recommended that the DCI abolish all existing compartments and replace them with one uniform Sources-and-Methods compartment. The intelligence community is moving in this direction (witness the 1999 abolition of the COMINT codewords UMBRA, SPOKE, MORAY and the TALENT-KEYHOLE codeword ZARF); but bureaucratic inertia and turf-consciousness pose major obstacles to the rational consolidation of SBU and secrecy rules today. Yet, the secrecy skeptic in me thinks that perhaps **centralization is not the cure-all**, that perhaps the diversity of our bureaucracy is actually a protection for dissenting views, for multiple perspectives, and for alternative policy options.

More important than centralization, **we must build into all of our secrecy systems multiple provisions for cost-benefit analysis, audits, oversight offices, cost accounting, and independent reviews**. We must limit the number of officials who have the power to wield the secret or SBU stamp. We must increase the number of officials whose jobs and careers depend on opening information. We must **change the internal bureaucratic incentives**, by tying promotions and raises to declassification and information sharing, while providing real penalties for knee-jerk secrecy and information hoarding.

There are interesting examples of carrot-and-stick provisions on government openness both abroad and at home. We could look to Sweden, for example, where the bishop of Stockholm, a public official, had to pay a fine (nearly $2,000) last year for violating the open records law, by withholding letters from priests in the state-supported church about their problems and challenges. Or we could look to Florida, where an Escambia County school board member went to jail for a week in 2003 for refusing to provide a public record to a Pensacola mother. The name of that school board member is now a household word among officials in Florida, deterring bad behavior. It's a more difficult question, but one we must address, about how to deter absurd classification decisions like the CIA's claim (now upheld by a federal court) that it can declassify the 1997 intelligence budget figure with no damage to national security, but the 1947 number still must be secret (Steven Aftergood testified in detail about this case at the August 24, 2004 hearing). Secrecy decisions like this one actually undermine the credibility of the entire information security system and make our real secrets less safe.

In the final analysis, of course, it is openness that empowers our citizens, weeds out the worst policy proposals, ensures the most efficient flow of information to all levels of law enforcement, makes a little more honest the despots who are our temporary allies against terrorism, and keeps our means more consistent with our ends.

Thank you, Mr. Chairman, and I look forward to any questions you may have.

Mr. SHAYS. Thank you very much.

Mr. Hammitt.

STATEMENT OF HARRY A. HAMMITT

Mr. HAMMITT. Thank you.

As I have listened to the other witnesses, I thought to myself, how much more can I say, and I said what I wanted to say in my written testimony. So I thought I would highlight one aspect that I don't think has been addressed here today, that isn't in my testimony but I hope to elucidate a little bit more.

Mr. SHAYS. And highlight anything you may disagree with.

Mr. HAMMITT. Verbally.

Mr. SHAYS. Anything in the statements earlier that you disagree with, please feel free.

Mr. HAMMITT. OK. What I wanted to do was quickly tell the story of how we got to where we are today in terms of critical infrastructure information as part of the Homeland Security Act. I think that because of what happened to us on September 11th, we frequently see most of this through the lens of threats to terrorism.

But the interesting thing about this, and I think it's kind of an interesting object lesson here, is that the critical infrastructure information exemption was created largely in response to a program that the EPA announced that it was going to put worst case scenario reports on the Internet for people. These worst case scenario reports are reports that facilities that store chemicals or manufacture chemicals or various other hazardous substances are supposed to file, talking about what would happen if there was an explosion, say, at their facility and how many people this might impact and how the community might be evacuated, what the safety precautions are, those sorts of things.

The EPA had concluded that under the Clean Air Act, it was required to make this as widely public as possible. When the chemical industry got wind of this, they enlisted the help of the FBI to argue before Congress that to disclose this information as widely as the EPA intended to do would be a potential boon for terrorists. This was 1999, I believe, so several years before the September 11th attacks.

Congress looked at the issue at that time and basically decided to study the issue. They told EPA not to put the information on the Internet at that time. At the same time, Congress was also looking at a piece of legislation to try to resolve a pressing issue which was commonly known as Y2K. In this issue, people were worried that computer software might not be able to understand when the calendar moved from 1999 to 2000 and there might be all sorts of deleterious problems caused by that.

In order to get industry to talk about this issue to the Government, Congress passed Y2K legislation which allowed industry to disclose some of this information to relevant Government authorities, but be protected, because the disclosure would not be made public and they would also be protected from liability. When Congress turned to the critical infrastructure information type of exemption, they looked at this Y2K exemption as a possible starting point. Indeed, this is basically the embodiment of this policy that's in the Homeland Security Act.

So I guess what I wanted to say about this is, we have an exemption where voluntarily submitted critical information about vulnerabilities in the private sector is given to the Department of Homeland Security, and as an observer, my guess is that the Department of Homeland Security needs this information so they can protect us domestically from possible threats.

Well, the problem is we have created a voluntary program in which we have essentially said, we won't tell anybody of the existence of this threat if you will voluntarily provide the information. As I said in my written testimony, I ran across an article recently in a publication called Security Focus that indicated, generally speaking, the industry hasn't been willing to give up this information. They are more worried about what would happen to the information if the Government had hold of it than they are than if the public had hold of it.

So I guess my point is this, that if the Government feels, and if as a policy the Government feels it needs this information to do its duty, my personal opinion is that the Government needs to require the industry to disclose this information to them, not say, please give me this information and in return I won't let anybody else know anything about it. I think at the end of the day, it seems to me that if we do not know about this sort of information, these vulnerabilities, we are basically fooling ourselves, we're lulling ourselves into a sense of false security that these situations don't exist. I think we're actually doing ourselves more harm than good.

I thought that Tom Blanton's recommendations for putting some of these offices like ISOO into individual agencies were extremely good. I guess part of my recommendation really is, I don't believe any of these programs are going to go away unless Congress makes them go away. So I think that at least at the very minimum you all need to think seriously about how to restrict the use of these programs within the agencies that are already using them now. When I talk about these programs, I'm talking about these programs of things like sensitive but unclassified and what-not.

[The prepared statement of Mr. Hammitt follows:]

Testimony of
Harry Hammitt
Editor/Publisher, Access Reports
House Subcommittee on National Security, Emerging Threats and International Relations
March 2, 2005

My name is Harry Hammitt. I am the editor/publisher of *Access Reports*, a biweekly newsletter on the Freedom of Information Act, open government issues, and informational privacy issues. I have attached a copy of the newsletter relevant to the topic of this hearing. I have been editing *Access Reports* for almost 20 years. During that time I have become the expert's expert on the Freedom of Information Act. I am the primary editor of *Litigation Under the Federal Open Government Laws*, considered the best source on the subject for requesters and plaintiffs. I have been a contributing editor to *Government Technology*. I am a former president of the American Society of Access Professionals, a Washington-based professional association of people who work with FOIA and privacy issues, and a current board member of the organization. I have taught FOIA training sessions for ASAP and various other public interest organizations and have spoken on these issues in various forums in the U.S. and internationally. Before becoming editor of the newsletter, I worked at the Consumer Product Safety Commission processing FOIA requests, and at FOI Services, a company that makes requests on behalf of business clients. I have both a master's degree in journalism from the University of Missouri-Columbia, and a law degree from George Washington University Law School. I think the combination has served me well in understanding and writing about information access issues.

I want to thank the subcommittee for inviting me to testify on this important and timely information issue. I hope to provide an overview of some of the programs that have developed, indicate where they came from and how and why they developed, and then close with my assessment of how these programs impact information policy.

In my judgment, these programs cause more harm than good. They are:

- too ill-defined and broad, and, as a result, are subject to abuse and substantial over-use;

- a solution to a problem that may not exist and based on the dubious proposition that secrecy will make us more safe rather than less safe and that agencies and companies will not use secrecy to hide their own mistakes and avoid public scrutiny;

Historical Perspective

The existence of such undefined categories of restricted information has accelerated during the Bush administration. But all these categories did not somehow appear fully formed after September 11, 2001. Several have existed for years. The term "sensitive, but unclassified" goes back at least to the Reagan administration, and has a statutory basis in the Computer Security Act of 1987. The concept of critical infrastructure information appeared during the Clinton administration and its protection today is modeled on legislation concerning the Y2K problem that Congress passed in 2000. Such terms as "sensitive security information," "sensitive homeland security information," and "critical energy infrastructure information" are more recent additions to the information lexicon. What all these categories have in common is their ill-defined nature.

The Card Memo

In March 2002, White House Chief of Staff Andrew Card sent a memo[1] to all agencies concerning the need to safeguard sensitive but unclassified information pertaining to homeland security. Because such undefined information did not qualify for classification on national security grounds, Card attached two short memos from Laura Kimberly, Acting Director of the Information Security Oversight Office,[2] and Richard Huff and Daniel Metcalfe, Co-Directors of the Justice Department's Office of Information and Privacy,[3] explaining possible FOIA exemptions that could be used to

[1] Andrew H. Card, Jr., Assistant to the President and Chief of Staff, Memorandum for the Heads of Executive Departments and Agencies; Subject: Action to Safeguard Information Regarding Weapons of Mass Destruction and Other Sensitive Documents Related to Homeland Security (Mar. 19, 2002).
[2] Laura S. Kimberly, Acting Director of the Information Security Oversight Office, Memorandum for Departments and Agencies (Mar. 19, 2002).
[3] Richard Huff and Daniel Metcalfe, Co-Directors, Office of Information and Privacy, Department of Justice, Memorandum for Departments and Agencies (Mar. 19, 2002)

withhold such information. Primary among them was Exemption 2,[4] which allows an agency to withhold records "related solely to the internal personnel rules and practices of an agency." Over the years, courts have stretched these words so they now allow an agency to withhold records where disclosure could lead to circumvention of a law or regulation. The Justice Department memo reminded agencies to consider using Exemption 2 for such sensitive but unclassified information on the untried theory that disclosure would allow a requester to circumvent a law or regulation. Although it said little about the scope of the problem, the Card memo was the first White House policy directive concerning the need to protect sensitive unclassified information and was certainly a primary factor in moving the development of such policies forward.

Sensitive Security Information

Sensitive security information is one of the few such categories with a statutory basis. In November 2001, Congress passed the Aviation and Transportation Security Act, creating the Transportation Security Administration. That statute defines sensitive security information as information describing air carrier screening procedures, airport or air carrier security programs, maritime transportation security procedures, or other related transportation security matters. It prohibits the disclosure of such information if the TSA Administrator determines disclosure would "be detrimental to the safety of passengers in transportation."[5] The Homeland Security Act of 2002 expanded this to cover information that "would be detrimental to the security of transportation." A May 2004 *Federal Register* notice set out 16 categories of information from traditional security plans to security directives and included "other information" that TSA at its discretion determined should be withheld. This statutory authority is structured so that it qualifies as an Exemption 3[6] statute under FOIA. Exemption 3 is a catch-all provision in FOIA that allows agencies to withhold records whose disclosure is prohibited or restricted by a provision in another statute as long as that statute either provides no discretion on the part of the agency or identifies specific categories of information to be withheld.

---

[4] 5 U.S.C. 552(b)(2).
[5] 49 U.S.C. 114(s)(1) and 49 U.S.C. 40119(b)(1).
[6] 5 U.S.C. 552(b)(3).

These sensitive security information provisions have been involved in several incidents that received national press coverage, including the refusal of TSA staff to allow former Rep. Helen Chenoweth-Hage to board a flight because she refused to submit to a pat-down search and asked for the legal authority to conduct such a search, a request that was denied. Other high-profile incidents involve a lawsuit by activist John Gilmore, after TSA again refused to disclose its authority for demanding personal identification before boarding a flight, and a lawsuit filed by the ACLU of Northern California on behalf of several people who were told they were on the "No Fly List," but were denied any information concerning why they were put on such a list. The judge hearing that lawsuit has told TSA that it "has not come close to meeting its burden [to justify withholding], and, in some instances, has made frivolous claims of exemptions. General statements that, for example, the information is sensitive security information are inadequate to satisfy the government's burden."[7]

Critical Infrastructure Information

The debate over critical infrastructure information predates the terrorist attacks of September 11, 2001. In 1999, Congress held several hearings and legislation was introduced after the EPA announced that it intended, as part of its public disclosure obligations under amendments to the Clean Air Act, to post on the Internet what are known as worst-case scenario reports – assessments of potential environmental damage that could occur if a catastrophic event took place at a manufacturing facility that stored chemicals or other hazardous materials. Such reports were required to help facilitate emergency response planning and to allow people to assess the risks such facilities posed for the community. After the EPA announced that it would make these reports available on the Internet, the chemical manufacturing industry protested and was able to convince the FBI that such widespread dissemination would allow terrorists to assess the vulnerabilities of such plants and maximize the potential damage from an attack. As a result of the hearings, Congress commissioned a two-year study of the problem. However, there is no apparent evidence that such a study ever actually took place and today worst-case scenarios are available in hard copy at various locations in the pertinent

[7] Access Reports, "Trend Towards Secrecy Continues to Grow," Dec. 15, 2004, v. 30, n. 24, p. 1.

communities, but are not available to a wider audience and are not available at all in electronic form.

The worst-case scenarios controversy dovetailed with a related concern then being brought up in Congress – the possibility that computers would fail to properly recognize the date change when the calendar moved from 1999 to 2000, potentially causing massive equipment failures. An important part of assessing the potential for such trouble was to encourage the private sector to share its concerns about vulnerabilities with the government. To encourage such information-sharing, Congress passed Y2K legislation that prohibited disclosure of any such voluntarily-submitted information under FOIA and also excused the private sector from any potential liability if their products did fail as a result of the date change.

The issue of protecting critical infrastructure information more generally was still being discussed when the Bush administration took office and some form of legislation might well have been passed in the next year or two. But the attacks of September 11, 2001 tied the issue more closely to terrorism. Instead of being an issue about protecting confidential business information, it was now rolled into the push to protect the nation from future terrorist attacks. As part of the Homeland Security Act of 2002, the House of Representatives passed a provision allowing the Department of Homeland Security to protect voluntarily-submitted critical infrastructure information. In the Senate, public interest groups helped craft a provision that, while allowing such voluntary submissions, would allow outside challenges, based on the D.C. Circuit's decision in *Critical Mass v. NRC*,[8] as to whether or not specific submissions did indeed qualify as critical infrastructure information. The amendment, offered by Sen. Robert Bennett (R-UT) and Sen. Patrick Leahy (D-VT), was adopted by the Senate but was dropped in conference, leaving the House provision as the final version.

The Department of Homeland Security issued proposed regulations concerning the voluntary submission of critical infrastructure information in 2004, although the regulations are not yet final. At least one controversial suggestion in the regulations was that critical infrastructure information could be submitted to other agencies and could then be passed along to Homeland Security. The statutory language appears to

[8] *Critical Mass Energy Project v. NRC*, 975 F.2d 871 (D.C. Cir. 1992).

contemplate that such submissions can only be made to the Department of Homeland Security and public interest groups were concerned that allowing other agencies to collect the submissions expanded the provision's reach.

A recent article in *SecurityFocus*[9] looks at how the submission process has worked so far and notes that at least the information technology industry is still wary of the program and has yet to submit any information. Although the information is protected from public disclosure, industries are more concerned about its potential wide dissemination within government. Sean Moulton, a policy analyst at the public interest group OMB Watch, explained to *SecurityFocus* the concerns of the public interest community. He indicated that industry had been given more protection than public interest groups thought was warranted, yet industry was still uncomfortable submitting such information. He pointed out that "I really find it troubling that it's industry driving the process and not the government driving the process, when it's the public who has a stake in this. It's the public who will be harmed if these infrastructures are attacked."[10]

Critical Energy Infrastructure Information

The Federal Energy Regulatory Commission has created its own category of sensitive information, known as critical energy infrastructure information, and has faced its own specific problems which it has had to finesse. The Commission oversees the energy industry and holds a number of administrative proceedings involving companies and utilities in that area. As a part of these hearings, the Commission requires submission of technical information, including infrastructure information. Generally, most of this information would be public when used in a proceeding. However, after September 11, 2001, FERC moved more aggressively than virtually any other agency to remove critical energy infrastructure information from the public domain. The agency's regulations define CEII as information that is exempt from FOIA and submitted to the agency by private parties about proposed or existing critical infrastructure that relates to

[9] Poulsen, Kevin. "U.S. Info-Sharing Initiative Called a Flop, *SecurityFocus*, Feb. 11, 2005.
[10] Ibid.

the production, generation, transportation, transmission or distribution of energy and which "could be useful to a person planning an attack on critical infrastructure."[11]

The most glaring problem with FERC's policy is that it is based on the assumption that this information is exempt from disclosure under FOIA. However, FERC's claims are based not on any court-accepted interpretation of FOIA, but on the Justice Department's suggested potpourri of possible exemptions. These include Exemption 2, which protects information the disclosure of which could allow someone to circumvent a law or regulation, Exemption 7(E), which allows a law enforcement agency to withhold information that would reveal investigative methods and techniques, and Exemption 7(F), which allows a law enforcement agency to withhold information the disclosure of which could endanger the physical safety of an individual. The agency also suggested that the information could be withheld under Exemption 4, which protects confidential business information, because a terrorist attack would clearly cause a company economic harm. The other problem is that FERC wanted to continue to share this information during its proceedings, requiring it to create a non-FOIA process of disclosure to those parties with a "need to know," which required parties to sign a non-disclosure agreement. It is difficult to see how information that was previously public could become non-public based solely on agency regulations.

The Impact on Disclosure of Such Categories of Information

These ill-defined categories – be they "sensitive but unclassified," "sensitive security information," or some form of "critical infrastructure information" – almost always do more harm than good. They are a solution to a problem that may not even exist and are based on what I consider to be an antithetical proposition in our democracy – that, when in doubt, always favor secrecy over openness. That is not to say that some government information should not remain secret; we can all agree that some information, such as troop movements in time of war, for instance, should be kept secret. But when our government fosters the attitude that there are vast undefined categories of information that must be, at a minimum, safeguarded by agencies, it does a grave disservice to the

[11] 18 C.F.R. § 388.113(c) (68 Fed. Reg. 9857, 9870 (March 3, 2003)).

ideal of an open democratic society. It is paternalistic for government to assume that people cannot handle the availability of such information.

Government officials say these designations, like "sensitive but unclassified," or "for your eyes only," have no legal status and cannot be used to deny access under FOIA. While this is true on a technical level, it is hard to believe that when agency personnel are faced with a document with such a designation they are not going to think twice before agreeing to disclose such a document. In other words, such a designation sets off red flags that suggest the record merits withholding. The problem with the Justice Department's memo attached to the Card memo is that it outlines a strategy for withholding information that perhaps should have been released. When a record says "sensitive, but unclassified," the first step for agency personnel is likely to try to figure out which FOIA exemption can be applied.

For years, most outside observers have complained that too much information is classified. The annual reports of the Information Security Oversight Office consistently show that the number of classification determinations, whether at the original or derivative level, continue to go up every year. But the national security classification scheme provides several potential remedies for forcing the disclosure of classified information. These include a mandatory declassification review, most often in conjunction with an FOIA request, or a review by the Interagency Security Classification Appeals Panel (ISCAP). Review by ISCAP, created by Executive Order 12958 issued by President Clinton, has resulted in further disclosure of previously classified information in a significant majority of cases. However, the number of cases heard by the panel is relatively small and resort to it is not a practical option for many requesters.

When it comes to the undefined categories of information that are the subject of today's hearing there are no remedies short of litigation, probably under FOIA. While the government's collection of recommended exemptions has not been thoroughly tested, at least two U.S. district court judges have accepted some combination of these claims.[12] Further, the expanded deference shown by the D.C. Circuit in litigation[13] over disclosure of the identities of individuals who were detained in the immediate aftermath of

---

[12] See *Living Rivers, Inc. v. Bureau of Reclamation*, No. 2:02-CV-644TC (D. Utah, Mar. 25, 2003) and *Coastal Delivery Corp. v. Customs Service*, No. 02-3838 WMB (C.D. Cal., Mar. 14, 2003).
[13] *Center for National Security Studies v. DOJ*, 331 F.3d 918 (D.C. Cir. 2003).

September 11, 2001, suggests that courts would likely be sympathetic to the government's arguments when it came to withholding information based on concerns about possible terrorist use. There is no administrative appeal aside from that available under FOIA. This means, realistically, that there are fewer checks against the improper denial of such undefined categories of information than exist for classified national security information.

When such real or imagined restrictions are placed on information, there are consequences for internal dissemination as well, a problem that particularly concerned the 9/11 Commission. The national security classification system has designations for "Top Secret," "Secret," and "Confidential" information. Not only must such designations be made only by individuals who have the delegated authority to do so, once classified that information may only circulate with specific limitations. To see a record classified as "Top Secret," an individual must have a top secret classification clearance. Those whose clearances are no higher than "Secret" or "Confidential" are not supposed to use information classified at a "Top Secret" level. And individuals who have no security clearance aren't supposed to have access to any classified information.

The same kinds of restrictions likely exist in practice for records labeled "sensitive, but unclassified" or "sensitive security information" or any of the other undefined categories under discussion here. Once these kinds of restrictions are put into place, they impose severe limitations on dissemination which may rob them of much of their value in the first place. While such limitations within the federal government can be disruptive enough, further dissemination to state and local officials, who in most instances are likely to have no clearance at all, may be that much more restricted. If information is to be useful, it must be available.

The wisdom of these programs is suspect at best, but once in place it is difficult to completely do away with them. There are, however, several options that might at least make them more tolerable. Using the national security classification system as a model, the definition of what constitutes sensitive information could be spelled out much more specifically and dissemination could be based on categories, with dissemination of the most sensitive information being more restricted than for information of a less sensitive nature. A standard definition of sensitive information could be crafted and its use could

be limited so that only agencies that would legitimately be expected to have such information would be able to categorize records as sensitive. Some degree of flexibility in defining subcategories, such as critical energy infrastructure information, could be given to those agencies whose information fits into that specific category. Regardless, any restrictions on such subcategories could be no broader than allowed under the overall definition of what constitutes sensitive information. Agencies using any of these categories should be required to implement standards designed to maximize public access to such information to ensure that the concept of sensitive information is not used as a broad brush to withhold or restrict information more generally.

Further, remedies to challenge the designation of such information must be made available. Requesters must not be forced to go to court as their only alternative. Instead, a process akin to mandatory declassification review should be instituted. Along these same lines, time limits for protection should be considered and implemented. Sensitive information may well be sensitive for a period of time and lose its sensitivity thereafter. Once information is no longer sensitive it should be made publicly available.

The obsession with protecting such information because under some scenario it might be of use to a terrorist, fails to consider the value of the information itself. Vulnerabilities in our infrastructure should not be broadcast to potential enemies, but should not be hidden under a basket either. A good analogy for fostering greater public disclosure is how open source software code works in the computer world. When such code is openly available, individuals tinker with it in an effort to improve it or to expand its utility. When such programs are closed, they stagnate rather than expand. Bridges or roads or manufacturing facilities that are vulnerable will not be fixed because their vulnerabilities are hidden. They are much more likely to be fixed, and thus become less useful as an end goal for terrorists, because individuals and groups put pressure on government or business to fix them. We need to be less fixated on the potential harmful use of information and more cognizant of the way in which we can use that information to achieve a result that makes us both safer from potential attack and safer because vulnerabilities have been addressed. As a nation we cannot very well address vulnerabilities when we do not know they exist.

These undefined categories of information stifle the availability and use of information. They expand the universe of information agencies are likely to withhold from the public solely because of their designation. They also restrict the availability of information within government and particularly between levels of government. One of the lessons of the 9/11 Commission's report is that information is most useful when it is available. Various bureaucratic gate-keeping regimes that slow or halt the flow of information, or worse still, hide its existence, are detrimental to our available knowledge base and, ultimately, do us more harm than good.

Thank you for allowing me the opportunity to share my view with the subcommittee. If I can answer any questions or provide more information, I will be glad to do so.

Volume 30, Number 24
December 15, 2004

ACCESS REPORTS
FREEDOM OF INFORMATION

A Journal of News & Developments, Opinion & Analysis

In this Issue

Trend Towards Secrecy Continues to Grow 1

Views From the States 3

The Federal Courts 5

Editor/Publisher:
Harry A. Hammitt
Access Reports is a biweekly newsletter published 24 times a year.
Subscription price is $350 per year.
Copyright by Access Reports, Inc
1624 Dogwood Lane
Lynchburg, VA 24503
434.384.5334
FAX 434.384.8272
email: hhammitt@accessreports.com
website: www.accessreports.com

No portion of this publication may be reproduced without permission.
ISSN 0364-7625.

Washington Focus: Sen. John Cornyn (R-TX) has indicated that he will offer FOIA amendments next session. Cornyn, who as Texas Attorney General oversaw administration of the Texas Public Information Act, wants to improve FOIA by adding features based on the Texas law. Issues he plans to look at include tightening time limits for a response and providing real consequences for an agency that misses its deadlines; providing some kind of impartial administrative review of denials; and making the litigation process more practical for requesters, in part by assuring that plaintiffs have some prospect of a fee award if they force the agency to disclose information. . . Not satisfied with the outcome of its earlier legislation prohibiting the Bureau of Alcohol, Tobacco and Firearms from expending any funds in responding to an FOIA request from Chicago concerning gun sale data, Congress has now passed new legislation making the agency "immune from legal process." The Seventh Circuit ruled in response to the earlier funding prohibition that the agency would still be required to process the request because Chicago had committed to pay all the fees. That decision sent the agency scurrying back to Congress for more specific language. The agency has now asked the Seventh Circuit to reconsider its decision in light of the new legislation.

Trend Towards Secrecy Continues to Grow

Over the past few months there have been increasing signs that government is moving further in the direction of secrecy, usually tying the need for increased secrecy to security concerns. Some developments include an incident in Idaho where a former member of Congress was not allowed to board a flight after she protested the authority of Transportation Security Administration security guards to conduct a further pat-down and was told she had no right to see a copy of the regulation providing such authority, the introduction of a non-disclosure agreement at the Department of Homeland Security restricting employees from disclosing sensitive but unclassified information, the refusal of the Bureau of Reclamation to share information concerning the safety of Jackson Lake Dam with county officials, and the beginning of an OPM policy that may well prohibit disclosure of all or most information on federal employees.

ACCESS REPORTS

Writing in the online magazine *Slate*, Steve Aftergood, who runs the Project on Secrecy for the Federation of American Scientists, noted that former Rep. Helen Chenoweth-Hage had been the victim of the pat-down search and that her refusal led to her driving to her destination rather than flying. Local TSA Security Director Julian Gonzales told the *Idaho Statesman* that "she said she wanted to see the regulation that required the additional procedure for secondary screening and she was told she couldn't see it." When asked why, Gonzales responded: "Because we don't have to." He explained that "that is called 'sensitive security information.' She's not allowed to see it, nor is anyone else." Aftergood pointed out that "sensitive security information" in this context originated in the 1974 Air Transportation Safety Act and was intended to protect airport and airline security programs. It was greatly expanded by a provision in the Homeland Security Act of 2002, which increased its scope to information that "would be detrimental to the security of transportation." A May 2004 Federal Register notice set out 16 categories of information from the traditional security plans to security directives of the type used in Chenoweth-Hage's case. A final category also included "other information" that TSA at its discretion determined should be withheld. Congressional Research Service analyst Todd Tatelman wrote in a recent report that "by removing any reference to persons or passengers, Congress has significantly broadened the scope of the SSI authority. As a result, it appears that the authority to classify information as SSI now encompasses all transportation-related activities, including air and maritime cargo, trucking and freight transport, and pipelines." Several other incidents in California have led to litigation. Software designer John Gilmore was not allowed to board a flight in 2002 because he refused to provide a picture ID. He has since sued, but the government contends the case cannot be heard in open court. In his suit Gilmore claims that he was told that "security directives mandated the showing of ID, but that he couldn't see them." The directives apparently "are revised as often as weekly, and are transmitted orally rather than in writing. To make things even more confusing, these orally transmitted secret rules change depending on the airport." In another suit brought by the ACLU of Northern California over the so-called "No Fly List," the court has indicated the TSA "has not come close to meeting its burden [to justify withholding], and, in some instances, has made frivolous claims of exemptions. General statements that, for example, the information is sensitive security information are inadequate to satisfy the government's burden."

Aftergood was also instrumental in bringing the DHS secrecy pledge to light. The agreement, which binds employees from disclosing sensitive security information, contains administrative, disciplinary, criminal and civil penalties. Aftergood noted that "its likely consequence will be to chill even the most mundane interactions between department employees and reporters or the general public. Employees will naturally fear that even the most trivial conversation could mean a violation of this draconian agreement, and so the result will be a new wall between the government and the public." Aftergood later reported that both the National Treasury Employees Union and the American Federation of Government Employees have challenged the legality of the agreement. In a joint analysis, the two unions noted that "the possibilities for abuse inherent in a regime that authorizes unlimited searches and provides supervisors unbridled discretion to censor employee speech by simply stamping documents 'for official use only' are obvious." In an editorial addressing both the secrecy agreement and the TSA's security directives, the *Washington Post* observed that "the department needs to remember that the homeland whose security it is protecting is one in which democratic debate is supposed to be open and freewheeling."

In Teton County, Wyoming, the Bureau of Reclamation refused to provide technical reports concerning the safety of Jackson Lake Dam. The agency provided what it called a "nonsensitive" version of an engineering report, but that still did not completely address the concerns of Commissioner Bill Paddleford. Paddleford had heard a lecture by a professor of seismology at the University of California at Santa Barbara who mentioned that an earthquake could cause part of the dam to liquefy. The Bureau assured Paddleford and the county that there was no significant danger posed by the dam and took the unusual step of posting online part of the engineering report. Noting that agencies were increasingly withholding sensitive security information, Patrice McDermott of the American Library Association told the Associated Press that agencies

ACCESS REPORTS December 15, 2004 Page 3

had "taken the leap from safeguarding information to withholding it. Agencies will err on the side of caution to cover their ass, and we're seeing a rising tide of agencies doing this."

Of even greater concern to the cause of access generally is a possible change in OPM's policy on disclosure of information about federal employees. In an interim response to an FOIA request from Syracuse University Professor Susan Long, co-director of TRAC, the agency referred to her request for an electronic copy of the "March 2004 Status file from the Central Personnel Data File," a file identical to ones TRAC had previously gotten from the agency. The letter went on to say that OPM "is currently conducting a review of the policy of disclosure of individual employee records as this relates to the Freedom of Information Act and the Privacy Act." Although the letter says nothing more, it is clear that OPM is thinking about changing its policy to something other than its previous position, which apparently was full, or nearly full, disclosure. Since the *Reporters Committee* decision 15 years ago, the government has become increasingly more inhospitable to the idea of releasing personal information on federal employees, even run-of-the-mill directory information. In the current climate where access decisions are frequently seen through the lens of terrorism, it does not take much imagination to foresee a new policy withholding such information solely on terrorism grounds, perhaps blended with privacy concerns. If OPM were to take that step, it would be a major move in the direction of anonymous government.

It is possible that years from now we will look back at this period and wonder why we could have overreacted so quickly to potential threats that were largely based on speculation. Unfortunately, we are living in the present and today there appears to be little concern that we are going too far too fast.

Views from the States...

The following is a summary of recent developments in state open government litigation and information policy.

California

The supreme court has ruled that Discovery Communications did not invade Steve Gates' privacy when it used public record information about Gates' 1992 conviction in a documentary aired in 2001. Gates pleaded guilty to being an accessory after the fact to a murder for hire in 1988. An automobile salesman was murdered and a prominent automobile dealer was later convicted of masterminding the murder to deter a class action suit the salesman had brought against a dealership owned by the dealer's parents. Gates was the dealer's assistant manager at the time and was charged as a co-conspirator, although the charges were later reduced. Discovery produced a 2001 documentary about the crime and Gates sued for defamation and invasion of privacy, claiming that he had led an obscure life since his conviction and the documentary had inappropriately dredged up his past. Gates' invasion of privacy claim relied heavily on *Briscoe v. Reader's Digest Association, Inc.*, 4 Cal. 3d 529 (1971), in which the supreme court had held that an invasion of privacy could occur through the injurious publication of true, but not newsworthy, information concerning the criminal past of a rehabilitated convict. But Discovery argued *Briscoe* had been overturned by subsequent U.S. Supreme Court rulings, particularly *Cox Broadcasting v. Cohn*, 420 U.S. 469 (1975), in which the Court found that Georgia could not punish a television station for revealing the name of a 17-year-old rape victim whose name had been obtained by examining public court records. After reviewing *Cox* and a handful of later cases, the court observed that "we, like the high court are 'reluctant to embark on a course that would make public records generally available to the media but forbid their publication if offensive to the sensibilities of the supposed reasonable man. Such a rule would make it very difficult for the media to inform citizens about the

public business and yet stay within the law. The rule would invite timidity and self-censorship and very likely lead to the suppression of many items that would otherwise be published and that should be made available to the public.'" (*Steve Gates v. Discovery Communications,Inc.*, No. S115008, California Supreme Court, Dec. 6)

Florida

A court of appeals has ruled that a county property appraiser cannot require commercial users of public records from his office to sign a licensing agreement. Microdecisions, Inc., which compiles and sells data concerning real estate in south Florida, requested copies of GIS maps created by the Collier County Property Appraiser. Appraiser Abe Skinner contended the maps were copyrighted and that Microdecisions could not have unrestricted use of the maps unless it signed a licensing agreement requiring a royalty payment if the maps were used commercially. Skinner first argued that the case was moot because he was not withholding the maps from Microdecisions. The court rejected the claim, noting that the use restriction provided grounds for claiming a violation of the Public Records Act. The court agreed that Skinner had the right to claim copyright in the map, but indicated that the Public Records Act overrode Skinner's copyright unless the legislature had specifically provided an exemption for such copyrighted material. The court pointed out that "Skinner has not claimed that any public records exemption applies, and indeed we have found none that do." Noting that the federal Second Circuit had upheld a copyright in such records by a New York county, the Florida court observed that "New York law is not Florida law. We offer no opinion on the federal circuit's analysis because it simply has no application in this case. Each state may determine whether the works of its governmental entities may be copyrighted. As we have explained, Florida's Constitution and its statutes do not permit public records to be copyrighted unless the legislature specifically states they can be." (*Microdecisions, Inc. v. Abe Skinner*, No. 2D03-3346, Florida Court of Appeal, Second District, Dec. 1)

Washington

In a decision that has received considerable criticism from editorial writers across the nation, the Washington supreme court has ruled that a mother violated the Privacy Act when she listened to a phone conversation between her teenage daughter and her daughter's boyfriend by activating the speakerphone function on her cordless telephone. San Juan County Sheriff Bill Cumming suspected that 17-year-old Oliver Christensen was involved in a local purse-snatching. He believed that evidence of Christensen's involvement might be found at the home of Lacey Dixon, Christensen's girlfriend. He contacted Mrs. Dixon, got permission to search the house, but came up empty-handed. He asked Mrs. Dixon to keep a lookout for any evidence. Christensen called Lacey Dixon. Her mother answered the phone and gave the cordless unit to Lacey, who went into her bedroom and shut the door. Mrs. Dixon then activated the speakerphone on the phone's base unit and listened to the conversation in which Christensen told Lacey he was involved in the robbery. Mrs. Dixon took extensive notes and testified against Christensen at trial. Mrs. Dixon was the only credible witness against Christensen, who was convicted of second degree robbery. Saying that the only issue to decide was whether Christensen had an expectation that his conversation was private, the court rejected the state's claim that the two teenagers should have known that their conversation could be overheard. The court found that by going to her bedroom and closing the door Lacey had shown an expectation of privacy and noted that "we have repeatedly held that the mere possibility that intrusion on otherwise private activities is technologically feasible does not strip citizens of their privacy rights." The court rejected the claim that parents could consent to recording their children's phone conversations, pointing out that "the Washington act, with its all-party consent requirement, contains no such parental exception and no Washington court has ever implied such an exception. We decline to do so now." The court added that "since it is Christensen's expectation of privacy with which we are concerned, even if Lacey did have a lower expectation of privacy based on the nature of the relationship with her mother, it cannot reasonably be said that Christensen's

ACCESS REPORTS December 15, 2004 Page 5

expectation was similarly lowered." Finding that the base unit was capable of "transmitting" a conversation, the court concluded that "we must interpret the privacy act in a manner that ensures that the private conversations of this state's residents are protected in the face of an ever-changing technological landscape. This must be done so as to ensure that new technologies cannot be used to defeat the traditional expectation of privacy. For purposes of the privacy act, the word 'transmit' means to disseminate or communicate. Here the base unit of the cordless telephone both received and transmitted. . .The base unit of the cordless telephone was a device designed to transmit within the meaning of Washington's privacy act." (*State of Washington v. Oliver C. Christensen*, No. 74839-0, Washington Supreme Court, Dec. 9)

The Federal Courts...

Judge Colleen Kollar-Kotelly has ruled that EPIC does not qualify for expedited processing because it failed to show sufficient public interest in its request concerning the use of a program called "Verity K2 Enterprise" for data mining purposes. Kollar-Kotelly noted that "fatal to EPIC's request for expedited treatment is the failure in its original FOIA to demonstrate that there is any current public interest in the specific subject of [its] request. EPIC requested 'all agency records. . .concerning [DIA] use of a program or system known as "Verity K2 Enterprise" for the purpose of analyzing intelligence and detecting terrorist activities.' However, Plaintiff's argument for expedited processing included in the FOIA request demonstrates only public interest in the subject of data mining in general. EPIC presented the agency with two articles from the New York Times focusing on a report by DOD's Technology and Privacy Advisory Committee entitled 'Safeguarding Privacy in the Fight Against Terrorism.'. . .However, Plaintiff does not argue that the TAPAC report discusses the Verity K2 Enterprise software specifically. The two New York Times articles cite to the TAPAC report, and like the report address data mining in general, but do not mention Verity K2 Enterprise as a specific software program utilized in the data mining process. Indeed, the articles make no mention of any specific program used in data mining, and the TAPAC report indicates that there are a 'host' of such programs." Kollar-Kotelly observed that "the fact that Plaintiff has provided evidence that there is some media interest in data mining as an umbrella issue does not satisfy the requirement that Plaintiff demonstrate interest in the specific subject of the instant FOIA request, the Verity K2 Enterprise software program." She added that the fact that the media had information about DIA's use of Verity K2 Enterprise and had chosen not to publicize it was an indication that there was no particular public interest in that specific program. She concluded that "it is neither the Court's nor the agency's responsibility to connect the dots for plaintiffs such as EPIC, by presuming that interest in a general topic necessarily indicates interest in a specific subpart of that topic. Indeed, in addition to being beyond the mandate of the Court or agency, it might well prove irresponsible. Although the leap between public interest in data mining in general and interest in Verity K2 Enterprise software in particular may appear obvious to Plaintiff, in the absence of evidence demonstrating as much, the Court cannot assume that such evidence (or such interest) exists. In light of this Circuit's position that expedition is to be sparingly granted because granting one request effectively forces other FOIA requestors further down in the queue, the Court is unable to overlook the absence of evidence supporting Plaintiff's request for expedition." (*Electronic Privacy Information Center v. Department of Defense*, Civil Action No. 04-1219 (CKK), U.S. District Court for the District of Columbia, Dec. 8)

The Seventh Circuit has ruled that the CIA properly refused to identify what records it had concerning whether or not it had information pertaining to Mahmoud Cherif Bassiouni, a DePaul Law School professor and human-rights activist. The CIA had told Bassiouni that it had some records, but that it would not identify them. Circuit Court Judge Frank Easterbrook noted that "the agency does not contend that the *contents* of all documents mentioning Bassiouni are classified; it could hardly do so, given not only its refusal to identify

which documents it holds but also the certainty that its files contain many U.N. reports, newspaper clippings, and other non-classified materials. Instead, the agency maintains that providing a list of the documents that mention Bassiouni, and claiming document-by-document exemptions for those whose contents are classified, would reveal details about intelligence-gathering methods." Bassiouni argued that the agency waived its right to make a neither confirm nor deny *Glomar* response when it indicated that it did have at least one record that mentioned him, a response known as a "no number, no list" response. Easterbrook observed that "how this can be a 'waiver' we do not grasp" and added that "Bassiouni does not contend that the statement 'we have some responsive documents' let the cat out of the bag. Both the [Glomar] and the [no number, no list] response leave to the imagination whether there is a cat to let out. The public is as much in the dark about the agency's sources and methods as it ever was. And Bassiouni is better off under a system that permits the CIA to reveal some things (such as the documents routed to the State Department) without revealing everything; if even a smidgen of disclosure required the CIA to open its files, there would be no smidgens." Bassiouni attempted to get around his FOIA exemption problems by arguing that the CIA was improperly maintaining records pertaining to his exercise of First Amendment rights under subsection (e)(7) of the Privacy Act. But Easterbrook nipped that argument, pointing out that "subsection (e)(7) says that the agency may not *maintain* records unless it meets certain conditions. It does not say that the agency must *disclose* records to the subject when that step would reveal classified intelligence sources and methods." (*Mahmoud Cherif Bassiouni v. Central Intelligence Agency*, No. 04-2258, U.S. Court of Appeals for the Seventh Circuit, Dec. 8)

■ ■ ■

Editor's Note: This is the last issue of *Access Reports* for 2004. The next issue, v. 31, n. 1, will be dated Jan. 12, 2005.

ACCESS REPORTS

1624 Dogwood Lane, Lynchburg, VA 24503 434.384.5334 Fax: 434.384.8272

Please enter our order for Access Reports Newsletter and/or Reference File, the two-volume, loose-leaf Reference Service. It will help us stay on top of developments in FOI and privacy. We may cancel for any reason and receive a refund for the unmailed issues.

- ❑ Bill me
- ❑ Check Enclosed for $_____

- ❑ Access Reports Newsletter for $350
- ❑ Access Reports Reference File for $450
- ❑ Newsletter and Reference File for $575

Credit Card
Master Card / Visa
Card # _____-_____-_____-_____ Expiration Date (MM/YY):_____/_____
Card Holder:_____ Phone # (_____) _____-_____

Name: _____ Phone#: (____) _____-_____
Organization: _____ Fax#: (____) _____-_____
Street Address: _____ email: _____
City: _____ State: _____ Zip Code: _____

Mr. SHAYS. Thank you, Mr. Hammitt.
Ms. Edmonds.

STATEMENT OF SIBEL EDMONDS

Ms. EDMONDS. Good afternoon. My name is Sibel Edmonds.

I have been invited to provide you with my testimony today regarding my direct experience with the use of excessive secrecy, rare privileges and overclassification by the Department of Justice against me during the past 3 years. Thank you for giving me this opportunity today.

I believe that my case clearly illustrates how the Government uses secrecy laws and classification to avoid accountability, to cover up problems and wrongdoings, and to gain an unfair legal advantage in court. I began working for the FBI as a language specialist for several Middle Eastern languages, starting shortly after September 11. I was granted top secret clearance.

During my work, I became aware of problems within the translation unit, involving criminal conduct against our national interests, potential espionage, serious security breaches threatening our intelligence, intentional mistranslation and blocking of intelligence. I was asked and later ordered to refrain from reporting these allegations. I reported them, together with evidence, to higher management within the Bureau. They refused to take any action, and they asked me not to pursue them.

I then took these issues and evidence to the Department of Justice's Office of the Inspector General and to the Senate Judiciary Committee, because I believed that according to our laws, these were the appropriate steps to take in this kind of a situation. As a result, I was retaliated against, I was ordered to submit to a polygraph, which I passed, and they confiscated my home computer. Finally, in March 2002, I was fired. The only explanation I received for getting fired was, for the convenience of the Government.

In March 2002, the Senate Judiciary Committee began investigating my case and allegations, and in July 2002, they had two unclassified briefings with the staff of Senator Grassley and Senator Leahy. During these two unclassified meetings, FBI confirmed basically my allegations, my court allegations. Again, these meetings were unclassified, they were public. These two Senators issued public statements and letters regarding these confirmations that FBI confirmed my allegations and my case. They demanded expedited investigation by the Inspector General and further response from the FBI.

These letters and statements were widely disseminated in the media and on the Internet, including on the Senators' own Web site. When the judge overseeing my legal cases asked the Government to produce any unclassified material that was relevant to my allegations, the Government took a truly extraordinary step. It moved to retroactively classify these letters, statements and news releases that had been public for almost 2 years.

It is quite clear that the Government's motivation was not to protect national security, although they cited national security, but rather to protect itself from embarrassment and from accountability. Senator Grassley characterized this retroactive classification as

ludicrous and gagging the Congress. However, the Congress complied. Only after this highly unusual retroactive classification was challenged in court by POGO, a Government watchdog organization, did the Department of Justice reverse itself and declare that this information was not considered classified and a danger to our national security after all.

I would like to request that these letters from Senators Grassley and Leahy be included in the record of today's hearing.

Mr. SHAYS. We would be happy to include them with no objection. They will be included.

[The information referred to follows:]

U.S. SENATOR PATRICK LEAHY

CONTACT: Office of Senator Leahy, 202-224-4242 **VERMONT**

Following is the text of a letter sent today (Wed., June 19) by Sen. Patrick Leahy, chairman of the Senate Judiciary Committee, and Sen. Charles Grassley, a senior member of the committee, to Glenn Fine, the Justice Department's Inspector General, in which the senators ask Fine to pursue answers to several questions during his inquiry into the matter of allegations made by a former FBI contract linguist. -

++++++++++++++++

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 11/10/03 BY

June 19, 2002

The Honorable Glenn A. Fine
Inspector General
Department of Justice
Washington, D.C. 20530

Dear Mr. Fine:

The Senate Judiciary Committee has received unclassified information from the FBI regarding allegations made by Ms. Sibel D. Edmonds, a former FBI contract linguist, that your office is currently investigating. We request that, as this investigation progresses, you consider the following questions on this matter:

(1) Ms. Edmonds has alleged, and the FBI has confirmed, that the FBI assigned a contract language "monitor" to Guantanamo Bay, Cuba, contrary to clear FBI policy that only more qualified "linguists" be assigned to Guantanamo Bay. What circumstances led to the contract language monitor being considered qualified for this assignment, and what were the consequences, if any, for the effectiveness of the interrogation of those being detained at Guantanamo?

(2) Ms. Edmonds has alleged, and the FBI has confirmed, that another contract linguist in the FBI unit to which Ms. Edmonds was assigned failed to translate at least two communications reflecting a foreign official's handling of intelligence matters. The FBI has confirmed that the contract linguist had "unreported contacts" with that foreign official. To what extent did that contract linguist have any additional unreported or reported contacts with that foreign official? What counterintelligence inquiries or assessments, if any, were made with respect to those contacts? Do you plan to interview field office and headquarters counterintelligence personnel regarding this matter?

(3) The FBI has said that, to review the other contract linguist's work that Ms. Edmonds questioned, it used three linguists in its language division, a supervisory special agent, and special agents who worked on the case that generated the communications under review. Was this a "blind" review by the linguists, or did they know the person whose work was under review? Were the linguists sufficiently independent to make objective judgments about the

translations in question? Would it have been appropriate to use linguists from outside the FBI?

(4) The FBI has said a determination was made by the supervisory special agent that the contract linguist whose work was reviewed made a mistake and that the matter was a training issue. Did this agent's position affect his ability to render an objective judgment? What input did the other special agents provide? Did their involvement in the case that generated the communications affect their ability to make an objective judgement about a person with whom they had worked on the case? Would it have been better to ask other counterintelligence agents to assess the importance of the untranslated information and the reason it was not translated?

(5) To what extent is the credibility of witnesses regarding Ms. Edmonds' allegations affected by their continuing employment in the same translation unit and under the same supervisor where the contract linguist discussed in question (2) is employed.

(6) The FBI has said that Ms. Edmonds prepared two classified documents with respect to her allegations on her home computer without authorization and that one witness reported Ms. Edmonds discussed classified information regarding her allegations in the presence of three uncleared members of her family without authorization. Would these actions disqualify her from a security clearance, given the circumstances of her concern about a foreign attempt to penetrate or influence FBI operations at her workplace?

(7) What guidance is provided to FBI contract linguists as to the steps they should take if they are concerned about a possible foreign attempt to penetrate or influence FBI operations? How well is this guidance understood by contract linguists in the FBI translation centers and other FBI personnel who would handle such matters?

(8) What improvements, if any, are needed to encourage FBI contract linguists and other FBI contract personnel to come forward with such counterintelligence concerns and to ensure that they are not adversely affected as a result of seeking to assist FBI counterintelligence efforts? Was Ms. Edmunds' case handled in a manner that would encourage such reporting in the future?

Please let us know the timetable for your investigation and advise us of the results.

Sincerely,

PATRICK LEAHY
Chairman, Committee on the Judiciary

CHARLES E. GRASSLEY
United States Senator

U.S. SENATOR PATRICK LEAHY

CONTACT: Office of Senator Leahy, 202-224-4242 VERMONT

August 13, 2002

The Honorable John Ashcroft
Attorney General
United States Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530

Dear Attorney General Ashcroft:

We are writing jointly in order that you might allay our concern about the status of the investigation into allegations made by Sibel Edmonds, a former contract linguist in the Washington Field Office of the FBI. Although we understand that the matter is currently under investigation by the Inspector General, we are troubled that the Department of Justice, including the FBI, may not be acting quickly enough to address the issues raised by Ms. Edmonds' complaints or cooperating fully with the Inspector General's office. We are sending a similar letter to Department of Justice Inspector General Glenn Fine.

By way of background, Ms. Edmonds first raised concerns about security problems and the integrity of important translations earlier this year. Unfortunately, nearly every person at the FBI who was notified of the situation reacted by questioning why Ms. Edmonds was "causing trouble." Indeed, the FBI's first internal security action in this case focused on Ms. Edmonds, instead of the allegations she raised in good faith as a whistleblower which bore on national security and the war against terrorism.

Ms. Edmonds has made a number of serious allegations, some of which the FBI verified were not unfounded during an unclassified briefing for Judiciary Committee staff on June 17. First, Ms. Edmonds has alleged that a contract monitor in her unit ("monitor") chose not to translate important, intelligence-related information, instead limiting her translation to unimportant and innocuous information. The FBI has verified that this monitor indeed failed to translate certain material properly, but has attributed the failure to a lack of training as opposed to a malicious act.

That conclusion is directly related to Ms. Edmund's second allegation. Ms. Edmonds alleged that the same contract monitor once worked for an organization associated with a counter-intelligence investigation and that the monitor had contacts with a foreign national who was a member of the target institution. Additionally, Ms. Edmonds states that some of the mistranslated recordings on which the monitor actually worked contained conversations by this same person with whom the monitor had such contacts and concerned matters pertinent to the investigation.

Even after verifying some of these allegations, the FBI downplayed the importance of this matter and seemed to imply that it had ceased looking into the complaints as a security matter until after the Inspector General finished their investigation. Anyone who remembers the long-time treachery of former FBI Supervisor Robert Hanssen, would be concerned at this reaction. For years, Hanssen's bizarre actions were also written off as minor security breaches and unworthy of serious consideration. If even routine diligence had been exercised earlier, Hanssen could have been stopped from doing untold

damage. The FBI needs to learn from its mistakes.

In addition to general concerns raised by this case, we have two specific concerns we wish to raise for your review. First, we have learned that a person central to the investigation will soon be leaving the country – perhaps before the investigation is resolved. If you or your staff would like to know the identity of this person, please contact Inspector General Fine's office, with whom Senator Grassley's staff has been in touch. This person may hold dual citizenship with the United States and a foreign country and may possess a valid passport issued by that foreign country. Thus, there will be little or no assurance that the person will return or cooperate with an investigation in the future. Based on these facts, we would like your assurance that you are satisfied that there has been and will be no delay that will prejudice, in any way, the outcome of this investigation.

Furthermore, we would like your assurance that the Department of Justice, including the FBI, will fully cooperate in all aspects of the inquiry. For instance, we draw your attention to the fact that the FBI currently opposes depositions of the monitor and her husband as part of the investigation into this case, even though the monitor's husband never worked at the FBI,and even though the military agency at which the monitor's husband does work is not opposing a deposition. Moreover, we understand that the monitor and her husband have signed a letter stating they will make themselves available for depositions. It is unclear, then, why the FBI is taking this position in the wake of such important allegations bearing on national security. We hope that you will ensure that the FBI is fully compliant with the Inspector General's inquiry as it proceeds.

Second, we are concerned about the most crucial evidence in the case – the raw material that was allegedly improperly translated. We seek your assurance that the recordings will be properly maintained and promptly translated by a competent and independent authority. That way the validity of the complaint can be quickly judged.

We know that you share our concern that the FBI address issues bearing on national security in a prompt manner, regardless of whether or not they cast the FBI in a positive light. Only by honest evaluation can the FBI learn from its past mistakes. We thank you in advance for your cooperation in this matter. We request a reply in writing at your earliest possible convenience.

Sincerely,

PATRICK J. LEAHY	CHARLES E. GRASSLEY
Chairman	Ranking Member
Committee on the Judiciary	Subcommittee on Crime and Drugs

Ms. EDMONDS. Thank you.

In March 2002, the Department of Justice's Office of the Inspector General began investigating my allegations. In July 2004, after almost 2 years delay, it completed its investigation. The Department of Justice immediately moved to classify the entire report and its findings. Six months later, they allowed the Inspector General to release only an unclassified version of its executive summary. This unclassified version confirmed my core allegations, concluded that I was fired for reporting misconduct and stated that the FBI had failed to investigate the reported espionage, even though other facts, documents, witnesses and evidence support my allegations.

I would like to request that the Inspector General's report also be included in the record of today's hearing.

Mr. SHAYS. We will be happy to do that as well, without objection.

[The information referred to follows:]

U.S. Department of Justice

Vesper Mei, Trial Attorney
Federal Programs Branch
Civil Division
P.O. Box 883, Ben Franklin Station
Washington, D.C. 20044
(202) 514-3367

VMG:VM
145-12-13170

February 18, 2005

VIA EMAIL AND FACSIMILE (202) 588-7795

Michael T. Kirkpatrick
Public Citizen Litigation Group
1600 20th Street, N.W.
Washington, D.C. 20009

Re: POGO v. Ashcroft, et al. 04-CV-1032 (JDB)

Dear Mr. Kirkpatrick:

I am writing with respect to the three letters at issue in this lawsuit: 1) the June 19, 2002 letter from Senators Patrick Leahy and Charles Grassley to Glenn Fine, Inspector General of the Department of Justice referred to in paragraph 9 of your Complaint; 2) the August 13, 2002 letter from Senators Leahy and Grassley to Attorney General John Ashcroft referred to in paragraph 10 of your Complaint; and 3) the October 28, 2002 letter from Senator Grassley to Robert Mueller, Director of the FBI, referred to in paragraph 11 of your Complaint. The FBI has determined that these documents are releasable in full, pursuant to the Freedom of Information Act. The first two letters are attached; we note that the third is available on the internet at http://grassley.senate.gov/releases/2002/p02r10-28.htm. We trust that this resolves the concerns that you raised in your case.

Sincerely yours,

Vesper Mei

Vesper Mei
Trial Attorney

Attachments

U.S. Department of Justice
Office of the Inspector General

A Review of the FBI's Actions in Connection With Allegations Raised By Contract Linguist Sibel Edmonds

UNCLASSIFIED SUMMARY

Office of the Inspector General
Office of Oversight and Review

January 2005

I. INTRODUCTION

This report describes the Office of the Inspector General's (OIG) investigation of allegations raised by Sibel Edmonds, a former Contract Linguist (CL) for the Federal Bureau ofInvestigation (FBI). Edmonds worked for the FBI from September 20, 2001, until March 2002, when her services as a CL for the FBI were terminated. Before that termination, she had raised a series of allegations regarding the FBI's CL program, including security concerns about actions by a co-worker related to potential espionage.

Our review found that Edmonds had written several memoranda to her supervisors raising her concerns about the co-worker. Edmonds prepared one of her memoranda, dated February 8, 2002, on her home computer, after first obtaining a supervisor's permission to write it at home. According to the FBI, that memorandum contained classified information, and Edmonds' use of her home computer to process classified information was a security violation.

Edmonds' supervisor referred Edmonds' February 8 memorandum containing her allegations to a Security Supervisor. The Language Supervisor also reported Edmonds' security violation to the Security Supervisor. After a cursory investigation of Edmonds' allegations, the Security Office concluded that Edmonds' allegations against the co-worker were unsubstantiated and that Edmonds' security violation was inadvertent.

Edmonds continued to complain about the co-worker, and asserted that FBI supervisors were protecting the co-worker. Edmonds also raised her concerns to higher-level officials in the FBI, to the OIG, and to Congress. In addition, Edmonds raised other allegations regarding the language program to the OIG. For example, Edmonds made allegations of travel voucher fraud and time and attendance abuse. Edmonds also alleged that the FBI had hired unqualified personnel and used one of them to translate military interviews despite that person's weak language skills.

On March 22, 2002, the FBI stopped using Edmonds' translation services, and on March 26 the FBI terminated her contract. Edmonds complained that the termination was in retaliation for her complaints, and the OIG agreed to investigate this matter.

II. SCOPE OF OIG INVESTIGATION

During the course of our investigation, the OIG interviewed more than 50 individuals, including FBI employees, contractors, and Department of Justice (DOJ) officials. The OIG interviewed Edmonds on three separate occasions, in April, June, and November of 2002. On January 28, 2004, the OIG wrote to Edmonds' attorney offering to meet with Edmonds again if she had additional relevant information to provide to the OIG. Her attorney said that Edmonds did not believe she had anything additional to provide the OIG, and the attorney did not request an additional meeting.

In addition, the OIG obtained and reviewed thousands of pages of FBI documents relating to Edmonds' allegations, including e-mails, notes, and other records. We also sought expert assistance with translations and other matters from another federal government agency outside the DOJ.

We closely examined nearly a dozen separate allegations by Edmonds against the co-worker which, when viewed together, amounted to accusations of possible espionage. We sought to determine, with respect to each individual allegation, whether the facts supported or refuted the allegation. However, the ultimate determination as to whether the co-worker engaged in espionage, as Edmonds' allegations implied, was beyond the scope of the OIG's investigation. We communicated to the FBI during our review that the OIG was not making such a determination, and that the potential espionage issue should be addressed by the FBI, not the OIG. Instead, our investigation focused on the FBI's response to the complaints Edmonds raised about her co-worker and other language translation issues.

According to some media accounts, Edmonds made additional allegations relating to the September 11 terrorist attacks and the allegedly inappropriate reaction by other FBI linguists to those attacks. However, Edmonds never raised those allegations to the OIG, and we did not investigate them in our review. Rather, we understand that staff from the National Commission on Terrorist Attacks Upon the United States (9/11 Commission) interviewed Edmonds regarding these claims. Our review focused on the allegations made by Edmonds to the OIG, particularly Edmonds' allegations regarding the FBI's handling of the concerns about the co-worker, her allegations about inappropriate practices in the language program, and her allegation that the FBI retaliated against her for raising those allegations.

This report is an unclassified version of the OIG's full 100-page report on Edmonds' allegations. The OIG completed the full report in July 2004 and provided copies of it to the 9/11 Commission and several congressional committees that have oversight of DOJ. Subsequently, two members of the Judiciary Committee specifically requested that the OIG create a declassified version of the report for public release. The letter stated that releasing a "declassified" version of the report, "or at least portions or summaries, would serve the public's interest, increase transparency, promote effectiveness and efficiency at the FBI, and facilitate Congressional oversight." In response, the OIG created this unclassified summary of the full report.1

1 The FBI conducted a classification review of the full version of this report and classified it at the Secret level. Because the information was from the FBI, the OIG did not have the authority to declassify or publicly release the report on its own. We conferred with the FBI and the DOJ Civil Division in the creation of this unclassified summary of the report. We believe this unclassified version summarizes the core of the OIG report, although it does not include all of the facts in the full report or even all of the allegations addressed in the full report. Moreover, we recognize that, in some instances, it is difficult to understand this version of the report fully because much of the information from the full report remains classified and cannot be included here. However, this version is the maximum that the FBI and the DOJ Civil Division agreed was unclassified and allowed to be released publicly.

This report describes the results of our investigation. In Part III of the report, we provide background information on Edmonds and relevant FBI components and procedures. In Part IV, we assess the factual basis underlying Edmonds' allegations against the co-worker. In Part V we provide a factual chronology of relevant events and an analysis of the FBI's handling of the allegations as they arose. In Part VI, we examine some of Edmonds' additional allegations, including concerns about travel voucher fraud and time and attendance abuse. In Part VII, we address the allegation that the FBI decided to stop using Edmonds as a linguist in retaliation for her allegations. Finally, in Part VIII, we make systemic recommendations to the FBI in an attempt to help it improve its foreign language translation program.2

2 It is important to note that the OIG completed a broader audit regarding the FBI's foreign language translation program. That audit is entitled "The Federal Bureau of Investigation's Foreign Language Program Translation of Counterterrorism and Counterintelligence Foreign Language Material." In it, the OIG examined the FBI's ability to translate critical foreign language material, its success at meeting linguist hiring goals, and whether the FBI's procedures ensure the appropriate prioritization of work, accurate and timely translations of pertinent information, and adequate pre- and post-hire security screening of linguists. The audit report was completed in July 2004 and classified by the FBI at the Secret level. Like the full Edmonds report, that audit report was provided to several Congressional committees and the 9/11 Commission. The OIG released an unclassified summary of the audit report in July 2004. It is available on the OIG's website at http:/www.usdoj.gov/oig/audit/FBI/0425/index.htm.

III. BACKGROUND

In this section of the report, we provide brief background information on Edmonds. We also describe the FBI's Language Services Section (LSS), which manages the FBI's language program and its linguists. We then describe some of the procedures regarding FBI language translations that are relevant to this case.

A. Edmonds

Edmonds, who was born abroad and speaks English fluently, moved to the United States in 1991 to attend college. She married an American citizen in 1992. Before joining the FBI, Edmonds worked as a volunteer at a local courthouse, as a court-appointed special advocate for children, and for the Rostropovich foundation, a non-profit organization that delivers medical supplies and food to a children's hospital. In addition, Edmonds served as a

corporate officer (Secretary) for her husband's consulting business.

Edmonds applied to the FBI on March 10, 1997, for a linguist position. After she took the requisite language tests, by letter dated May 6, 1998, the FBI offered Edmonds a position as a CL. The offer was contingent upon Edmonds receiving a Top Secret security clearance.

Pursuant to instructions in the offer letter, Edmonds completed, on June 4, 1998, an SF-86 Questionnaire for National Security Positions - the standard form used by the federal government to collect information for background investigations of persons applying for positions that require a security clearance. As part of the background investigation, Edmonds was polygraphed on December 4, 1998. The FBI also conducted a Personnel Security Interview (PSI) of Edmonds on December 16, 1998. Her security file does not reflect any activity on her background investigation during 1999. It appears that through a series of oversights and lack of follow through, the FBI did not take action on her background investigation, and therefore Edmonds did not begin work as a CL during this time period.

In February 2000, the FBI asked Edmonds to submit another SF-86. In April 2001, LSS wrote a memorandum requesting that the PSI be updated, and asking that the necessary work be done to complete the background investigation. The FBI conducted supplemental PSIs of Edmonds on May 1, 2001, and July 19,2001. On September 13,2001, four years after she first submitted her application, the FBI granted Edmonds a "Top Secret" clearance. No job interview was conducted other than the PSIs.

Edmonds began working for the FBI on September 20, 2001, first as a Contract Monitor (CM), and shortly thereafter as a CL.3 As we describe below, on March 22, 2002, the FBI stopped using Edmonds' translation services.

> The various linguist positions in the FBI are described more fully in the next section of this report. In brief, a CM can provide summary translations of oral and written communications, and analyses of those translations, for internal dissemination. In addition to those services, CLs also can act as interpreters in FBI interviews, review material produced by other linguists, produce written communications for internal and court dissemination, and testify as expert witnesses in federal court. A CL can perform the same duties as a Language Specialist, which is the term for a linguist who is a permanent employee of the FBI.

B. The FBI's Language Services Section

1. Organization

In the early 1980s, the FBI began hiring linguists for translation, interpretation, and other language services necessary for the FBI's work. Before that, the FBI used Special Agents to perform such services. The number of linguists hired by the FBI grew from a mere handful in 1983 to over 1,100 by 2002.

Through its Foreign Language Program (FLP), the FBI seeks to ensure that the language needs of its field offices and Headquarters units are met. The FLP and the personnel who perform language services for the FBI are directed by the LSS. LSS personnel handle approximately 60 languages covering 95 percent of the world's population. Since March

2002, the LSS has been placed within the Office of International Operations at FBI Headquarters, which is under the jurisdiction of the FBI's Director for Law Enforcement Services. Immediately before the March 2002 reorganization, LSS was part of the Investigative Services Division.4 A copy of the FBI's organizational chart, dated March 4, 2004, is attached as Appendix A.

4 Before that, LSS had been placed, at various times, in the Laboratory Division and the Criminal Investigative Division.

During the early part of 2002, the time relevant to this review, LSS was composed of three units. The Language Training and Assessment Unit (LTAU) was responsible for developing and conducting language assessments of FBI applicants and personnel. The LTAU also provided foreign language and cultural training to FBI personnel. The Translation and Deployment Unit (TDU) managed national translation and interpreting resources in support of the FBI's investigative and administrative priorities. The TDU ensured that linguists were assigned to offices requesting their services or that a requesting office's work was sent to available linguists. The Language Administration and Acquisition Unit (LAAU) handled the administrative functions of the FLP. The LAAU also was responsible for hiring linguists and for researching, acquiring, and integrating language-related technologies. An organizational chart for the LSS, dated November 13,2001, is attached as Appendix B.

2. Types of Linguists

The FBI uses three types of linguists. First, the FBI has permanent employees known as Language Specialists (LS). LSs provide translations of written or oral communications and analyze those translations. They also can act as interpreters in FBI interviews, review material produced by other linguists, produce written communications for internal and court dissemination, and testify as expert witnesses in federal court.

In addition, the FBI uses contract employees as linguists. The Contract Linguist Program (CLP), which is administered by the LAAU, enables the FBI to acquire linguist resources without adding permanent employees. It also gives the FBI the opportunity to recruit permanent LSs from linguists who already have been evaluated through the CLP. The FBI uses two types of contractors with different skill levels, CLs and CMs. Linguists' designation as CL or CM depends upon their performance on language tests administered by the LSS.5

5 In this report, the generic terms "linguist" and "translator" refer to any of the three categories - LS, CL, and CM.

According to an LSS Operational Manual, CLs perform translation duties "similar to those of Language Specialists." CLs provide translations of written or oral communications and analyze those translations. They also act as interpreters in FBI interviews, review material produced by other linguists, produce written communications for internal and court dissemination, and testify as expert witnesses in federal court.

The FBI created the additional position of CM in response to a critical need for linguists and the inability to find a sufficient number of linguists who qualify for LS or CL positions. A CM can provide summary translations of oral communications and analyses of those translations, and written communications for internal dissemination. An FBI memorandum

explains that the CM position was proposed to address a critical need for linguists to perform summarization work. The memorandum explained that a CM's work may require some additional clarification and review. It stated that CMs should not be asked to write foreign language transcriptions, nor should they testify regarding the accuracy of their translations. In addition, according to the memorandum, a CM's work should be reviewed by a fully qualified linguist before it is used for other than internal use. Moreover, the memorandum recommended that the CMs not be given assignments in offices where they are the only speakers of the language in question.

Thus, CMs are more limited in their duties than CLs. For example, a CL is qualified to provide a verbatim translation. A CM, in contrast, is not approved for verbatim translations of documents, but may provide summary translations. However, in order to cope with these limitations, the FBI often has CMs do verbatim translations and then has the translations reviewed by CLs.

LSS directs from FBI Headquarters all of the linguists in the FLP. The linguists themselves generally are assigned to assist FBI agents in their work, and the linguists generally are grouped according to language. FBI linguists translate a wide variety of materials, including recordings, written documents, and audio recordings of interviews.

3. Language Services Section Computer System and Training

As discussed more fully in the OIG's foreign language translation audit, (cited at footnote 2), an FBI computer network links FBI offices and permits large quantities of material to be moved between offices for translation, to better utilize FBI linguistic resources.

More than one linguist may be assigned to a particular task, due to resource issues. The FBI's computer system only keeps a record of the last person to work on a particular task; it does not maintain records of any other linguist's prior access. In addition, the work does not remain on the computer system for long because of space limitations. Material may be removed from the system in as little at three days, whether or not a linguist has reviewed it. Once material is removed from the local network, it is stored, or archived, so it can be reviewed later. However, information about who reviewed the material is not retained in this archiving process, though material that has been archived can be retrieved. The FBI attempts to ensure that reviewed material is removed before un reviewed material. A senior LSS supervisor told the OIG that a "conscientious" supervisor can "protect" unreviewed material by specially marking it so that it will not be deleted from the system.6

6 6 This senior supervisor noted that if a linguist is out of the office when material is removed, the linguist may not even be aware of the removal. He described this as a "huge problem."

Documents created by linguists are automatically shifted from an individual linguist's computer directory to the agents' computer directory on a scheduled basis. A linguist can prevent a document from being automatically moved only by taking steps to prevent this automatic feature from activating.

General training for linguists is handled by LSS, not by the agents the linguists will be assisting. The linguists are assigned to assist the Special Agents with respect to the subject matter of their cases. The Special Agents instruct the linguists as to what they do and do not

want them to translate. A Special Agent told the OIG that he also briefs the linguists on guidelines they need to know to do their work. This Special Agent said that, for the first six months to a year, he does not expect much from the linguists because they are still learning what is important and how to do the work.

C. FBI Security Procedures

Linguists must obtain security clearances to work for the FBI. Edmonds and the co-worker went through this process. The adequacy of the co-worker's security review was a significant issue in this case.

1. Personnel Security Interview

In addition to completing the required forms for a national security position, an individual whose background is being investigated by the FBI must undergo a PSI.7 According to the instructions on the SF-86, the interview is an "opportunity to update, clarify, and explain information on your form more completely." According to the FBI's Manual of Investigative Operations and Guidelines (MIOG), the interview must be conducted at the "inception of the [background] investigation with the purpose of obtaining information to facilitate our investigative efforts," and "to ensure that complete (current and accurate) information is available concerning the candidate." MIOG, Part 2, Section 17-5.6.

7 7 Not all federal agencies use the FBI to conduct background investigations. However, because the FBI conducts background investigations on Contract Linguists such as Edmonds and the co-worker, this section addresses the FBI policies and procedures for conducting background investigations on its applicants and employees.

According to the MIOG and a relevant FBI Electronic Communication (EC), areas to be covered in the background investigation include personal and business credit issues, denials and dismissals from employment, business circumstances that could lead to conflict-of-interest allegations, membership or involvement in organizations that are discriminatory and organizations that advocate activities against the interest of the United States, and concealment of any activity that could be used to compromise the applicant or have an adverse effect on their character. MIOG, Part 2, Section 17-5.6.

2. Pre-employment Polygraph

All applicants for employment with the FBI, including CLs, also must undergo a pre-employment polygraph examination. Manual of Administrative Operations and Procedures (MAOP), Part 1, Section 22-9.1. The examination focuses on national security issues, use or sale of illegal drugs, and completeness of the Application for Employment. MIOG, Part 2, Section 13- 22.12. An expanded polygraph examination may be requested regarding any national security concerns remaining after the PSI.

3. Security Clearance

The LSS conducts the background investigation and the pre-employment polygraph to ensure that the candidate is suitable for employment. The applicant's file is then passed to the Initial Clearance and Access Unit (ICAU) in the Personnel Security Section within the

FBI's Security Division.8 ICAU's function is to determine if the applicant will be granted a security clearance. The adjudicators within ICAU may request that a risk assessment be performed. A risk assessment is meant to address any security concerns that surface during the applicant's background investigation, including those that might indicate the applicant's vulnerability to coercion.

8 Before the creation of the Security Division in December 2001, these duties were performed by the Industrial Security Unit within the FBI's National Security Division.

The risk assessment is initiated by sending a lead to the relevant operational division at FBI Headquarters.9 A Special Agent or analyst who has the expertise for that specific area completes the risk assessment. According to the ICAU Unit Chief, the decision to conduct a risk assessment for an applicant depends on the specific circumstances of the case.10 He stated that as of March 2004, risk assessments are completed for approximately 95 percent of applicants for CL positions.

9 When an FBI field office needs assistance or information from another office or from FBI Headquarters, it "sets a lead" for the assistance. Leads are initially written out in ECs, hard copies of which are mailed to the appropriate offices.

10 Throughout this report, individuals are identified using the title they held at the time of the event or action under examination.

If the ICAU determines that a potential contractor should be granted a security clearance, a Security Officer gives that person a security briefing.11 The purpose of the briefing is to inform individuals that they may not disclose sensitive or classified information obtained while working for the FBI, and to inform the individuals of the consequences for unauthorized disclosure.

11 The Special Agents who serve as Security Officers are responsible for processing administrative paperwork for FBI employees, contractors, and others who need security clearances, country clearances, and travel warnings. They also pass clearances to other organizations. The Security Officer also provides security briefings and covers leads for background investigations.
Security Officers also conduct investigations of reported and suspected security violations. The types of violations they investigate include using home computers to process classified information, processing Top Secret information on the internal FBI Secret network, unauthorized access to FBI files, and sharing computer passwords.

At the briefing, new contractors sign a Security Acknowledgement Form in which they acknowledge that they understand the information provided in the briefing and agree to adhere to instructions printed on the form for handling classified information. They also sign a Classified Information Nondisclosure Agreement. The Agreement is an 11-point agreement between the individual and the United States government stating that the individual possesses a security clearance for access to classified information, has been briefed about security responsibilities, and will not improperly divulge classified information. The Agreement also sets forth the potential punishments for improperly divulging classified information. Until the form is signed, the individual does not have clearance and cannot have access to national security information.

IV. THE OIG'S EXAMINATION OF EDMONDS' ALLEGATIONS AGAINST A CO-WORKER

In this section, we examine the allegations Edmonds made against her co-worker. In the classified version of the report, we fully described and evaluated the evidence underlying nearly a dozen separate allegations Edmonds made regarding the co-worker which, when viewed together, amounted to an accusation against the co-worker of possible espionage. With respect to each individual allegation, we analyzed the facts supporting or refuting the allegation. We did not attempt to reach a definitive conclusion on the truth of each allegation or whether the implication of espionage was supported. Rather, given the available evidence, we assessed whether the FBI treated each allegation appropriately. Because the facts underlying each allegation remain classified, we cannot include our detailed description and analysis of each individual allegation in this unclassified summary. Instead, we describe our evaluation of Edmonds' allegations in general terms.

We found that many of Edmonds' core allegations relating to the coworker were supported by either documentary evidence or witnesses other than Edmonds. Moreover, we concluded that, had the FBI performed a more careful investigation of Edmonds' allegations, it would have discovered evidence of significant omissions and inaccuracies by the co-worker related to these allegations. These omissions and inaccuracies, in turn, should have led to further investigation by the FBI. In part, we attributed the FBI's failure to investigate further to its unwarranted reliance on the assumption that proper procedures had been followed by the FBI during the co-worker's hiring and background investigation, which did not include a risk assessment, contrary to FBI practice. We also found that Edmonds was justified in raising a number of these concerns to her supervisors. For example, with respect to an allegation that focused on the co-worker's performance, which Edmonds believed to be an indication of a security problem, the evidence clearly corroborated Edmonds' allegations.

With regard to some of Edmonds' allegations, the OIG did not find evidence to support her allegation or the inferences that she drew from certain facts. However, Edmonds' assertions regarding the co-worker, when viewed as a whole, raised substantial questions and were supported by various pieces of evidence. While there are potentially innocuous explanations for the coworker's conduct, other explanations were not innocuous. Although the exact nature and extent of the co-worker's security issues are disputed, it is clear from the OIG's investigation that the facts giving rise to Edmonds' concerns could have been uncovered had the FBI investigated Edmonds' allegations further. We believe that the FBI should have investigated the allegations more thoroughly. We also believe the FBI's handling of these allegations reflected an unwarranted reluctance to vigorously investigate these serious allegations or to conduct a thorough examination of Edmonds' allegations. As will be discussed in the next section, the FBI did not, and still has not, conducted such an investigation.

Finally, as we discuss in Part V, rather than investigate Edmonds' allegations vigorously and thoroughly, the FBI concluded that she was a disruption and terminated her contract. We concluded that the FBI could not show, by clear and convincing evidence, that it would have terminated Edmonds' services absent her disclosures.

V. FACTUAL CHRONOLOGY RELATED TO EDMONDS' ALLEGATIONS AGAINST A CO-WORKER

In this section of the report, we provide a chronological summary of relevant events and issues pertaining to Edmonds' allegations against the coworker. 12 We also examine the FBI's handling of the allegations against the coworker.

12 This version of the report uses male pronouns throughout for individuals who are not named, regardless of gender.

A. Edmonds' Initial Allegations

Edmonds began contract work at the FBI on September 20, 2001. At her request, she worked part-time for approximately 20 hours per week. Edmonds initially was assigned as a CM, and shortly thereafter as a CL. Edmonds and her colleagues were assigned to assist agents with translations on various operational matters.

Toward the end of 2001, Edmonds became suspicious of a co-worker for various reasons. In Edmonds' view, information she learned about the coworker's background, coupled with certain of the co-worker's actions with regard to the co-worker's work at the FBI, raised a security concern. Edmonds told the OIG that a series of events in December 2001 and January 2002 formed the initial basis for her complaints to her supervisors and to the OIG. First, Edmonds told the OIG that her conversations with the co-worker and her observations of the co-worker's conduct made Edmonds uneasy about the coworker from a security standpoint. Edmonds also told the OIG that in early January 2002, she saw documents that increased her suspicion about the coworker. Also in early January, according to Edmonds, documents began to disappear from her work space, and she became suspicious due to revisions in the distribution of work assignments that recently had been implemented. On January 22,2002, Edmonds documented some of her concerns and provided them to her supervisor. As a result of Edmonds' written concerns, on January 25, 2002, meetings were held to address the issues she raised. After the meetings, the FBI took a number of steps in response to the information Edmonds had provided. In addition, although her Language Supervisor told an FBI manager about the allegations, no one reported the matter to the Security Office at that time.

We concluded that the actions taken by the FBI after Edmonds raised concerns in writing on January 22,2002, and orally on January 25,2002, were insufficient and did not address fully the concerns raised. Moreover, we found that the approach taken by the FBI in response to Edmonds' allegations compromised, in certain respects, its opportunities to investigate further.

Several FBI witnesses told the OIG that allegations suggesting potential espionage by one FBI employee against another are exceedingly rare. This allegation was extremely serious - even if the evidence was not clear. Once Edmonds submitted her detailed written complaints about her colleague, a sufficient basis existed to justify a thorough inquiry by the FBI. However, as will be described below, the FBI's inquiry was seriously deficient. 13

13 As demonstrated by the espionage of former FBI Agent Robert Hanssen, the FBI must take seriously allegations suggesting security,breaches, even if the evidence is not clearcut. The Hanssen case demonstrates that an individual reporting a security-related concern about another employee may not have the whole story, but may provide sufficient information to focus attention on a person deserving of further scrutiny. See the OIG's report entitled "A Review of the FBI's Performance in

Deterring, Detecting, and Investigating the Espionage Activities of Robert Philip Hanssen," August 2003. It is available on the OIG's website at http://www.usdoj.gov/oig/special/0308/final.pdf.

B. Edmonds Documents Additional Complaints in a February 8 Memorandum Written on Her Home Computer

In the two weeks following the January 25 meetings, Edmonds made additional complaints, including assertions that the co-worker was being protected inappropriately by a supervisor.14 Edmonds also alleged that the coworker threatened her. Ultimately, Edmonds was asked to provide the details of her complaints in writing. Edmonds asked if she could write them up at home due to her concerns about items being removed from her computer, and the Language Supervisor agreed to the request. Using her home computer, Edmonds wrote a memorandum about her complaints dated February 8, 2002.

14 The OIG's examination of FBI records did not substantiate the allegation that the coworker was being inappropriately protected.

Edmonds provided the memorandum to the Language Supervisor on February 9, 2002. That day, the Language Supervisor sent a copy of the memorandum to the Chief of the LAAU. Initially, the Language Supervisor expressed no concern to the LAAU Chief about whether Edmonds' memorandum contained any classified information, nor did the Language Supervisor indicate that he would contact the Security Office. The Language Supervisor explained to the LAAU Chief that a copy of Edmonds' memorandum was provided to others for response. In addition, the Language Supervisor spoke to the Special Agent who Edmonds assisted and asked him to conduct some follow-up on Edmonds' memorandum. In addition, the Language Supervisor decided to begin supervising Edmonds directly. The Language Supervisor also notified his superior about Edmonds' allegations.

The OIG found problems with the manner in which the FBI initially handled Edmonds' February 8 memorandum. In response to Edmonds' February 8 memorandum, the Language Supervisor provided a copy to a person (other than the co-worker) who was discussed in the memorandum, for his response, even though this created a risk that the investigation could be compromised. In addition, the Language Supervisor spoke to the Special Agent who Edmonds assisted and asked him to conduct certain follow-up, although this also could have compromised any investigation. Edmonds had raised an extremely serious allegation that deserved to be handled more carefully. The Language Supervisor's requested follow-up action was not a prudent step, given the possible consequences if Edmonds' allegations were true.

C. Security Office Investigation

On February 11, 2002, the Language Supervisor gave a Security Officer a copy of Edmonds' February 8 memorandum and called his attention to the security concerns related to the co-worker. The Security Officer told the OIG that the Language Supervisor stated that Edmonds had included some classified information in the memorandum that she had written on her home computer. The Security Officer was assigned to investigate the matter.

On February 12,2002, the Security Officer interviewed Edmonds. Edmonds told the Security Officer she had written the memorandum on her home computer because of her

concerns about documents being taken from her office, and said she had done so with the Language Supervisor's permission. Edmonds acknowledged that her husband used the home computer for work, including faxing documents and sending e-mail. Edmonds said that her husband did not look at her documents. Edmonds also repeated her concerns about the co-worker to the Security Officer.

The Security Officer told the OIG that he believed Edmonds was credible. The Security Officer said that based on this interview, he was primarily concerned about two things: Edmonds' allegation that she was threatened by the co-worker and the fact that classified information was on Edmonds' home computer.

The next day, the Security Officer interviewed the co-worker. The Security Officer asked the co-worker questions pertaining to the allegations raised by Edmonds, and the co-worker denied Edmonds' allegations. The Security Officer told the OIG he also found the co-worker to be credible, which he said undermined his confidence in Edmonds. However, we found the Security Officer did not challenge the co-worker with respect to any information the co-worker provided, although that information was not consistent with FBI records. In addition, while the Security Officer reviewed some records, he did not review other crucial FBI records, which would have supported some of Edmonds' allegations.

On February 13, with Edmonds' consent, the FBI seized her home computer. That same day, Edmonds also wrote to a higher-level FBI official about her allegations and requested to meet with him regarding her concerns.

On February 14, the Security Officer observed while a member of the FBI's Computer Analysis Response Team analyzed Edmonds' computer to determine what information had been processed on it. The Security Officer said that there appeared to be another version of the February 8, 2002, memorandum on the computer. The FBI removed the classified information from the computer and returned the computer to Mr. Edmonds on February 15.

On February 20, the Security Officer conducted an interview of a potential witness to the co-worker's alleged threat to Edmonds. After the interview, the Security Officer reported up his supervisory chain that he believed that Edmonds' allegations were unfounded. This assessment was, in turn, reported to a manager higher up the supervisory chain.

On February 25, the Security Officer requested polygraph examinations of Edmonds and the co-worker in connection with this matter.

We concluded that once the Security Officer was notified on February 11 of Edmonds' potential security violation, he took swift action with respect to the security violation Edmonds committed. The Security Officer quickly took custody of Edmonds' home computer and analyzed it. The Security Officer also deleted classified information from the computer and returned the computer to Edmonds.

By contrast, we believe that the Security Officer's investigation of Edmonds' claims against the co-worker was significantly flawed. The Security Officer neither adequately prepared for nor adequately followed up on information obtained during the course of the investigation. The Security Officer also failed to memorialize adequately crucial information derived during the course of the investigation. While an investigator's impressions of the witnesses are significant in any investigation, in this case the absence of

any effort by the Security Officer to corroborate information provided by witnesses with independent evidence suggests that he relied unduly on his subjective impressions of the witnesses.15 Moreover, the Security Officer over-relied on the absence of corroboration of the threat allegation, which the Security Officer believed to be the most serious aspect of Edmonds' allegations. This overreliance resulted in a premature conclusion that Edmonds' security concerns lacked merit.

15 In an e-mail dated February 14, 2002, three days after the Security Office was notified of these allegations, the Language Supervisor wrote that it was his opinion and the opinion of the Security Officer and the Special Agent who Edmonds assisted that Edmonds was trying to get the co-worker "fired." The Security Officer denied expressing that opinion by that date.

In addition, the Security Officer failed to perceive as a security issue what he considered were merely performance issues. He did not, therefore, adequately address these issues and, as will be discussed later, deferred to others completely for an evaluation of this aspect of the case. We believe it was the Security Officer's responsibility to gather all the facts related to these allegations, many of which the Language Supervisor would not have known, and it was inappropriate for the Security Officer to defer to the Language Supervisor or others on certain critical questions.

In sum, the Security Officer conducted a superficial investigation that focused almost entirely on Edmonds' allegation regarding a threat to her. The Security Officer seemed not to appreciate or investigate the allegation that a coworker may have been committing espionage. Nor did the Security Officer refer the allegations of potential espionage elsewhere in the FBI. The Security Officer told the OIG that he believed, based on the amount of evidence at hand, a referral would have been pointless. Our review revealed that a thorough investigation by the Security Office would have shown otherwise.

D. Follow-up by the Language Supervisor

On February 14, the Language Supervisor sent an e-mail to the LAAU Chief and another FBI manager providing an update on the case. In the e-mail, the Language Supervisor asserted that there was no basis for Edmonds' concerns. In response to the Language Supervisor's e-mail, the LAAU Chief wrote an e-mail dated February 15 stating that he was "still concerned" about Edmonds' allegations. The LAAU Chief stated that crucial FBI records (those that the Security Officer never personally reviewed) did not resolve a significant aspect of Edmonds' allegations. He asked that the matter be looked into further. He also urged that the matter be addressed quickly and fairly to avoid losing any "precious linguistic resources" due to "morale problems."

On February 21,2002, the Language Supervisor sent an FBI manager and the LAAU Chief an EC summarizing his actions in connection with Edmonds' allegations. In the EC, the Language Supervisor stated that the security allegations related to the co-worker had been referred to the Security Office. With respect to some of Edmonds' allegations, the Language Supervisor wrote that the matter would be addressed by him and others in his office as a "performance and management issue." The Language Supervisor added that it could be a "training issue" and that language translators had voiced concerns about their inadequate training. He stated that he would hold appropriate persons responsible for any problem of that nature and he would continue to address the matter in a mid-year performance review. In addition, the Language Supervisor described his efforts to determine whether certain of

Edmonds' other allegations were true.

The Language Supervisor also stated in the EC that he had put Edmonds under his supervision. In addition, he wrote that on February 11 Edmonds told him that she was considering going public and bringing criminal charges. Finally, the Language Supervisor reported that on February 19, despite the fact that Edmonds was told that the matter was being investigated and she should be patient, Edmonds said she had retained a lawyer and had written letters to "high level" officials within the FBI. The Language Supervisor said he cautioned Edmonds on both occasions not to reveal classified information.

E. Edmonds Meets with FBI Management

On February 22, Edmonds met with FBI management. An FBI manager told the OIG that his purpose in holding the meeting was to try to reduce Edmonds' anxiety and to find out from her if there were other facts that would support her allegations. He said he told Edmonds that the Security Office investigation had not borne out the most serious aspect of her security concerns. He said he explained to Edmonds that he had also contacted others within the FBI and no basis for that aspect of her security concerns existed. At the meeting, Edmonds asked this manager to put his statements to her in writing. He declined.

Edmonds described this meeting to the OIG as confrontational and hostile. The FBI manager denied that and said his impression of Edmonds after the meeting was that she was "very bright" and "aggressive." He said that, at the time, he did not believe she was fabricating her allegations. Immediately after the meeting, however, the manager began to explore whether the FBI had the option to cease using Edmonds as a CL.

F. Follow-up by the Special Agent who Edmonds Assisted

On February 26, an FBI Special Agent wrote an EC analyzing the additional information the Language Supervisor had requested as a result of Edmonds' allegations of deficient performance by the co-worker. The Special Agent believed that a remedial measure would adequately address the performance aspect of Edmonds' allegations. The remedial measure was then implemented. No other action was taken as a result of the review. However, the remedial measure was rescinded, at the request of this Special Agent, less than three weeks later, and Edmonds questioned the decision to rescind the remedial measure.

G. Polygraph Examinations

The Security Office decided that polygraph examinations would be helpful in making determinations about Edmonds' security allegations and the security violation committed by Edmonds. In a four-page request for polygraphs, drafted on February 25, 2002, the Security Officer stated that "preliminary investigation" indicated that the co-worker had not made any threats to Edmonds, but the polygraph was needed to thoroughly pursue these issues and determine whether or not the co-worker posed a security risk. The Security Officer also noted that "preliminary investigation" indicated that Edmonds had written, on her home computer, multiple memoranda containing classified information, had retained an attorney, and had threatened to go to the press. The Security Officer asked that a polygraph be conducted of Edmonds to determine whether she had written additional memoranda on her home computer or whether she released classified information to unauthorized parties. 16

16 Once Edmonds was notified of the polygraph, she began writing letters to FBI managers requesting a written explanation of why she was being polygraphed and what questions she would be asked. The FBI declined to provide her with anything in writing on that subject.

Based on the Security Officer's request of February 25, which was approved by the FBI, polygraph examinations of Edmonds and the co-worker were scheduled for March 2002. The Chief of the FBI's Polygraph Unit e-mailed an FBI manager to say that the focus of the polygraph examinations would be to determine if classified or confidential material had been passed to any unauthorized individuals. He also stated that the polygraph examinations would focus on broad security concerns, rather than the threat that had been alleged by Edmonds.

On March 7, the day before her polygraph, Edmonds met with a higherlevel FBI official who listened to Edmonds repeat her allegations and then thanked her for the information. This official then contacted a manager in Edmonds' supervisory chain, who told the official that the matter was being looked into by the FBI, including by the FBI's Office of Professional Responsibility (OPR).17 The official with whom Edmonds met took no further action.

17 That same day, Edmonds contacted FBI OPR and the OIG to report her allegations. Because the OIG opened its investigation shortly after FBI OPR was contacted, FBI OPR did not pursue the matter further.

On March 8, Edmonds took the polygraph examination. The polygraph questions asked of her related to whether she had disclosed classified information to unauthorized persons and whether she was maintaining classified information outside FBI office space. She denied those charges, and the polygrapher concluded that she was not deceptive in her answers.

The co-worker was polygraphed on March 21. The co-worker was asked about her activities. The co-worker denied having engaged in inappropriate activities. The polygrapher concluded that the co-worker was not deceptive in these answers.

The Security Officer and other FBI managers later expressed disappointment with the questions asked in the polygraphs. The Security Officer said the questions were not responsive to the allegations raised by Edmonds. An FBI manager said that the polygraphs should have been "customized" to obtain optimal results and that he was hoping the polygraphs would be more conclusive in the investigation of these allegations. The Chief of the Polygraph Unit later told the analyst that more precise questions could have been asked.

We also concluded that the polygraph examinations of Edmonds and the co-worker were not ideal. In addition, we found that despite the concerns about the polygraph, the FBI never considered doing any additional polygraphs and continued to rely on the polygraph as support for its position that Edmonds' allegations were unfounded.

H. Additional Complaints

Between February 8 and March 22 (the day the FBI stopped using her services), Edmonds' relationship with FBI management deteriorated significantly. By the end of February, the Language Supervisor was becoming increasingly frustrated with Edmonds' allegations. For

example, on March 5 the Language Supervisor began taking detailed notes of all his interactions with Edmonds.

At the same time, Edmonds seemed to become increasingly frustrated. In addition to meeting frequently with the Language Supervisor about her suspicions, Edmonds wrote numerous e-mails and memoranda raising additional complaints. Edmonds also warned the Language Supervisor of the penalties for retaliation against a Whistleblower. Edmonds also requested information about any allegation made against her. The Language Supervisor declined to provide the information requested by Edmonds.

On March 8, Edmonds complained that work she had been asked to translate had not been loaded properly onto her computer, and that FBI Special Agents had been waiting for the translations for three weeks. The Language Supervisor responded that since February 22, 2002, Edmonds had only worked one day, on March 8,2002. The Language Supervisor also stated that Edmonds did not indicate which work she was referring to until March 5, 2002, when she was in the office briefly. In response, Edmonds repeatedly complained to the Language Supervisor about the fact that she never was provided information about the polygraph or the allegations against her.

On March 15, the relationship between the Language Supervisor and Edmonds became even more tense. Edmonds asked the Language Supervisor why the Special Agent who she assisted had not been in contact with her in over a month. Edmonds also inquired about her work assignments. The Language Supervisor responded that he did not know why the Special Agent had not met with Edmonds and that, due to Edmonds' limited work hours and the need to have certain work assignments completed, he had requested that linguistic resources be reallocated. In response, Edmonds stated that in the past few weeks, "coincidental" to her reports of wrongdoing, she had received no new assignment and no offers of temporary duty (TDY) assignments.

Later that day, the Language Supervisor informed Edmonds that he would not submit for payment an invoice of Edmonds' that included 5.25 hours spent in meetings related to her allegations. Before advising Edmonds that he would not submit the invoice, the Language Supervisor consulted with the FBI contracting office and was told that CLs are paid only for "actual hours worked." Edmonds ultimately disputed this decision, and the FBI relented and paid her for the time.

Also on March 15, Edmonds made a claim to the Language Supervisor about time and attendance abuse by the co-worker. The Language Supervisor subsequently found no abuse, but sent out an e-mail reminding the linguists to sign out as they leave for the night, rather than annotating it the next day.

In addition, Edmonds reiterated a number of her security concerns and asserted that she was being obstructed and retaliated against for her complaints. She also alleged that documents had "disappeared" from the location where she kept her work papers. The Language Supervisor asked for a list of the missing items. Edmonds requested a secure location for her documents, commenting that requiring her to keep her documents in a location accessible by those whom she had accused of wrongdoing was ridiculous.

Edmonds also wrote that the Language Supervisor had told her that the Special Agent was unhappy with her performance and personality and he did not want to deal further with

Edmonds. Edmonds requested a IS-minute meeting with the Special Agent and the Language Supervisor to iron out any issues and re-establish a proper working relationship.

In a lengthy EC the Language Supervisor wrote on March 19 to an FBI manager and the Security Office, the Language Supervisor denied ever telling Edmonds that the Special Agent was unhappy with her work. However, the Language Supervisor also said that the Special Agent would not meet with Edmonds because he had been instructed not to do so due to Edmonds' fabrications.

On March 19, a Supervisory Special Agent wrote that he did not want to use Edmonds' translation services anymore because she had been a complete disruption to the office, often making groundless accusations. The Supervisory Special Agent said that he already had devoted too much time to the matter, and he had lost faith in Edmonds' ability to carry out her assignments. He cited her security violation and recommended that Edmonds be removed from working his assignments in light of security concerns and some other "agenda" she was pursuing.

Tension between Edmonds and her colleagues also increased during this period. On March 20, the Language Supervisor noted that he had to act as an intermediary of behalf of Edmonds with others due to these tensions. The Language Supervisor also expressed frustration with Edmonds' impatience at the time it took to resolve her allegations, writing that Edmonds did not seem to the Language Supervisor to understand that he had more pressing issues to deal with at times.

Edmonds again wrote to the Language Supervisor on March 22 alleging that the co-worker had cheated on the co-worker's timesheet. In fact, the coworker was out of the office for her polygraph examination during the time period Edmonds questioned. The Language Supervisor told Edmonds via e-mail that Edmonds did not have all the facts and instructed Edmonds not to mark on anyone's time sheet but her own.

I. FBI's Decision to Stop Using Edmonds' Services

As described above, after the February 22 meeting with Edmonds, an FBI manager began inquiring about the FBI's options with respect to the "use/nonuse" oflinguist contractors. On February 26, the FBI Contracting Officer for the General Contracting Unit of the Finance Division informed this manager that, if it was determined that a CL was "unsuitable," the FBI would have sufficient reason to terminate her contract.

By March 20, the FBI manager had drafted an EC recommending that his office discontinue using Edmonds' services. In the introductory paragraph he mentioned that Edmonds had raised issues concerning security, performance, and favoritism. Without further discussion of Edmonds' individual allegations, he wrote that the Security Office's inquiry had concluded that some allegations of Edmonds were not substantiated and that she had not been completely forthcoming about the extent of the sensitive and classified information on her home computer. In the EC, the manager said he found it most telling that Edmonds had written to other high-level FBI officials nine days before his first meeting with her, and he commented that Edmonds seemed inclined to put forth additional complaints, as the discussion continued, that were not mentioned previously. He wrote that she had a propensity to inflate and misstate facts, and he described the tone of her letters to the Language Supervisor as condescending and somewhat threatening. The manager also noted

in the EC his frustration at the pace of efforts by the Security Office to resolve the matter in a clear-cut manner [i.e., to revoke Edmonds' security clearance]. He remarked that Edmonds was using her newly claimed whistle blower status as a "club" against her supervisors. He concluded that no action taken by his office would be satisfactory to Edmonds. He recommended that LSS immediately discontinue using her as a linguist, and that her FBI access badge be cancelled and taken until "this situation" was resolved. The manager e-mailed the draft of his EC on March 20 to the LAAU Chief and others.

The following day, the FBI manager issued the final EC, which was substantially less harsh in tone, and to which he had added the statement that Edmonds had a "disruptive effect" on operational matters. The final EC also omitted the manager's earlier comments that Edmonds was not completely forthcoming about the extent of the sensitive and classified information on her home computer, that she had a propensity to inflate and misstate facts, and that she was using her Whistleblower status as a "club." He also removed the comment he had made about her appeals to other FBI officials.

The final EC also contained additional recommendations. First, the manager recommended that Language Supervisors and higher-level Security officials be apprised of the actions being taken. Second, he recommended that Edmonds be debriefed regarding her future responsibility not to disclose classified information and the criminal penalties that apply to such disclosures, and that her clearance be re-adjudicated. Third, he recommended that the Security Office complete its pending investigation and refer any findings for administrative or disciplinary action, or for further substantive investigation.

On March 22, FBI managers met with Edmonds and told her that her services would no longer be used by the FBI. One manager reminded her of the requirements of the Security Acknowledgement Form. Edmonds told the OIG that the meeting was hostile and that one manager threatened her with jail. FBI managers denied that the meeting was hostile or that Edmonds was threatened with jail.18

18 When the GIG asked the manager whether anyone at any time during the meeting told Edmonds she could go to jail, he said he thought it was implied in the Security Acknowledgement Form. However, he denied telling Edmonds, as she alleged, that the next time they saw her it would be in jail. Another manager denied that there was any discussion of Edmonds possibly going to jail.

Prior to being escorted out of the building, Edmonds gave the Language Supervisor and Security Officer a memorandum that documented additional performance problems related to the co-worker, which Edmonds considered to be additional support for her underlying security concerns. 19

The Language Supervisor subsequently requested verification of the facts Edmonds put into this memorandum. The follow-up confirmed that Edmonds' description of the facts was accurate, but the Language Supervisor took no further action.

Edmonds was then escorted out of the building by FBI personnel and her access badge was taken.

J. Security Office's Damage Assessment

Shortly after her termination, additional allegations of security violations were made against Edmonds, including an allegation that Edmonds had discussed classified information outside the FBI with unauthorized persons at a social setting, and that Edmonds put a copy of the March 22 memorandum she gave to the Language Supervisor into an envelope for delivery to the OIG and OPR, although neither the memorandum nor the envelope contained the required classification markings.

On March 26, the Security Officer drafted an EC with the heading, "Damage assessment conducted and provided to FBIHQ regarding the processing of classified information on the home computer of a contract linguist." He recommended revocation of Edmonds' security clearance. The Security Officer wrote that the Security Office considered it a threat to national security to continue to allow Edmonds access to classified information.

The Security Officer's EC was not finalized until May 2,2002, because he and his supervisor disagreed about its contents. According to the Security Officer, the supervisor took the position that Edmonds' security clearance should be "re-adjudicated" by the proper authorities at FBI Headquarters. The final version of the EC stated that the Security Office "questions" Edmonds' trustworthiness with sensitive national security information, based on her having processed classified information on her home computer and because she was seen putting a memorandum containing classified information into an envelope for delivery to the OIG and OPR, without the proper markings. The EC recommended that she not be used for classified translation duties with the FBI and that her clearance be re-adjudicated.20

20 The Security Office's May 2 EC recommending re-adjudication of Edmonds' clearance failed to point out that the polygraph results undercut the claim that she had discussed classified information outside the FBI with unauthorized persons at a social setting.

K. Subsequent Review by FBI Security Officials

In May 2002, after the media and Congress began making inquiries about Edmonds' allegations, the Section Chief of the Personnel Security Section in the FBI Security Division asked one of his unit chiefs to take a look at this matter. The unit chief assigned an Investigative Analyst Consultant with the Security Division to gather information about the case.

During the course of the analyst's work, he wrote two memoranda. The first, written June 4, 2002, stated that Edmonds had been "suspended" and that she had committed three security violations: the two classified memoranda written on her home computer (the February 8 memorandum and the memorandum found during the analysis of Edmonds' computer) and the discussion of classified information outside the FBI with unauthorized persons at a social setting. However, the analyst's memorandum noted that she was not fired for security reasons and her clearance had not been revoked. The memorandum then summarized the allegations against Edmonds, Edmonds' allegations against the co-worker, and the Security Officer's investigation.

The analyst conducted additional investigation and found substantial flaws in the Security Officer's investigation. In a second memorandum, dated June 14, 2002, the analyst described the inaccuracies and flaws in the Security Officer's investigation. As a result,

another Security Officer interviewed the co-worker again. The co-worker stated that the co-worker was mistaken about some facts in the original interview, but the co-worker also disputed the accuracy of a portion of the write-up of the initial interview.

The analyst's review also noted that the polygraphs were not as precise as they could have been because the polygraphs focused on broad security concerns, rather than the precise issues Edmonds had raised. The analyst reported that the Polygraph Unit Chief admitted that questions directly on point could have been asked but were not. However, the Polygraph Unit Chief asserted to the analyst that the more generic question "would have elicited a discernible reaction."

Despite the fact that the analyst's review unearthed these problems with the Security Officer's investigation, FBI Security officials did not request any further review or re-investigate Edmonds' allegations.21 We found that the analyst's review revealed substantial infirmities in the Security Officer's investigation at that time. Nevertheless, higher-level FBI Security officials failed to initiate a more thorough investigation. As noted above, we believe ample basis existed for such a review.

21 The analyst's two memoranda later were used as the basis for talking points provided to the head of the Security Division, who briefed several Congressional staff members about the Edmonds case on June 17, 2002. The briefing was unclassified because a staffer at the briefing lacked the appropriate security clearance. During the course of the briefing, the Security Section Chief inadvertently revealed what the FBI considered to be classified information.

In sum, we believe the FBI's initial inquiries in response to Edmonds' allegations were seriously deficient. Had they been more thorough, an appropriately focused analysis could have been conducted much earlier. Moreover, even when the FBI was notified of additional information, the FBI still did not promptly document and act on the information provided. The remedial action taken to address one aspect of Edmonds' concerns was not sufficiently thorough, and the FBI reversed itself prematurely. This was an inadequate response under the circumstances.

We also note that, at the time of these events, the FBI had no protocol for the receipt and investigation of derogatory information provided by someone within the FBI about a co-worker. In May 2002 (after Edmonds was terminated), in response to the Hanssen case, the FBI created a new counterespionage section, CD-4, to investigate allegations of espionage, including all allegations of penetrations of the U.S. Government. According to the Chief of CD-4, however, if Edmonds' allegations were made today, they might still be investigated by the Security Office. But he said that at a minimum the Security Office should consult with CD-4 during the investigation.

VI. OTHER ALLEGATIONS

Edmonds made additional allegations to the OIG regarding the foreign language translation program. She claimed, for example, that she was directed to slow down the pace of her work so that material would pile up and the FBI would have a basis to request more translators. Edmonds alleged that the FBI hired an unqualified translator because of his connection to FBI Headquarters' personnel and subsequently sent him to translate military interviews despite his weak language skills. In addition, Edmonds claimed that travel

voucher abuse was condoned and that supervisors improperly received gifts from subordinates. In our full report, we reviewed the facts and conclusions regarding these and additional allegations. In this section, we briefly summarize our core findings.

A. Alleged Slow Down of Work

Edmonds alleged that shortly after she began work for the FBI, linguists were directed to slow the pace of their work so that the material to be translated would "pile up" and the FBI would have a basis to request more translators. Edmonds also said that she was reprimanded for working too quickly. Edmonds provided the OIG with the names of several linguists whom she believed had heard these instructions.

The persons supervising Edmonds denied ever telling Edmonds or any other linguist to slow down so that more linguists would be hired. Instructions to slow down, the OIG was told, only were given if a linguist's pace was adversely affecting the quality of the linguist's work. The OIG was told that such an instruction was never given to Edmonds because the quality of her work was good.

The OIG interviewed ten linguists who were either named by Edmonds in her allegations or were named by Edmonds as having information relevant to her allegations, including those whom Edmonds specifically stated could corroborate her allegation regarding the alleged instruction to slow down. Only three of these linguists stated that they recalled hearing about the alleged instruction to slow down. Two said they heard the allegation only from Edmonds. The third said that she had heard about the slow down instruction from others in addition to hearing about it from Edmonds, but said she could not recall who those others were. The other seven denied ever hearing about such an instruction.

We found insufficient evidence to substantiate Edmonds' allegation that such time and attendance abuse was condoned or occurred. Moreover, given the backlog of translation work at the FBI, we do not believe the FBI would need to intentionally slow down the linguists' work to support hiring additional translators.

B. Hiring and Assignment of an Unqualified Translator

Edmonds told the GIG that the FBI hired a contract monitor based on the person's personal connections to the FBI, even though he had not scored high enough on the language tests to qualify for the position. Edmonds also questioned the fact that this CM was assigned to translate military interviews despite weak language skills.

The GIG concluded that the CM was hired and assigned to translate military interviews even though he did not meet the minimum passing score for the position. The FBI took this action without following appropriate written procedures, and without notifying appropriate officials who supervised the CM's work, and in a manner that created the appearance of a conflict of interest. Although the CM ultimately demonstrated that he could meet the minimum requirements, we found that he clearly had difficulties with his written translation work for the FBI. However, it appears that those supervising the military interviews he helped to translate were satisfied with his translation work.

C. Travel Voucher Fraud

Edmonds alleged that a supervisor made arrangements for two linguists to "switch" work locations, at FBI expense. FBI travel records reflect that on at least three occasions, two linguists who translate the same language did "swap" work locations at FBI expense. These three "temporary duty" assignments cost the FBI over $35,000 in travel reimbursements.

After initially asserting that the swap was necessary for proper coverage of the translation work of the office, the FBI supervisor could not explain why it was necessary to have both linguists travel at such expense, when the translation work of the two linguists could have been moved from one location to the other over the FBI's computer system. He provided to the GIG an EC in which, he stated, his supervisor approved this arrangement. The document, however, is dated many years earlier and refers to one 60-day temporary duty assignment for a linguist who had been working on the same project years earlier.

Edmonds alleged that this "swapping" arrangement was due in part to favoritism on the part of the supervisor. One linguist told the OIG that he had also heard rumors of favoritism. The supervisor adamantly denied any favoritism towards any of the linguists. No other witness stated that he heard similar rumors, and the OIG found no other evidence of any such favoritism.

We believe that the arrangement was wasteful. At the time these two linguists swapped places, other linguists were available to handle this work in both locations. We do not believe the EC provided to us by the supervisor applies to the time period in which we found evidence of wasteful travel. Moreover, the supervisor provided no explanation for the failure to use the FBI's computer system to send the work electronically between offices.

D. Additional Travel-Related Allegations

Edmonds made additional allegations related to misuse of travel vouchers. She claimed, for example, that some linguists had gone to a distant location to attend a concert and had been improperly reimbursed by the FBI for this travel. She did not identify the particular linguists. The OIG examined FBI travel records and found that only one linguist traveled at FBI expense to the location of the concert during the relevant time period, but this linguist stated that he did not attend the performance. We reviewed documentation that supported this linguist's assertion that this was a legitimate business trip.

Edmonds also alleged that a supervisor traveled to particular cities at FBI expense in order to attend a seminar, visit a sick relative, and visit other family members. The OIG reviewed the supervisor's travel records dating back to October 1, 1999, and found no trips to the cities mentioned by Edmonds.

Edmonds also claimed that when another linguist traveled to perform translation work, a supervisor permitted him to stay through the weekend at FBI expense so that he could do some personal shopping and bring items back for the supervisor. FBI travel documents reflect that at the time Edmonds made her allegations, the linguist in question had made two trips to the location Edmonds cited, at FBI expense. On one of those trips, the linguist stayed over on a Friday night and returned the next day. The FBI paid for the hotel on Friday night. FBI records show that the linguist worked until 5:00 p.m. If he had returned that day, he would have arrived late in the evening. He therefore stayed overnight and returned on Saturday. He acknowledged buying gifts while he was on the trip to give to the supervisor and other friends and co-workers.22 However, the linguist denied staying

overnight on Friday for the purpose of shopping for himself or the supervisor. The supervisor denied sending the linguist on travel to shop.

22 The gifts he purchased are discussed in the next section.

In sum, we found the allegations regarding travel for concerts, shopping, or family visits were unsubstantiated.

E. Improper Receipt of Gifts by Supervisors

Edmonds alleged that FBI language supervisors received expensive gifts from subordinates. The only specific example she provided to the GIG was that, on his return, the same linguist who she said had been permitted to stay on travel so that he could shop brought back sets of ladies' and men's watches for the supervisors. Edmonds said the linguist had told her that the watches cost him $135, and that the supervisor who approved the extension of the travel asked the linguist to give the same sets of watches to the other supervisors so that "no one will ever talk." Edmonds said that the linguist also gave her a set of the watches, but she returned them.

The linguist told the GIG that he bought several sets of the watches while he was on the trip, for $10 each, and that he gave the sets to Edmonds, three supervisors, and a Special Agent. He denied telling Edmonds that the watches cost $135, and denied saying that a supervisor instructed him to give the same gift to other supervisors so that no one would talk.

The GIG was unable to determine the specific value of the watches, but they do not appear to be expensive watches. We found that the same brand of watches was advertised on the Internet for $4.90 per set. In addition, ajeweler told the GIG that the watches do not contain a karat mark, indicating that they do not contain any gold. The jeweler said that he had seen similar watches for sale by street vendors. He estimated that the watches could be worth anywhere from $20 to $100.

The GIG interviewed ten linguists and four supervisors who work in the same office. None told the GIG that subordinates gave "expensive" gifts to supervisors. Several witnesses stated, however, that linguists frequently gave their supervisors and colleagues small food items or trinkets that they had purchased while traveling on FBI business. A supervisor told the GIG that he had received from the linguists under his supervision many such items, including key chains, shot glasses, worry beads, brass plates, coffee mugs, a clock, and a stone from the Berlin Wall. The supervisor told the GIG that he always tells the linguists that he cannot accept a gift worth more than $20. Another supervisor told the GIG that he had accepted small gifts from the linguists because to refuse them would be a "cultural affront" and the linguists are aware that the gifts must cost less than $10.

The FBI MAGP provides that a supervisor may not accept a gift from a subordinate employee who receives less pay than the supervisor. A supervisor may accept from subordinates voluntary gifts of a nominal value made on a special occasion such as marriage, illness, or retirement. A supervisor may also accept gifts worth less than $10 on "on an occasional basis, including any occasion on which gifts are traditionally given or exchanged," such as holidays. MAOP, Part 1, Section 13.1. This provision of the MAOP is the same as the DOJ regulation prohibiting gifts from subordinates to supervisors. 5 C.F.R.

§ 2635.302 and 304.

We found insufficient evidence to substantiate Edmonds' allegation that a supervisor received expensive gifts from subordinates. We also found that the practice of giving gifts to supervisors was widespread in LSS, was not limited to special occasions such as marriage, illness, or retirement, and occurred on more than "an occasional basis." Although we found no proof that supervisors received items worth more than $10 on any occasion, we believe the commonplace acceptance of gifts from subordinates violates the FBI MAOP. Indeed, the commentary to the DOJ regulation upon which the MAOP provision is based specifically states that an employee "whose job responsibilities require frequent travel may not bring her supervisor, and her supervisor may not accept, souvenir coffee mugs from each of the cities she visits in the course of performing her duties, even though each of the mugs costs less than $5. Gifts given on this basis are not occasional." 26 C.F.R. § 2635.304 (a), Example 2. Accordingly, we believe the FBI should instruct supervisors and linguists to stop the practice of supervisors accepting gifts from linguists.

F. Unauthorized Disclosure of Information to Congress

The OIG also received an allegation from the FBI of a possible "unauthorized disclosure of classified information to a congressional staffer." The OIG found that on June 17,2002, the Section Chief of the Personnel Security Section in the Security Division conducted a briefing regarding Edmonds' allegations for congressional staff members. Because one of the congressional staff members present lacked the appropriate security clearance, the briefing was unclassified. The Security Section Chief inadvertently used a term which, according to the FBI, could have the effect of revealing classified information. 23

23 This briefing recently has become the subject of congressional complaints regarding retroactive classification of information by the DOJ.

We found that the Security Section Chiefs use of the term during the briefing was inadvertent. However, we believe this incident demonstrates the problems inherent in attempting to "talk around" classified information.

VII. EDMONDS' CLAIM OF RETALIATION

As described in this report, on March 22, 2002, an FBI manager notified Edmonds that her translation services would no longer be needed and took her access badge from her. On April 2, the FBI sent a letter to Edmonds terminating her contract as of March 26. Edmonds has claimed that her termination was in retaliation for her raising allegations of misconduct to the FBI.

Edmonds does not qualify for "Whistle blower" status under the FBI Whistleblower regulations because she was a contractor, not an FBI employee. See 28 C.F.R. § 27.1(a). However, in examining the question of whether the FBI retaliated against Edmonds because of her allegations of misconduct, we used the principles underlying these regulations.

Pursuant to these regulations, the FBI cannot take a personnel action against an employee in retaliation for any "protected disclosure" the employee has made. 28 C.F.R. § 27.2. For a disclosure to be "protected" under the regulations, it must be made to the OIG, DOJ OPR, FBI OPR, the Attorney General, the Director of the FBI, the Deputy Director of the FBI, or

the highest ranking official in any FBI field office. 28 C.F.R. § 27.1(a). In addition, the employee making the disclosure must reasonably believe the disclosure evidences a violation of law, rule, or regulation; mismanagement, a gross waste of funds, an abuse of authority; or a substantial and specific danger to public health or safety. 28 C.F.R. § 27.1 (a). The complainant has the burden of showing by a preponderance of the evidence that her protected disclosure was a contributing factor in the decision to take the personnel action. Once that showing is made, the burden shifts to the agency to show by clear and convincing evidence that it would have taken the personnel action against the complainant in the absence of the protected disclosure. Id. at § 27.5(e)(2).

Edmonds' allegations would clearly qualify as protected disclosures under the FBI Whistleblower regulations. Thus, the key issue would be whether her disclosures were a "contributing factor" in the termination of her services. Under the Whistleblower regulations, the FBI would have to prove by clear and convincing evidence that it would have taken the same action absent her disclosures.

We believe the evidence indicates that the FBI could not show, by clear and convincing evidence, that at the time the decision was made it would have terminated Edmonds' contract absent her disclosures. According to an EC from an FBI manager that summarizes the reasons for terminating Edmonds' services, the FBI's primary reasons were that she represented a "disruptive effect" on operational matters and her "documented" mishandling of classified information at her residence.

The mishandling of classified information on her home computer related to Edmonds' writing, at her supervisor's request, a memorandum describing her allegations of misconduct and including classified information in that memorandum. However, a Security Official told the OIG that he did not believe the Security Office had enough information to "fire" Edmonds based on her security violation of processing classified information on her home computer. Similarly, the Security Officer who conducted the investigation told the OIG he did not view Edmonds' security breach as intentional and said the FBI did not intend to pursue administrative charges against Edmonds for the violation.

Rather, the primary reason for the FBI's termination of Edmonds related to the claim that she had a "disruptive effect" on operational matters. This disruption related primarily to Edmonds' aggressive pursuit of her allegations of misconduct, which the FBI did not believe were supported and which it did not adequately investigate. In fact, as we described throughout our report, many of her allegations had bases in fact and should have been more thoroughly investigated by the FBI. We believe that the FBI's failure to handle her allegations adequately contributed to Edmonds' increasingly vociferous complaints, which ultimately led to the termination of her services.

We also recognize that Edmonds was not an easy employee to manage, and that some of her complaints, based on her self-initiated reviews, were unsupported and a distraction to her supervisors. Edmonds also aggressively asserted her opinions about the management of the translation program, which was frustrating to her supervisors. But we believe that many of her allegations were supported, that the FBI did not take them seriously enough, and that her allegations were, in fact, the most significant factor in the FBI's decision to terminate her services.

In addition, the FBI has not asserted that Edmonds' contract was terminated because it had no further need of her services. In fact, the Chief of LSS told the OIG that there has been no

reduction in the need for linguists to translate the language Edmonds translated. Indeed, at the time Edmonds' services were terminated, there remained a need for such services.

We also believe the FBI could have handled the matter much more effectively than it did. For example, as an LSS Unit Chief suggested, the FBI could have moved Edmonds to another location while it pursued a thorough investigation of Edmonds' allegations. Had it done so, the "disruptive effect" on operational activities created by Edmonds' persistent complaints could have been avoided or at least minimized.

In sum, while Edmonds does not fall within the protection of the FBI's Whistleblower regulations, we believe that the FBI significantly mishandled this matter. The FBI should not discourage employees or contractors from raising good-faith allegations of misconduct or mismanagement. By terminating Edmonds'services, in large part because of her allegations of misconduct, the FBI's actions also may have the effect of discouraging others from raising concerns.24

In response to a draft of this report, the FBI expressed disagreement with this conclusion. A copy of the FBI's response to the OIG is attached as Appendix C.

VIII. OIG RECOMMENDATIONS

In light of the issues that we examined in this case, particularly the issues relating to Edmonds allegations regarding the co-worker, we are providing systemic recommendations to the FBI in an attempt to help it improve its foreign language translation program.25

25 One recommendation was removed in its entirety because it contained classified information.

1. The FBI should consider having an employee from the LSS or a case agent from the relevant squad interview CLs before they are hired by the FBI. The FBI's hiring process for CLs includes both language testing and a full background investigation. Although the background investigation includes a Personnel Security Interview designed to obtain information relevant to the security clearance, CLs are not interviewed by employees from the LSS or operational agents before being hired. As a result, the supervisors of CLs or CMs never have an opportunity to meet with the linguist and explore any issues relating to their qualifications and background. While we recognize that these linguists are used on a contract basis only, we believe the FBI should consider including an interview during the hiring process for CLs and CMs. Such an interview could include the applicant's future supervisor or a case agent from a relevant operational squad.

2. The FBI should establish written guidelines for when risk assessments should be performed in background investigations. The FBI failed to conduct a risk assessment of the co-worker during her background investigation. We believe the FBI should create written guidelines that clearly state the factors to be weighed when deciding whether a risk assessment is necessary in a particular case.

3. The FBI should provide written guidelines to linguists to assist them in reviewing materials. The CLs we interviewed said they received oral training from case agents and other linguists. However, they did not receive any written guidance

regarding reviewing materials. We recognize that many cases are different, and what applies to one case may not apply to another, but we believe that generalized guidance would be useful to help ensure that CLs have a common understanding of their work requirements when reviewing materials. We recommend that general guidelines be provided to all linguists, in writing, when they are hired by the FBI.

4. The FBI should ensure that supervisors determine the assignment of material that linguists will review. The FBI should ensure that supervisors assign material for linguists to review. Failure to assign material creates potential security risks and also contributed to the conflict that arose between linguists in this case. We were told by Language Services Section supervisors that these decisions should not be left to the linguists.

5. The FBI should establish a uniform policy with regard to work assignment sheets for linguists. In the LSS, work assignment sheets that should contain the signatures of the translator, reviewer, and editor who worked on a particular translation are destroyed after the information is entered into a database. We also were told that the practice with respect to the signatures on these forms is not uniform. For example, some individuals only put a checkmark by their name when they complete the assignment, while others simply forward the sheet without marking it in any way . We recommend that the FBI establish and enforce a uniform policy requiring signatures on work assignment sheets, and that it maintain those sheets for a reasonable period of time so that issues relating to a particular translation can be addressed adequately.

6. The FBI should implement a system to track which linguist reviews which material. We found that, because of resource issues, more than one linguist may be assigned to a particular task. While the LSS computer system keeps track of the last person to work on a particular task, that information may be overwritten or lost if a second person later works on the same task. Although the work product of an individual linguist provides some indication of which tasks that linguist carried out, there is no method to establish, with certainty, which linguist reviewed which material.

A Language Services supervisor stated that one of the linguists he supervises had developed a practice of keeping track of all the material he reviews. The supervisor said that when the linguist finishes work each day, he transfers this information to the relevant case agents along with the other work completed. In this manner, the agents have a clearer picture of the case. In addition, the supervisor said that extending this practice might cause less attentive linguists to take more care in their work. We recommend that the FBI consider implementing this or some other practice to ensure that the FBI has a record of work completed on a particular task. In addition, the FBI should evaluate the feasibility of installing audit trails to preserve a record of each person who worked on a particular task.

7. The FBI should reinforce ethics rules regarding gifts to supervisors. We found that the practice of giving small gifts to language supervisors was widespread, and was not limited to special occasions such as marriage, illness, or retirement. We believe the FBI should reiterate the ethics rules regarding gifts and specifically instruct language supervisors and linguists to stop the practice of supervisors regularly accepting gifts from linguists.

IX. CONCLUSION

The majority of the allegations raised by Edmonds related to the actions of a co-worker. The allegations raised serious concerns that, if true, could potentially have extremely damaging consequences for the FBI. These allegations warranted a thorough and careful review by the FBI.

Our investigation concluded that the FBI did not, and still has not, adequately investigated these allegations. Our review also found that many - although not all - of Edmonds' allegations about the co-worker had some basis in fact. This evidence does not prove, and we are not suggesting, that there is sufficient evidence to conclude that espionage or any improper disclosures of FBI information occurred. However, we believe the FBI should have taken Edmonds' allegations more seriously and investigated them more thoroughly. As discussed in this report, the FBI's investigation of the information regarding the co-worker was significantly flawed. Had the FBI investigated the claims thoroughly, it would have found that many of Edmonds' allegations regarding the co-worker were supported by documentary evidence or other witnesses. Instead, the FBI seems to have discounted Edmonds' allegations, believing she was a disruptive influence and not credible, and eventually terminated her services. Even now, the FBI has not carefully investigated the allegations about the co-worker to determine if the co-worker compromised any FBI information. In light of the need for FBI vigilance about security issues, as demonstrated by the Hanssen case, we believe the FBI should have investigated these serious allegations more thoroughly.

Edmonds also alleged that the FBI retaliated against her by terminating her services as a CL. We concluded that Edmonds' allegations were at least a contributing factor in why the FBI terminated her services. We recognize that the FBI Whistle blower regulations do not apply to Edmonds because she was a contractor rather than an FBI employee. We also recognize that her varied and insistent allegations of misconduct may have been frustrating, and that not all of her allegations were true. However, many of her allegations had a basis in fact, and the way the FBI responded to her allegations contributed to her persistent claims. Moreover, we believe the FBI should not discourage employees or contractors from raising good-faith allegations of misconduct or mismanagement and the FBI's termination of Edmonds' services may discourage others from raising such concerns.

With regard to Edmonds' other allegations of misconduct, most were not supported by the evidence we reviewed. However, she did raise a valid concern about unnecessary travel for certain linguists.

Finally, our review also found problems in the oversight of FBI CLs. The FBI needs to more carefully oversee and monitor their work. Towards this end, we made several recommendations regarding the FBI's hiring and oversight of CLs. We believe that the FBI should carefully consider these recommendations, which we believe could help improve the operation of the FBI's language translation program.

Appendix A: FBI Organizational Chart

Appendix B: FBI Language Services Section Organizational Chart

Appendix C: FBI Response to OIG Report

Source: DoJ PDF Version

Ms. EDMONDS. Thank you.

In the summer of 2002, I also began to pursue legal remedies to challenge my unjust dismissal under First Amendment and Privacy Act, and also under the Freedom of Information Act. Rather than respond to the merits of my claim, in October 2002, Attorney General Ashcroft asserted a rarely invoked state secret privilege, arguing that the entire case must be dismissed in the name of national security, even if my allegations were correct. According to the state secret privilege that they invoked, everything about my case, everything about it was considered classified and it could not be argued in court.

The Department of Justice asked the court to try the case without any hearings, without any depositions or discovery. Even though the Department of Justice's own Inspector General had confirmed the seriousness of my allegation, and concluded that I was fired for raising them, the DOJ still continued to insist that my case cannot go forward because it would jeopardize national security. So far, the Department of Justice has been successful in this effort to silence these court cases.

In June 2004, the court ruled in favor of this far-reaching assertion of the state secrets privilege. Currently I am applying this case and the Department of Justice is still invoking the state secret privilege.

The Government invoked the state secret privilege a second time in an attempt to block me from being deposed in a case brought by families of those killed on September 11 against Saudi individuals and entities alleged to have financed Al-Qaeda. The Government insisted that almost every single question that the families wished to ask would require the disclosure of classified information.

The problems I have reported have serious consequences to our national security and have already been confirmed by the IG report and the inquiry of Senators Grassley and Leahy. Translation units are the front line in gathering, translating and disseminating intelligence. A warning in advance of the next terrorist attack may and probably will come in the form of a message or a document in a foreign language that will have to be translated. If an attack then occurs which could have been prevented by acting on information in such a message, who will tell family members of the new terrorist attack victims that nothing more could have been done? There will be no excuse that we did not know, because we do know today.

Yet knowing full well the seriousness of these confirmed issues and problems, rather than addressing them, the FBI and the Department of Justice spend time and effort to cover them up by overuse of secrecy and excessive classification. Contrary to their claims, they seem to be far more concerned with avoiding accountability than protecting our national security. I believe that my case clearly illustrates the Federal Government's capricious use of secrecy laws and classification to cover up problems and wrongdoing and to avoid accountability.

Thank you again for inviting me to testify today. You are the first congressional committee after 3 years to request my testimony and hear my story. I believe this testimony is a good first step in examining the situation. But what is really needed is an actual

congressional investigation. Therefore, with respect for your critical role in our Constitutional system of checks and balances, I request that you be the first congressional committee to investigate not just my case but what is going on over there at the FBI and the Justice Department regarding the very serious problem of overclassification and the abuse of secrecy.

Thank you.

[The prepared statement of Ms. Edmonds follows:]

Statement of Sibel Edmonds
Before the House Committee on Government Reform,
Subcommittee on National Security, Emerging Threats and Internal Relations
March 2, 2005

Emerging Threats: Overclassification and Pseudo-classification

Good afternoon, my name is Sibel Edmonds. I have been invited to provide you with testimony today regarding my direct experience with the use of excessive secrecy, rare privileges, and over-classification by the Department of Justice against me during the past three years. Thank you for giving me this opportunity. I believe that my case clearly illustrates how the government uses secrecy laws and classification to avoid accountability, to cover up problems and wrongdoing, and to gain unfair legal advantage in court.

I began working for the Federal Bureau of Investigation (FBI) as a language specialist for several Middle Eastern languages starting shortly after 9/11, and was granted Top Secret Clearance. During my work, I became aware of problems within the translation unit involving criminal conduct against our national interests, potential espionage, serious security breaches threatening our intelligence, intentional mistranslation, and blocking of intelligence. I was asked, and later ordered, to refrain from reporting these allegations. I reported them, together with evidence, to higher management within the bureau. They refused to take any action, and again, they asked me not to pursue them. I then took these issues and evidence to the Department of Justice Office of the Inspector General and to the Senate Judiciary Committee, because I believed that according to our laws these were the appropriate steps to take in this situation. As a result, I was retaliated against, was ordered to submit to a polygraph, and had my home computer confiscated. Finally, in March 2002 I was fired. The only explanation I received for getting fired was 'for the convenience of the government.'

In March 2002, the Senate Judiciary Committee began investigating my case and allegations, and in June and July 2002, during two unclassified briefings with the staff of Senators Grassley and Senator Leahy, the FBI publicly confirmed all of my core allegations. These two Senators issued public statements and letters regarding these confirmations and my case, demanding expedited investigation by the Inspector General and response from the FBI. These letters and statements were widely disseminated in the media and on the Internet; including on the Senators' own websites. When the judge overseeing my legal cases asked the government to produce any unclassified materials that was relevant to the substance of my allegations, the government took a truly extraordinary step: it moved to *retroactively* classify these letters, statements, and news releases that had been public for almost two years. It is quite clear that the government's motivation was not to protect national security, but rather to protect itself from embarrassment and accountability. Senator Grassley characterized this retroactive classification as 'ludicrous,' and 'gagging the congress.' However, the Congress complied. Only after this highly unusual retroactive classification was challenged in court by POGO, a government watchdog organization, did the Department of Justice reverse itself and declare that this information was not considered classified and a danger to national security after all. I would like to request that these letters from Senators Grassley and Leahy be included in the record of today's hearing.

In March 2002, the Department of Justice's Office of the Inspector General began investigating my allegations, and in July 2004, after almost two years delay, completed its investigation. The Department of Justice immediately moved to classify the entire report and its findings. Six months later, they allowed the Inspector General to release only an unclassified version of its executive summary. This unclassified version confirmed my core allegations; concluded that I was fired for reporting misconduct; and stated that the FBI had failed to investigate the reported espionage, even though other facts, witnesses and evidence supported my allegations. I would like to request that the Inspector General's report also be included in the record of today's hearing.

In the summer of 2002 I also began to pursue legal remedies to challenge my unjust dismissal, and filed cases under First Amendment and Privacy Act, and the Freedom of Information Act. Rather than respond to the merits of my claim, in October 2002, Attorney General Ashcroft asserted a rarely invoked 'State Secrets Privilege', arguing that the entire case must be dismissed in the name of national security, even if my allegations were correct. The Department of Justice asked the courts to throw out the case without any hearings, depositions, or discovery. Even though the Department of Justice's own Inspector General has confirmed the seriousness of my allegations and concluded that I was fired for raising them, the DOJ has continued to insist that my case cannot go forward because it would jeopardize national security. So far, the DOJ has been successful in this effort to silence me. In June 2004, the court ruled in favor of this far-reaching assertion of the "state secrets privilege". Currently I am appealing my case, and the Department of Justice is still invoking the "state secrets privilege" and arguing that everything about my issues is covered by classification.

The government invoked the state secrets privilege a second time in an attempt to block me from being deposed in a case brought by families of those killed on September 11 against Saudi individuals and entities alleged to have financed al-Qaeda. The government insisted that almost every single question that the families wished to ask me would require the disclosure of classified information.

The problems I have reported have serious consequences to our national security; and have already been confirmed by the Inspector General's report and the inquiry of Senators Grassley and Leahy. Translation units are the frontline in gathering, translating, and disseminating intelligence. A warning in advance of the next terrorist attack may, and probably will, come in the form of a message or document in a foreign language that will have to be translated. If an attack then occurs, which could have been prevented by acting on information in such a message, who will tell family members of the new terrorist attack victims that nothing more could have been done? There will be no excuse that we did not know, because we do know.

Yet, knowing full well the seriousness of these confirmed issues and problems, rather than addressing them the FBI and the Department of Justice spend time and effort to cover them up by over use of secrecy and excessive classification. Contrary to their claims, they seem to be far more concerned with avoiding accountability than protecting our national security. I believe that my case clearly illustrates the federal government's capricious use of secrecy laws and classification to cover up problems and wrongdoing, and to avoid accountability, regardless of the damage to our national security. It demonstrates as well how excessive secrecy and pseudo classification can be used as retaliation tactics against national security whistleblowers.

This type of excessive classification and the effort to expand the "state secrets privilege" does not increase our national security but actually makes us less safe and it impedes oversight of the executive branch, as part of the checks and balances demanded by our Constitution.

Thank you again for inviting me to testify today. You are the first Congressional Committee after three years to request my testimony and hear my story. I believe this testimony is a good first step in examining this situation but what is really needed is an actual Congressional investigation. Therefore, with respect for your critical role in our Constitution's system of checks and balances, I request that you be the first Congressional Committee to investigate not just my case but what is going on over at the FBI and the Justice Department regarding the very serious problem of over-classification and the abuse of secrecy. Thank you.

Mr. SHAYS. Thank you. I will have questions for all three of you, but I would first like to turn to Mrs. Maloney, and she'll start out.

Mrs. MALONEY. I would like to thank all of the panel members for your testimony, and Ms. Edmonds, your testimony was very, very upsetting, basically that our Government used their own system of classification to dismiss you, to cover up complaints and the FBI, according to your testimony, substantiated your position. You should be given an award, not fired, if you are standing up for what you think is right and speaking up and pointing out where you think there may be a threat to our country.

I am going to write a bill and I am going to name it after you. It is going to follow very closely the bill that I authored along with Senator DeWine on the Nazi War Crimes Disclosure Act. It was the largest disclosure of documents since the Nuremburg Trial. Mr. Blanton, you pointed out that one of the great successes of this bill, they authored what needed to happen, but the way it was implemented was the constant oversight of a review board of which Mr. Richard Ben-Veniste was one of the public appointees. And in fact, we are still working and confronting the CIA which is refusing to release the documents. We are working now in a bipartisan way to get an extension of the bill to get them.

But I am going to take that model and write it for every single agency. One of the themes that all of you had was that if disclosure is out there, it strengthens our Government. It strengthens us when we know what's wrong, because then we know what we have to do to fix it. That was what was so important about the 9/11 Commission report that it was a strong bipartisan effort. It showed that secrecy and failure to communicate and the stovepiping and failure to share information was one of the reasons, it was an intelligence failure. So if we didn't know the information, then we couldn't work to correct it.

But I think that your report is tremendously upsetting to me. I do a lot of work on discrimination against women in employment. But this was truly your standing up to report espionage at the FBI, if I understand it correctly. And instead of investigating your claim, the FBI fired you. Is that basically what happened in your case, Ms. Edmonds?

Ms. EDMONDS. Yes, absolutely.

Mrs. MALONEY. And as we sit here today, even though the Justice Department Inspector General has sided with you, is that correct?

Ms. EDMONDS. Correct. They said that my allegations were confirmed by other witnesses, facts, evidence and documents.

Mrs. MALONEY. Even though this was confirmed, your allegations, when you were trying to help our Government, yet the administration, am I correct, is still fighting you?

Ms. EDMONDS. Correct. They are still continuing to invoke the state secret privilege and they are saying that despite these confirmations and by the Senate, we are considering these issues, all of them, classified. Therefore it cannot proceed in court. Even the IG report, what we have today, is their unclassified version of the executive summary. A big portion of this report has not been released yet to date.

Mrs. MALONEY. Our system, when we classify things, it's supposed to be used for national security, not to punish whistle blowers or cover up a "mistake" possibly in an agency. I think that your testimony is tremendously upsetting. It underscores that a system that we've tried to put in place is not working. I am very upset about it.

Would you say, it's almost unbelievable what you said, you're a translator, correct?

Ms. EDMONDS. Yes.

Mrs. MALONEY. What are the languages that you speak?

Ms. EDMONDS. According to the Department of Justice, that information is classified. So I cannot name the languages I speak.

Mrs. MALONEY. Are you making a joke or are you being serious?

Ms. EDMONDS. No, I have actually questions that were submitted and after these questions were submitted, the FBI, the Department of Justice, declared the languages I speak, all of them, all three of them, classified.

Mrs. MALONEY. I don't understand. Are you telling me that the language, they are interpreting that the languages you speak in telling this committee what these languages are, affects our national security?

Ms. EDMONDS. Correct. That's what they have asserted. That's what they have invoked for the past 3 years, that information is classified.

Mrs. MALONEY. I fail to understand how in any way, shape or form, Ms. Edmonds telling us the languages she speaks affects our national security. Why does the Justice Department claim that this is classified information? Why do they claim the languages you speak are classified information? On what grounds?

Ms. EDMONDS. What they are saying is they can't even say why because the information is so classified and it involves state secrets that even explaining it would present danger to our national security. Even if I'm right with my allegations and my case, nothing about me can be discussed because everything about me and everything about my case is considered the highest level of national security and state secrets.

Mrs. MALONEY. I find this ludicrous and ridiculous and an example of how this system is out of control. We have to have some oversight on it.

Can you tell me something about yourself? Where did you go to school?

Ms. EDMONDS. That information is classified. [Laughter.]

Mrs. MALONEY. Were you born in this country?

Ms. EDMONDS. I can say no, but I cannot tell you where I was born. That information is classified.

Mrs. MALONEY. Mr. Chairman, I find this absolutely absurd. I hope it's an area we can work in together. We need an independent review board, I would say, in every single agency. It's probably more compelling in national security, but every single agency that may have a whistle blower that they want to silence or whatever can just sit there and classify everything about that person so they can't even express their situation.

I have a series of other questions for the other two, but I see the red light is on, and my time is up.

Mr. SHAYS. Why don't I ask a few questions, and then we'll——

Mrs. MALONEY. OK, thank you.

Mr. SHAYS. Why don't the two of you just react to Ms. Edmonds' testimony?

Mr. BLANTON. I would be glad to.

Mr. SHAYS. What I would like you to do first, I would like you to explain why there is a National Security Archive at George Washington University, I would like you to explain why there is an Access Report: Freedom of Information at Lynchburg, Virginia. Just explain to me the significance of what each of you do before you answer the question.

Mr. BLANTON. When the Freedom of Information Act really started to apply to national security information, it was only in 1974, it was over President Ford's veto. About 10 years after that, a number of journalists and historians had amassed so much documentation released through FOIA that I think their spouses threatened to divorce them if they didn't get it out of the house. Thus, the National Security Archive was born. We've always stood up for family values ever since. I'm only partly joking.

Mr. SHAYS. But it's part of the university?

Mr. BLANTON. Yes, sir, we are an affiliate of George Washington University. We're housed in the main library at George Washington University.

Mr. SHAYS. How many staff?

Mr. BLANTON. We have about 33 people on staff here and about 11 people around the world that we pay part or all of their salaries.

Mr. SHAYS. What is the value of this institution?

Mr. BLANTON. We file more Freedom of Information requests than anybody else in the non-profit, non-commercial world.

Mr. SHAYS. You request them?

Mr. BLANTON. We file the requests. We request the documents. What we are after is, we're trying to create an institutional memory against this most shrouded area of American governance.

Mr. SHAYS. That's helpful. Thank you.

Mr. Hammitt, tell me, what is the Access Reports: Freedom of Information? What is that?

Mr. HAMMITT. I started writing Access Reports in 1985, then I bought it from the small company that originally owned it in 1989. Access Reports is a bi-weekly newsletter that deals specifically about the Freedom of Information Act. It also deals about Government information issues generally and what I refer to as informational privacy. The four statutes that I cover rather closely are the Freedom of Information Act, the Privacy Act, the Federal Advisory Committee Act and the Sunshine Act. I also cover cases that have happened on the State level. As you know, in Connecticut, you have your own FOIA and all the other States have similar sorts of laws.

Mr. SHAYS. So now just tell me, how did you digest what Ms. Edmonds was saying? First, let me ask you, Ms. Edmonds, is some of this information being held up because the court says it's not public information now because you're in a court case? Or is this all the Government saying that you can't discuss this?

Ms. EDMONDS. No, these are all invoked by the Government, and in various cases, not only court cases. That's what they did, even

when they retroactively classified those Senate letters. They said they could not even refer to——

Mr. SHAYS. So it wasn't the court?

Ms. EDMONDS. No.

Mr. SHAYS. Let me just tell you the problem of being the "first to investigate a case." I'm going to be asking the staff to look at the IG's report and be in contact with the IG about it. But when someone chooses a venue in court, we do not want to be used by the plaintiff to be the source of information. We don't want to be used that way. So we kind of back off when someone goes into court. It puts us in a situation where we don't know whether we're doing your bidding or trying to find—it kinds of distorts the issue. So it complicates it a bit. But we'll be doing some looking at the staff level at this case.

Would you both explain to me what your reaction is?

Mr. HAMMITT. Well, as I listened to what Ms. Edmonds said, when she says that the language that she can speak or where she was born or where she went to school is classified, I mean, that's information that intrinsically belongs to her. I see absolutely no way in which the Government can classify that information, or prevent her from speaking about it on her own. I can see that there are certain aspects of her case that theoretically could come under the shroud of the state secrets privilege.

To go a little further, I have seen other cases in which the Government has invoked the state secrets privilege. From my point of view as an observer, the state secrets privilege is almost invariably invoked by the Government when it just wants to stop litigation dead in its tracks. The district court judge basically ruled against Ms. Edmonds in this case, as I understand it, having read the decision, because all it takes to invoke the State Secrets Act is to have the attorney general sign the declaration and submit it to the court.

Mr. SHAYS. So the court then becomes obligated to—case closed in a way.

Mr. HAMMITT. As the privilege is interpreted now, I believe that once the court has agreed that the privilege has been improperly invoked, they have no more power. Her case is up before the D.C. Circuit now. I don't know that there is a date set for it yet or not.

Mr. SHAYS. You're almost implying it's stacked against her because the absurdity of classification can be used against her and a court can't evaluate whether it's being misused, in a sense.

Mr. HAMMITT. Absolutely. The State Secrets Act, a state secret privilege is the broadest privilege I've ever run across.

Mr. SHAYS. When you heard this, you thought, well, I'll tell you what I thought. I thought this is an absurdity. It makes me want to understand why someone wouldn't be rewarded for reporting concerns that an employee has. But were you listening to this and saying, this isn't so surprising, I've seen it before?

Mr. HAMMITT. No, no. I don't mean to imply that. I think that what Ms. Edmonds said, as I say, about her background, I think that I haven't heard anything any more absurd, although I think as Mr. Ben-Veniste said, I'm never surprised at how absurd certain things are in life. So no, I would completely agree with you. But this is an extraordinarily broad based privilege. Litigating in this

area of national security, and this is just part of that, is like hitting your head, butting your head up against a brick wall.

Mr. SHAYS. Ms. Edmonds, if I had reported what I thought was evil work against my Government and I was then punished, it would be my life work not just to vindicate myself, because I don't think I would need vindication, but to hold every one of those people accountable. Certainly we will be looking at that issue.

Mr. Blanton.

Mr. BLANTON. Mr. Chairman, with many secrets, not all, I should say, many secrets there is a kernel of truth in the sense that the FBI probably maintains internally, they're not all evil people, in fact a lot of people of goodwill, that to reveal the languages that Ms. Edmonds speaks would reveal something about their targeting of foreign nationals, about their pattern of wire tapping, about what they're trying to gather. At least that's the claim that I can imagine in their papers. I've seen claims like that in countless Freedom of Information cases.

When there is any kind of independent review of those claims, they almost always fall apart. Not always, there are some real secrets. But they almost always fall apart. The problem with the state secrets privilege is the courts don't provide any such independent review.

The one case that set the precedent, the so-called Reynolds case in 1952 in the Supreme Court, which upheld what turns out to be a false Air Force affidavit. We know this because of the declassification of the 1990's. One of the survivors' kids got a copy of the crash report that was released in the big declassifications of the 1990's. She was able, like in a DNA data base, to go back and unconvict the murderer, she was able to go back to that case and say, wait a second, Air Force was covering up negligence in the airplane crash.

She can't get a hearing. The Supreme Court refused to accept the case. The state secrets privilege continues as kind of the neutron bomb of whistle blower litigation. It leaves no plaintiff standing.

Mr. SHAYS. Is the case that's still out there?

Mr. BLANTON. The law firm in Philadelphia, the so-called Reynolds case, has tried to reopen it. They were rejected at the Supreme Court. I believe they have a petition at the Federal courts in Pennsylvania. It's still out there. It's a fascinating case, because it shows you when you look closely and have any kind of independent check on these claims, you get a different result than what you start with.

Mr. SHAYS. Well, we have a full committee, we have been looking at the case in Boston of where four people were falsely accused of murder and held in jail, two died, I think, in prison and two were set free. But they were even on death row for a while. He was separated from his wife and children for 30 years. As far as I'm concerned, the Government owes him so much and yet it is a struggle.

The interesting thing is there, I would be somewhat involved in wanting to help them in that court case, so I have to think through this one as well.

Mrs. Maloney.

Mrs. MALONEY. Based on the IG report that substantiated your case, just let me know any time you're going into court and let me see how many women leaders I can get to come stand with you.

I find this extremely upsetting. It basically shows that the Government can close down any information, including the ability of a "defendant" to defend himself or herself. If you can't even say what languages you speak, how in the world can you defend yourself in court? I mean, it's just really disturbing. If we can't look at it as a Government and the courts can't look at it, what's there to protect these people? I would ask Mr. Hammitt and Mr. Blanton, what recourse do they have if they can come in and say their entire court case is classified, what in the world can they do? No one can look at it. No one can do anything about it. You are basically taking the rights of these individuals away. To me, it's very upsetting.

What recourse do people have when they come in and say, your case is classified, no one can look at it? What can you do?

Mr. HAMMITT. I think everything you're saying is absolutely right and it's incredibly distressing. The only thing I think that somebody like that has is the power of publicity. That's not necessarily going to get them a hearing. I mean, the only other tool available to them after they've had their litigation shut down is to try to embarrass the Government to such an extent that the Government decides to come to the table. It's terrible that you have to do that.

Mrs. MALONEY. Believe me, it's hard to get publicity on anything. Take Ms. Edmonds' case, what is she going to do, go down to a paper and say, just write up my case? I think that's a hard thing to achieve. Do you want to talk about that, Mr. Blanton?

Mr. BLANTON. If she wins in the appeals court, it will be a great victory. If she loses, she'll be back in front of you, asking for your help as a committee of this Congress to push further. Because the reality is, there are very few recourses. That's why Congress, I think, in the interests of the same checks and balances that as an institution you represent, needs to think very creatively about how do you balance off something like the state secrets privilege?

Mr. SHAYS. When will your case be heard?

Ms. EDMONDS. You mean my court case? We have an appeal, our hearing is on April 21, 2005.

Mr. SHAYS. If there was an issue of you losing on the merits, that's one thing. If there is an issue of you losing because it can't be heard because of state secrets, I want you to knock our door down.

Ms. EDMONDS. May I say something?

Mr. SHAYS. Sure.

Ms. EDMONDS. That is a court case. That is a totally separate case. The issue of retroactively classifying congressional documents, which the Government changed its mind, this is the Department of Justice, just 2 weeks ago, saying for 9 months, we consider it national security, top secret, classified, but it no longer is. And the fact that there is an IG report currently out, even in its own classified executive summary version, confirms all my core allegations. It clearly says that the FBI, to this day, has failed to investigate these espionage cases, the cases where translations were intentionally blocked. Those translators are currently in there receiving

our intelligence and they are translating it right now. They are the ones that we are entrusting our national security with.

These issues actually have nothing to do with my court cases. These issues have to do with the U.S. Congress and the oversight and the system of checks and balances.

Mr. SHAYS. If the gentlelady would yield again?

Mrs. MALONEY. If I could please ask her a question first. Am I hearing you right, to this day the FBI has not investigated your espionage allegations? And even though the IG report has been out for some time, would you clarify that?

Ms. EDMONDS. Correct. The Department of Justice's Inspector General's report says that FBI, despite the fact that all these issues and allegations were confirmed by other sources, evidence, facts and documents, they still have not acted. They have not taken any action. That's correct.

Mrs. MALONEY. So in other words, rather than investigate the allegations thoroughly, the FBI concluded that you were disruptive or whatever and terminated you, is that correct?

Ms. EDMONDS. That's what the report says, that they terminated me because I was not backing up from these allegations and that was being disruptive.

Mr. SHAYS. Excuse me, Mrs. Maloney, if the gentlelady would yield just a second.

Mrs. MALONEY. I would be happy to yield.

Mr. SHAYS. I'm happy to have her go beyond her 5 minutes, but I just want to make sure that after the meeting, you get with my two staff members here and Mrs. Maloney's staff, and you give us the names of the people that you are accusing of illegal actions against their Government. We will contact the FBI tomorrow and ask for an accounting of whether or not they are looking into those individuals. We will be happy to pursue that.

So after this meeting, you get together with the two staff behind me. You have the floor again, Mrs. Maloney.

Mrs. MALONEY. Well, I have a series of questions on this, but I really would like to speak to my colleagues, particularly my colleague in Government and my colleagues in this room, about these serious ramifications that her case illustrates. I would say throughout every agency in Government, that the individual can basically be told to shut up if the agency doesn't like what they're saying, and not even bother to investigate what the person is saying is in my opinion an outrageous abuse of power.

But also I would say, Mr. Chairman, given the focus that we now have on homeland security and the amount of dollars that we are allocating, I would say clearly a third of a trillion dollars we've put into various homeland security, defense and Iraq and other areas, the inability to be able to look at these contracts or to have a whistle-blower come to us or anyone else and talk about it, they can effectively gag them under these provisions that they have, and they absolutely have no recourse.

I think it's wrong for any person in any agency, even if you're an educator and you think there is an abuse in the purchasing of the books or whatever, but it's particularly problematic with tremendous ramifications in homeland security dollars and homeland security allegations. I find quite frankly your testimony absolutely

and completely terrifying. I don't even want to believe it, because I want to believe in my Government. But what happened to you is extremely wrong, and upsetting to me.

I want to go back and make sure that I understand where we are. Basically, Ms. Edmonds, you testified that the FBI ignored your allegations of criminal conduct. I find that hard to believe, but that's what you said.

Ms. EDMONDS. Absolutely correct.

Mrs. MALONEY. Then you took the information to the Senate Judiciary Committee, correct?

Ms. EDMONDS. Correct.

Mrs. MALONEY. Then the Department of Justice Office of IG?

Ms. EDMONDS. Correct.

Mrs. MALONEY. And after the Senate Judiciary Committee began investigating your claims in a bipartisan way, Senators Grassley and Leahy, they issued public statements and letters demanding an expedited investigation by the IG and a response from the FBI, is that correct?

Ms. EDMONDS. Yes, they said during their unclassified briefings with the FBI, "FBI confirmed all their allegations and they denied none."

Mrs. MALONEY. And even though these statements and letters were widely distributed, the administration then chose to retroactively classify them years later?

Ms. EDMONDS. Two years later.

Mrs. MALONEY. Two years later they then retroactively decide, you know, to me, it's wrong in your case, but it's wrong that the Government has the ability, or power to jump back 2 years and classify information they don't want to come out. I find this tremendously upsetting.

So let me make sure I understand. So after two U.S. Senators, in a bipartisan way, issued public statements about unclassified briefings, the administration actually went back and classified them?

Ms. EDMONDS. Correct.

Mrs. MALONEY. And this happened 2 years after they issued these statements?

Ms. EDMONDS. Yes.

Mrs. MALONEY. Did you have an attorney? Were they able to do this? Do you have an attorney representing you?

Ms. EDMONDS. Yes, I did.

Mrs. MALONEY. By law they can go back and classify 2 years past? And after all that time, why do you think these public statements and letters were classified? Why did they jump back 2 years and classify these letters and statements?

Ms. EDMONDS. They believe that it was due to the fact that at that point they were trying to gain their upper hand both in court cases and also with respect to the Inspector General's report and also other cases brought by the September 11 family members against certain countries.

Mrs. MALONEY. OK. I'd like to ask you in your view, was there anything in the statements and letters that in any way in your opinion constituted a threat to our country's national security?

Ms. EDMONDS. No, absolutely not. Not only that, if that was the case, there were thousands of Web sites that displayed these letters for over almost 2 years, over the Internet. These letters were quoted extensively, on the front page of the Washington Post, in other newspapers.

So the Government never went back and took out that information, those letters, from all other sources that had this information available. They just wanted to shut down these congressional investigations and these line of questions and investigations by the Senate.

Mrs. MALONEY. Well, what I find tremendously upsetting, Mr. Chairman, is this fact pattern that she's putting out there is showing that the public has absolutely no chance against the Federal Government. If the Federal Government decides to close you down, there is no court case, the so-called independent court system wouldn't be able to look at it, because you can't even say where you were born or what languages you speak, much less what happened. All I can say is that, congratulations to the IG system that this Congress put into place that has one form of resource of independent review that has come in and substantiated what you've said.

I find her story incredibly upsetting. I would like to ask Mr. Hammitt and Mr. Blanton, what is your response to her story? I have never heard of this before? What is your response to this?

Mr. BLANTON. It happens all the time.

Mrs. MALONEY. This is an abuse of power.

Mr. BLANTON. Absolutely, and it happens all the time, and anyone who has looked at classified-declassified information and Freedom of Information cases sees the same kinds of claims. I think it will only stop when we figure out a way to give the court some backbone. Right now, the case law is almost complete deference.

But there is a wonderful precedent right here in the D.C. Circuit. We brought a Freedom of Information case about the failed Iran rescue mission. We asked the judge, when the Pentagon said, it's all totally classified, not a page can be released, we said, appoint a special master. You do it in desegregation cases of public schools. Appoint somebody who actually has some expertise, a person who held some clearances, who can look at it.

Just by bringing in the special master, the court was able to pry loose ultimately 88 percent of the total body of information the Pentagon originally said not one word could come out. And let me tell you one of the top secrets that was included. It was the after-action report from the helicopter pilots who told the Pentagon, don't include milk in our box lunches, it goes sour in the desert heat.

So if Congress could actually endorses this kind of precedent, which only really exists here in the D.C. Circuit, encourage courts to take creative countervailing power, like appointing special masters, in cases that involve national security secrets, where the judge, for some good reasons, does not feel expert, does not feel able to argue with the Government claim, will show total deference to the Government claim. You have to move some other countervailing power into the system. If the appeals court appointed a special master to look at Ms. Edmonds' case and to look at the case file, my bet is that 90 percent of what's in the IG report, what's

in the complaint file and the investigations file would be released tomorrow.

Mr. HAMMITT. At the risk of piling on, I'm afraid I completely agree with Tom. I think these sorts of instances happen much, much too frequently, and I think that the state, when I see the state secrets privilege invoked by the Government, my first reaction personally as an observer is, the Government doesn't want this litigation to happen. It doesn't have to specify why it believes this is a state secret, it just has to, as I said earlier, it has to provide this affidavit signed by the Attorney General.

And that, if the Attorney General is on board, that's not a terribly difficult obstacle to overcome. This sort of thing happens when the Government just does not want this litigation to go forward. I completely agree with Tom. I can't personally believe that there's any national security involved in there.

Mrs. MALONEY. I just want to thank the chairman for an extraordinary hearing. I just have one last question for Mr. Blanton. When I read redacted Freedom of Information claims, they always cite section 5. They get an exemption or we're blacking it out because of section 5. Could you in a general sense tell me what is section 5? How come they can redact so much under section 5?

Mr. BLANTON. This is the deliberative process exemption. Like many exemptions, it comes from a kernel of a good idea. You want to encourage the most candid exchanges of views, you want to encourage officials inside any proceeding to give their frankest possible advice.

But I would say today, with the Ashcroft memoranda and the way the Government is interpreting it, the B(5) exemption, so-called, is now a shadow covering the entire body, or as much as they can cover of Government information. The problem fundamentally I think comes to the core question: How does it really make us safer? If a Government official would change their advice to a policymaker for fear of being public, the remedy is to fire that weak-kneed official, not keep that opinion secret.

Mrs. MALONEY. Thank you very much.

Mr. SHAYS. Ms. Edmonds, I'm a little confused as to what the status of your relationship is with Grassley and Leahy. Are they pursuing this? Have they dropped your case? What have they done?

Ms. EDMONDS. That's what I am waiting to hear back, because I have been sending letters saying, for 2 years I was told that everybody in the Congress has to wait for the Inspector General's report to come out before——

Mr. SHAYS. You're not being responsive to my question. My question is, what is your relationship with Mr. Leahy and Mr. Grassley right now? These are two distinguished elected officials who have had a chance to review your case far more than Mrs. Maloney and I have. I want to know, are they actively pursuing your case?

Ms. EDMONDS. I really can't answer, because I don't know. They're not being responsive.

Mr. SHAYS. So there is a challenge that you have working with these two very distinguished people.

Ms. EDMONDS. They have been actually very supportive and good in the past. It's just that they haven't been responsive since the IG report.

Mr. SHAYS. Which is how long ago?

Ms. EDMONDS. The IG report, they gave it to the Senators because they could review it, the classification, etc., in July 2004. So since July 2004, I haven't had any response.

Mr. SHAYS. I think the first thing will be obviously to contact them and find out what work they've already done so we don't have to duplicate it and so on.

Is it conceivable that the FBI felt that some of your complaints were beyond your ability to know? In other words, a question of someone's time sheet? As we're just going through it, the IG said you made a complaint about someone's time sheet and that person wasn't even there that day.

Ms. EDMONDS. I didn't make complaints about those. In fact, those issues came out much later with the IG, because the IG says, a lot of cases in the FBI were criminal, and that to be exact, they said since the Inspector General's office is not in the business of conducting criminal investigations, we want to find out about these nitty-gritty administrative stuff. That's how they worded it.

Mr. SHAYS. I just want to say, in the report, you accuse someone of a time sheet not being accurate, and they found out that the person wasn't even in the office that day. That takes away your credibility, obviously, when you are making complaints about someone and are wrong about that.

I'm just saying, I want you to know I am deeply concerned about your testimony and I have to accept on the face of it certain comments. But it's a "he said, she said," and I don't know what the other side is. I just want to respond to you that I don't know what the other side is on this.

I do know that I don't like classification to be used as the basis not to know both sides. I do know that if you have accused someone of espionage, I sure as hell am not going to have you tell me that nothing's been done and then just not respond to it. We're going to respond to it, and you're going to tell us who those people are and we're going to find out what happened. So we're not going to drop the ball here.

But I just want you to know, I've been in this business now 30 years. We have one side of this story. We will try to understand the other side and then take appropriate action. That's my point.

Ms. EDMONDS. That's exactly what I believed that the IG report was going to do, and also the Senate letters.

Mr. SHAYS. Do you think it did that?

Ms. EDMONDS. Yes, to a certain degree, and also the Senate letter saying that the FBI had already confirmed all those allegations.

Mr. SHAYS. I'm asking about the IG. In other words, you suggest the IG's report be something that is submitted for the record, and we submitted it for the record, we're going to be looking at it.

But when we look at the record, it's not something that makes you, it does raise one or two questions about what your participation in this is. It has a "Keystone Cops" kind of feel to it, with espionage, which is extraordinarily serious, somehow intertwined in here. So it has charges that seem petty that you are making as well as espionage at the same time. So it's just an interesting kind of mix of stuff here that we haven't looked at yet and will look at.

Ms. EDMONDS. That was by IG's choice, sir.

Mr. SHAYS. What was that?

Ms. EDMONDS. That was by IG's choice, because the allegations that I took to the Senate and to the IG were those core allegations you see at the beginning that had to do with mistranslations, intentional block of translations and espionage cases. But the other ones that——

Mr. SHAYS. Espionage case, in other words, involved in espionage or they were guilty of espionage?

Ms. EDMONDS. How it was told to this date is potential espionage case, security breaches that were confirmed by other witnesses, facts, evidence.

Mr. SHAYS. I just want to be clear. Are you accusing people of committing espionage?

Ms. EDMONDS. I am accusing people with documents, evidence, dates and other witnesses of involving in actions against the United States, national security, intelligence, military secrets and nuclear secrets.

Mr. SHAYS. What about military and nuclear secrets, that they were doing what?

Ms. EDMONDS. I cannot talk about that information unless I am in a secured facility.

Mr. SHAYS. You're accusing them of committing espionage is the answer or not?

Ms. EDMONDS. Right.

Mr. SHAYS. So you will meet with our staff afterwards.

Is there anything that any of you would like to put on the record before we adjourn? Any last points? We weren't intending to focus this much on one case, but it certainly was illustrious of an issue and very informative. We thank you for being here.

Mr. HAMMITT. I guess from my point of view, I would just like to thank the subcommittee for its interest in this subject. I think that it's going to take serious congressional oversight and possibly legislative initiatives on the part of Congress to do something about the growth of these sorts of non-classified systems of information. I really appreciate the fact that you are looking at this, because this is an extremely serious problem.

Mr. BLANTON. Mr. Chairman, you asked the question last summer that got all this started, because you forced people on the record to say how much overclassification is there. If you ask the same questions about the pseudo-classification, it's the beginning of reining it in and having a more rational system that actually protects us and accountability.

Mr. SHAYS. Let me just quickly, that was one of my intentions before I was thinking so much of Ms. Edmonds' case. Are these pseudo-classifications something that have been, 2 years ago, 3 years ago, 10 years ago, 15?

Mr. BLANTON. They have happened as long as there have been bureaucrats in the world. Harold Relyea's paper, which is a fascinating read, takes us back to the 1950's, it has the battles of pseudo-classification just like this. It's a bad idea, it's a natural, I think, human response, if you're in a bureaucracy it's how you protect your turf, it's how you get more resources, it's how you keep other people out.

General Groves, the head of the Manhattan Project, listed six or eight reasons of why we have to have secrecy around the nuclear bomb. The first three were the Germans, the Japanese and the Russians. But the next one was to keep prying outsiders and other executive agencies and the Congress from knowing what we were doing. Another one was, keep our folks focused on their own work and not messing around in other compartments. Another was to have surprise. He said, but of course that one got lost as soon as we blew up the bomb. That was the big secret, that it worked. Once you knew it worked, any competent physicist could go back and make a nuclear bomb. It wasn't really a secret any more.

The people who have real secrets to protect will also tell you, there's a bureaucratic imperative. So you have to count them, cost them, limit the people who can create them, put in countervailing powers, have independent reviews, and then you're part-way there.

Mr. SHAYS. We had a staff retreat yesterday in which I was telling my staff that I wanted to be able to do "cutting edge issues" and then do some significant follow-through. I guess this qualifies on both levels.

Mr. BLANTON. Yes, sir, that's true.

Mr. SHAYS. This is a very interesting issue and one which will get some good attention for this subcommittee.

Any closing words from you, Ms. Edmonds, before we adjourn?

Ms. EDMONDS. No, I just want to repeat one thing and that is——

Mr. SHAYS. So yes, you want to repeat? [Laughter.]

Ms. EDMONDS. Yes, thank you.

And that is, aside from the issues that we will be discussing, with the other reports out there regarding the FBI's translation units and what has happened there in terms of inaccuracies, incompetence, back-door hirings, these have been already confirmed, not only through me. I can also give you the names, you can get it from the IG. We do need hearings regarding these issues, because to this date, they have not addressed these issues internally. We are in touch with translators in there who are saying, there are only cosmetic changes.

Mr. SHAYS. Some things we can maybe even achieve without hearings, but by simply asking questions and having staff do a little investigative work. It's amazing what we can get done doing that.

So your testimony has been very helpful to us and we will definitely follow through. You're due to meet with staff afterwards.

So with that, with no additional comments, we are going to adjourn this hearing.

[Whereupon, at 5:11 p.m., the subcommittee was adjourned.]

[Additional information submitted for the hearing record follows:]

U.S. Department of Transportation
Office of the Secretary of Transportation

400 Seventh St., S.W.
Washington, D.C. 20590

May 9, 2005

The Honorable Christopher Shays
Chairman, Subcommittee on National Security,
Emerging Threats, and International Relations
Committee on Government Reform
House of Representatives
Washington, DC 20515

Dear Chairman Shays:

We are pleased to provide for the record the following responses to questions related to my testimony on March 2, 2005. Before I do that, I would like make a brief comment about the role of the Department of Transportation (DOT) in classification of intelligence information that may assist in clarifying my testimony.

DOT and its operating administrations, such as the Federal Aviation Administration (FAA), are consumers, not collectors, of intelligence information. The agencies of the U.S. Intelligence and Law Enforcement Communities, as collectors of intelligence information, have the authority and responsibility for the original classification and dissemination of intelligence reporting to other agencies of the Federal Government. Agencies that receive these intelligence reports, such as DOT and FAA, must observe and respect the original classification decision when reproducing, extracting or summarizing classified information from these reports and cannot declassify, or otherwise change the classification status of the information without the consent of the originating agency.

Question 1. What individuals in the Department of Transportation were involved in the review, classification, and declassification of the 9/11 Commission staff monograph? Did these individuals have contact with other agencies and who were their points of contact in these agencies?

Answer. The individuals involved were a staff Intelligence Operations Specialist in the Department's Office of Intelligence and Security (now, the Office of Intelligence, Security, and Emergency Response); FAA's Assistant Administrator for Security and Hazardous Materials, Lynne Osmus, and her deputy, Claudio Manno; and Shirley Miller, Special Assistant to the Deputy FAA Administrator. Each of them only reviewed the information and neither classified nor declassified any of it.

To our knowledge, these individuals did not contact any other agencies, except that the Intelligence Operations Specialist recommended to the Department of Justice that it consult the Transportation Security Administration (TSA) of the Department of Homeland Security (DHS), which is legislatively charged with aviation security.

Question 2. To the best of your knowledge, who made final decisions on what to declassify in the 9/11 monograph and when?

Answer. We have no knowledge on this.

Question 3. You testified that the "FAA recommended to Justice that DHS be consulted on FAA's recommendations." What were the FAA recommendations? Did the FAA have any direct interaction with the Department of Homeland Security?

Answer. Pursuant to the Aviation and Transportation Security Act of 2001 and the Homeland Security Act of 2002, the aviation security mission vested with DHS/TSA. Therefore, the Intelligence Operations Specialist who did the review for FAA recommended that the Department of Justice consult with DHS on whether the security-related information contained in reviewed portions of the monograph remained classified. FAA made no recommendations relative to final classification of any information in the monograph, and did not interact with DHS regarding the monograph.

Question 4. Did the FAA recommend redacting any information? If so, are there any differences in the redactions the FAA recommended and the final redactions in January? If so, what are those differences?

Answer. No, FAA did not recommend redacting any information (nor did it recommend against redacting any information).

Question 5. Did FAA officials ever consult or negotiate with the staff of the 9/11 Commission who wrote the report regarding redactions?

Answer. No. The Commission ceased to exist in August 2004 and the monograph, dated August 26, 2004, was not circulated for review until September 2004.

Question 6. Did the FAA officials ever suggest language changes that might have avoided classification?

Answer. No, FAA officials never suggested language changes that might have avoided classification. Since they were not the original classifiers of the information, they were in no position to do that. Moreover, as noted above, the Commission no longer existed.

Question 7. On May 16, 2002, National Security Advisor Condoleezza Rice held a press conference to address questions about what the government knew about the likelihood of a terrorist attack before September 11, 2001. She stated: "I don't think anybody could have predicted that these people . . . would try to use an airplane as a missile, a hijacked airplane as a missile." Prior to holding her press conference, did Ms. Rice ever contact you, your predecessors, or your office regarding what the Department of Transportation or the FAA knew about the possibility that terrorists might use hijacked airplanes in suicide attacks?

Question 8. On April 8, 2004, Ms. Rice testified before the 9/11 Commission, stating that "this kind of analysis about the use of airplanes as weapons actually was never briefed to us." Between the time she held her press conference on May 16, 2002, and when she testified before

the 9/11 Commission on April 8, 2004, did Ms. Rice consult with you, you predecessor, or your office on this specific question?

Question 9. Did anyone at the National Security Council consult with anyone in your office before Ms. Rice made either of these public statements?

Answer. As I indicated in my oral responses at the hearing, I have no knowledge relating to these questions.

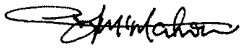
Question 10. You testified that in fiscal year 2001, "FAA made one SECRET classification and the United States Coast Guard, now part of DHS, made one." You also testified that in fiscal year 2002, "FAA made six secret classifications and the Coast Guard made one." In addition, you testified that in fiscal year 2003, "DOT made no original security classifications," and that in fiscal year 2004, "we also made no original security classifications." Provide the number of designations made by FAA, the Coast Guard, and the Department of Transportation in fiscal years 2001, 2002, 2003, and 2004, based on "for official use only," "sensitive security information," or any other restricted information designations that fall outside the national security classification system.

Answer. During the period in question, we did not keep records of restricted information designations other than national security classifications. Since January 2005, we have kept records of SSI designations, of which there have been two. Information has also been designated as "For Official Use Only" this year, but we have no records of how many times. There is no regulatory or other national policy governing the use of the FOUO designation, as opposed to the controls on classified national security information.

Finally, you asked that we provide the Subcommittee with FAA or DOT memoranda or correspondence regarding the agency's review and redaction of the 9/11 Commission FAA staff report on FAA intelligence warnings. The only such memorandum or correspondence was a facsimile message from the FAA to the Department of Justice, transmitting the notations of the Intelligence Specialist in the text of the monograph. A copy of the transmittal sheet for that message is enclosed.

Please let us know if we can provide additional information to the Subcommittee.

Sincerely,



Christopher A. McMahon, RADM, USMS
Office of Intelligence, Security, and Emergency Response

Enclosure

○