AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

DROWNING IN A SEA OF FAUX SECRETS: POLICIES ON HANDLING OF CLASSIFIED AND SENSITIVE INFORMATION

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

SECOND SESSION

MARCH 14, 2006

Serial No. 109–167

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html
http://www.house.gov/reform

DROWNING IN A SEA OF FAUX SECRETS: POLICIES ON HANDLING OF CLASSIFIED AND SENSITIVE INFORMATION

DROWNING IN A SEA OF FAUX SECRETS: POLICIES ON HANDLING OF CLASSIFIED AND SENSITIVE INFORMATION

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

SECOND SESSION

MARCH 14, 2006

Serial No. 109–167

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

29–385 PDF WASHINGTON : 2006

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
JON C. PORTER, Nevada
KENNY MARCHANT, Texas
LYNN A. WESTMORELAND, Georgia
PATRICK T. MCHENRY, North Carolina
CHARLES W. DENT, Pennsylvania
VIRGINIA FOXX, North Carolina
JEAN SCHMIDT, Ohio

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)

DAVID MARIN, *Staff Director*
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*
ANNA LAITIN, *Minority Professional Staff Member*

CONTENTS

Page

Hearing held on March 14, 2006 1

Statement of:

Blanton, Thomas S., director, National Security Archive, George Washington University, Washington, DC; Anna K. Nelson, distinguished historian in residence, American University, Washington, DC; and Matthew M. Aid, Washington, DC 301

Aid, Matthew M. 332

Blanton, Thomas S. 301

Nelson, Anna K. 324

Weinstein, Allen, Archivist of the United States, National Archives and Records Administration; J. William Leonard, Director, Information Security Oversight Office, National Archives and Records Administration; Davi M. D'Agostino, Director, Defense Capabilities and Management, U.S. Government Accountability Office; Robert Rogalski, Acting Deputy Under Secretary of Defense, Counterintelligence and Security, U.S. Department of Defense; and Glenn S. Podonsky, Director, Office of Security and Safety Performance Assurance, U.S. Department of Energy 231

D'Agostino, Davi M. 243

Leonard, J. William 238

Podonsky, Glenn S. 271

Rogalski, Robert 257

Weinstein, Allen 231

Letters, statements, etc., submitted for the record by:

Aid, Matthew M., Washington, DC, prepared statement of 334

Blanton, Thomas S., director, National Security Archive, George Washington University, Washington, DC, prepared statement of 305

D'Agostino, Davi M., Director, Defense Capabilities and Management, U.S. Government Accountability Office, prepared statement of 245

Kucinich, Hon. Dennis J., a Representative in Congress from the State of Ohio, prepared statement of 17

Leonard, J. William, Director, Information Security Oversight Office, National Archives and Records Administration, prepared statement of 240

Maloney, Hon. Carolyn B., a Representative in Congress from the State of New York, prepared statement of 163

Nelson, Anna K., distinguished historian in residence, American University, Washington, DC, prepared statement of 327

Platts, Hon. Todd Russell, a Representative in Congress from the State of Pennsylvania, prepared statement of 350

Podonsky, Glenn S., Director, Office of Security and Safety Performance Assurance, U.S. Department of Energy, prepared statement of 272

Rogalski, Robert, Acting Deputy Under Secretary of Defense, Counterintelligence and Security, U.S. Department of Defense, prepared statement of 259

Shays, Hon. Christopher, a Representative in Congress from the State of Connecticut:

Prepared statement of 6

Various reports and letters 3, 168

Waxman, Hon. Henry A., a Representative in Congress from the State of California, prepared statement of 10

Weinstein, Allen, Archivist of the United States, National Archives and Records Administration, prepared statement of 234

DROWNING IN A SEA OF FAUX SECRETS: POLICIES ON HANDLING OF CLASSIFIED AND SENSITIVE INFORMATION

TUESDAY, MARCH 14, 2006

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

The subcommittee met, pursuant to notice, at 2:04 p.m., in room 2154, Rayburn House Office Building, Hon. Christopher Shays (chairman of the subcommittee) presiding.

Present: Representatives Shays, Kucinich, Maloney, Van Hollen, and Waxman.

Staff present: Lawrence Halloran, staff director and counsel; J. Vincent Chase, chief investigator; Robert A. Briggs, analyst; Marc LaRoche, intern; Karen Lightfoot, minority communications director/senior policy advisor; David Rapallo, minority chief investigative counsel; Anna Laitin and Andrew Su, minority professional staff members; Earley Green, minority chief clerk; and Jean Gosa, minority assistant clerk.

Mr. SHAYS. A quorum being present, the Subcommittee on National Security, Emerging Threats, and International Relations hearing entitled, "Drowning in a Sea of Faux Secrets: Policies on Handling of Classified and Sensitive Information," is called to order.

It has been said, bureaucracies always seek the path of least disclosure. During the cold war, the innate tendency to excessive secrecy was useful against the monolithic threat of Soviet military and industrial espionage. But today, against the polymorphic perils of stateless terrorism, the reflexive concealment of broad categories of official information harms more than enhances national security. Unreformed habits of secrecy blind us to the dispersed shards of information that, if linked, could reveal the enemy's shadowy plans.

Recent reports of a secret program to reclassify previously declassified documents reflect the stubborn refusal of many cold warriors to move from the "need to know" to the "need to share" security paradigm. Operating since 1999, the program culled materials from public archives that had already been viewed, copied, or republished. Claiming the bureaucratic "equities," code for "turf," had been ignored in the rush to declassify, the reclassifiers have taken tens of thousands of pages from the open files in what I would refer to as an arrogant and futile attempt to unwrite history. Many of

the documents deal with issues having no current security implications. As a result, obvious non-secrets, like the stunning wrong estimate in 1950 that the Chinese would not enter the Korean War, are once again stamped "secret."

This absurd effort to put the toothpaste back into the tube persists, despite the growing consensus supported by testimony before this subcommittee that from 50 to 90 percent of the material currently withheld should not be classified at all.

The inbred penchant for over-classification has also spawned a perverse offspring in the form of a vast and rapidly growing body of pseudo-secrets withheld from public view in the name of national and homeland security.

As this subcommittee learned in two previous hearings on post-September 11th barriers to information sharing, what is not classified can still be kept from the public through the use of "Sensitive But Unclassified," designated as SBU, designations, like, for instance, "For Official Use Only," [FOUO], or "Official Use Only," [OUO], and there are countless others. The unchecked proliferation of documents bearing these and other access restriction labels is choking what the 9/11 Commission said should be, must be free-flowing pathways for critical information about an adaptable, decentralized foe.

After our hearing last year, Mr. Waxman and I asked key cabinet departments how many documents they had shielded with SBU markings over the past 4 years. Claiming the task so burdensome and the numbers so large, they could not even venture an estimate.

At the same time, we asked the Government Accountability Office [GAO], to examine policies and procedures on FOUO and OUO documents at the Department of Defense and Energy, respectively. Stamping something "For Official Use Only" should only mean someone has determined the information may meet the limited criteria for exemption from automatic public release under the Freedom of Information Act [FOIA]. But increasingly in this security-conscious era, SBU designations are being misused as an unregulated form of "classification light."

I am going to digress a second. A case in point: The report from the Department of Homeland Security Inspector General bears this ominous-looking green cover warning recipients the document is "For Official Use Only." The report is an audit of screening done on trucks carrying municipal solid waste from Canada into the United States. It is 18 pages long. The IG was good enough to send along an unclassified summary of what is really an already unclassified FOUO report. This is the summary. It is one page. So our conclusion is apparently there is a great deal the public should never know about Canadian garbage. Can you believe it?

[The information referred to follows:]

DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Audit of Screening Trucks Carrying Canadian Municipal Solid Waste

(Unclassified Summary)

Office of Audits

OIG-06-21

January 2006

Department of Homeland Security

FOR OFFICIAL USE ONLY

THE ATTACHED MATERIALS CONTAIN DEPARTMENT OF HOMELAND SECURITY INFORMATION THAT IS "FOR OFFICIAL USE ONLY," OR OTHER TYPES OF SENSITIVE BUT UNCLASSIFIED INFORMATION REQUIRING PROTECTION AGAINST UNAUTHORIZED DISCLOSURE. THE ATTACHED MATERIALS WILL BE HANDLED AND SAFEGUARDED IN ACCORDANCE WITH DHS MANAGEMENT DIRECTIVES GOVERNING PROTECTION AND DISSEMINATION OF SUCH INFORMATION.

AT A MINIMUM, THE ATTACHED MATERIALS WILL BE DISSEMINATED ONLY ON A "NEED-TO-KNOW" BASIS AND WHEN UNATTENDED, WILL BE STORED IN A LOCKED CONTAINER OR AREA OFFERING SUFFICIENT PROTECTION AGAINST THEFT, COMPROMISE, INADVERTENT ACCESS AND UNAUTHORIZED DISCLOSURE.

Mr. SHAYS. In a report released today, GAO finds a lack of clear standards governing the use of the FOUO and OUO labels. Almost anyone can apply the "Official Use Only" restriction and no one can make it go away unless someone happens to request the document under the FOIA, but then they have to know the document exists.

Against a rising tide of global terrorism, we are drowning in a sea of our own faux secrets, hiding public information from its real owners, the public, behind spurious FOUO and OUO labels. To right the balance between the public's right to know and countervailing public interest in security and privacy, the habits of secrecy must give way to the culture of shared information.

Our discussion today is timely. This is, and I kid you not, Sunshine Week 2006, the second annual observance by organizations and individuals seeking greater openness in government. At the same time, policies and procedures on classification, reclassification, and designation of sensitive but unclassified material appear to be rushing headlong in the opposite direction.

We are joined by two panels of highly qualified and knowledgeable witnesses, including the Archivist of the United States. We welcome him. We look forward to all their testimony and to a constructive discussion of what can be done to sustain and enhance the public's access to their information.

[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
MARK E. SOUDER, INDIANA
STEVEN C. LATOURETTE, OHIO
DOUG OSE, CALIFORNIA
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

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 14, 2006

It has been said bureaucracies always seek the path of least disclosure. During the Cold War, that innate tendency to excessive secrecy was useful against the monolithic threat of Soviet military and industrial espionage. But today, against the polymorphic perils of stateless terrorism, reflexive concealment of broad categories of official information harms, more than enhances, national security. Unreformed habits of secrecy blind us to the dispersed shards of information that, if linked, could reveal the enemy's shadowy plans.

Recent reports of a secret program to reclassify previously declassified documents reflect the stubborn refusal of many Cold Warriors to move from the "need to know" to the "need to share" security paradigm. Operating since 1999, the program pulled materials from public archives that had already been viewed, copied or republished. Claiming that bureaucratic "equities" (code for "turf") had been ignored in the rush to declassify, the reclassifiers have taken tens of thousands of pages from the open files in an arrogant and futile attempt to un-write history. Many of the documents deal with issues having no current security implications. As a result, obvious non-secrets – like the spectacularly wrong estimate in 1950 the Chinese would not enter the Korean War – are once again stamped "Secret."

This absurd effort to put the toothpaste back into the tube persists despite the growing consensus – supported by testimony before this Subcommittee – that from fifty to ninety percent of the material currently withheld should not be classified at all.

That inbred penchant for overclassification has also spawned a perverse offspring in the form of a vast and rapidly growing body of pseudo-secrets withheld from public view in the name of national and homeland security.

As this Subcommittee learned in two previous hearings on post-9/11 barriers to information sharing, what is not classified can still be kept from the public through the use of Sensitive But Unclassified (SBU) designations like "For Official Use Only" (FOUO) or "Official Use Only" (OUO). The unchecked proliferation of documents bearing these and other access restriction labels is choking what the 9/11 Commission said should be free-flowing pathways for critical information about an adaptable, decentralized foe.

After our hearing last year, Mr. Waxman and I asked key cabinet departments how many documents they had shielded with SBU markings over the past four years. Claiming the task so burdensome and the numbers so large, they could not even venture an estimate.

At the same time, we asked the Government Accountability Office (GAO) to examine policies and procedures on FOUO and OUO documents at the Department of Defense and Energy. Stamping something "For Official Use Only" should only mean someone has determined the information may meet the limited criteria for exemption from automatic public release under the Freedom of Information Act (FOIA). But increasingly, in this security-conscious era, SBU designations are being misused as an unregulated form of "classification-lite." In a report released today, GAO finds a lack of clear standards governing use of the FOUO and OUO labels. Almost anyone can apply the "Official Use Only" restriction and no one can make it go away unless someone happens to request the document under the FOIA.

Against a rising tide of global terrorism, we are drowning in sea of our own faux secrets, hiding public information from its real owners behind spurious FOUO and OUO labels. To right the balance between the public's right to know and countervailing public interests in security and privacy, the habits of secrecy must give way to the culture of shared information.

Our discussion today is timely. This is Sunshine Week 2006, the second annual observance by organizations and individuals seeking greater openness in government. At the same time, policies and procedures on classification, declassification, reclassification and designation of Sensitive But Unclassified material appear to be rushing headlong in the opposite direction.

We are joined by two panels of highly qualified and knowledgeable witnesses, including the Archivist of the United States. Welcome. We look forward to their testimony and to a constructive discussion of what can be done to sustain and enhance the public's access to their information.

Mr. SHAYS. At this time, the chair would acknowledge we have both the ranking member of the full committee and the ranking member of the subcommittee and I would call on the ranking member of the subcommittee if he has a statement.

Mr. KUCINICH. I do have a statement, but I would more than be willing to defer to the ranking member of our full committee. Please, Mr. Waxman.

Mr. WAXMAN. Well, thank you very much, Mr. Kucinich and Mr. Chairman, for the opportunity to make this opening statement. As Mr. Shays indicated, this week is openness and transparency for government because it is called Sunshine Week. These are the bedrock principles of our democracy.

Unfortunately, sunshine rarely penetrates the inside of the Bush administration. They have a penchant for secrecy. It is legendary and the examples are numerous. The Vice President refused to reveal which campaign contributors and energy executives had special access to his energy task force. The President rolled back Reagan-era regulations on the release of Presidential records. The Department of Health and Human Services withheld estimates of the true cost of the Medicare prescription drug legislation. And the Defense Department redacted hundreds of Halliburton overcharges from audits given to the United Nations.

This is not a new issue. In September 2004, I released a comprehensive report on secrecy in the Bush administration. The report found that the Nation's open government laws had been repeatedly eroded during the first 4 years of the Bush administration, while laws authorizing secret government action had been systematically expanded. These trends have continued and worsened in the months since I released that report.

Last month, researchers discovered that the administration had been secretly removing thousands of previously classified documents that had been publicly available on the shelves of the National Archives. Some of these documents were more than 50 years old and already had been published in books and journals.

According to these researchers, one of the documents is a 1948 memorandum regarding delays in implementing Project Ultimate, a CIA program to drop propaganda leaflets out of hot air balloons to the citizens of Eastern Europe, and this memo was published already in a 1996 State Department volume. Yet incredibly, this 58-year-old document has now been removed from the shelves, according to the researchers.

There are a lot of questions about the administration's actions to which we don't have the answers. Who oversees this program? Under what legal authority are they operating? And why is the order governing this program evidently still classified? I hope we can begin to get answers to these questions at today's hearing.

Another important issue we will consider today is the administration's abuse of designations such as "Sensitive But Unclassified" to block the public release of government information. Many of these designations have no basis in statute, no criteria for use, no limitations on who can withhold documents using these designations.

Last year, Chairman Shays and I sought documents from three agencies, the Defense Department, State Department, and the De-

partment of Homeland Security, that had been restricted as "Sensitive But Unclassified" or "For Official Use Only." To date, we have received none of these documents.

It is particularly telling that in their responses, the agencies claimed they had no way to provide such information because they don't keep track of it. As another agency wrote, there is no regulatory or other national policy governing the use of "For Official Use Only," this designation, as opposed to the controls on classified national security information.

A year ago, I wrote to Chairman Shays about the abuses of these pseudo- or faux classifications. My letter described specific examples where documents were restricted from public dissemination because they would be embarrassing, not because they would jeopardize national security.

Today, we are going to hear from the GAO about the results of its investigation into the management of these types of documents by two agencies, the Department of Energy and the Department of Defense. As GAO will testify, neither of these departments have clear policies regarding the designations and neither has adequate oversight of their use.

Mr. Chairman, I have criticized the administration for its secrecy. I have even criticized the Republican Congress for failing to conduct meaningful oversight of the Bush administration. I think that has become a failure to do our constitutional responsibilities. It undermines accountability and it creates a climate in which secrecy flourishes. I think this is a hearing that is very much worth holding and I commend the chairman for calling the hearing. It won't undo the consequences of years of neglect, but I think it is an important step in the right direction and it illustrates how far things have gone, to the point now where it is so absurd that we can no longer ignore this business of classifying, reclassifying, declassifying, re-reclassifying, playing games with classifications, not for national security but simply to keep everybody in the dark, not just the enemies, but our own citizens and people in government itself.

So I commend you for holding this hearing and I am pleased that we are going to hear from these witnesses scheduled today who can maybe bring a greater light to the dark spot in the whole issue of openness in government and sunshine. Thank you.

Mr. SHAYS. I thank the gentleman.

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

Statement of Rep. Henry A. Waxman, Ranking Minority Member
Committee on Government Reform
Before the Subcommittee on National Security, Emerging Threats and International Relations Hearing on "Drowning in a Sea of Faux Secrets: Policies on Handling of Classified and Sensitive Information"

March 14, 2006

Thank you, Mr. Chairman, for holding this important hearing.

This week is "sunshine week," so it is particularly appropriate that we are focusing today on openness and transparency in government as bedrock principles of our democracy.

Unfortunately, sunshine rarely penetrates inside the current Administration. The Bush Administration's penchant for secrecy is legendary, and the examples are numerous. The Vice President refused to reveal which campaign contributors and energy executives had special access to his energy task force. The President rolled back Reagan-era regulations for the release of Presidential records. The Department of Health and Human Services withheld estimates of the true cost of the Medicare prescription drug legislation. And the Defense Department redacted hundreds of Halliburton overcharges from audits given to the United Nations.

In September 2004, I released a comprehensive report on secrecy in the Bush Administration. The report found that the nation's open government laws had been repeatedly eroded during the first four years of the Bush Administration, while the laws authorizing secret government action had been systematically expanded. These trends have continued — and worsened — in the months since I released the report.

Last month, researchers discovered that the Administration has been secretly removing thousands of previously declassified documents that had been publicly available on the shelves of the National Archives. Some of these documents were more than 50 years old and already had been published in books and journals.

According to these researchers, one of these documents is a 1948 memorandum regarding delays in implementing "Project Ultimate," a CIA program to drop propaganda leaflets out of hot air balloons to the citizens of Eastern Europe. This memo was published in a 1996 State Department volume.

Yet incredibly, this 58-year-old document has now been removed from the shelves, according to the researchers.

There are a lot of questions about the administration's actions to which we don't yet have the answers. Who oversees this program? Under what legal authority are they operating? And why is the order governing this program evidently still classified?

I hope we can begin to get answers to these questions at today's hearing.

Another important issue we will consider today is the Administration's abuse of designations such as "sensitive but unclassified" to block the public release of government information. Many of these designations have no basis in statute, no criteria for use, and no limitations on who can withhold documents using these designations.

Last year, the Chairman and I sought documents from three agencies — the Defense Department, the State Department, and the Department of Homeland Security — that had been restricted as "Sensitive but Unclassified" or "For Official Use Only." To date, we have received none of these documents.

It is particularly telling that in their responses, the agencies claimed they had no way to provide such information because they don't keep track of it. As another agency wrote: "There is no regulatory or other national policy governing the use of For Official Use Only

designation, as opposed to the controls on classified national security information."

A year ago, I wrote to the Chairman about abuses of pseudo-classifications. My letter described specific examples where documents were restricted from public dissemination because they would be embarrassing, not because they would jeopardize national security. Today, we will hear from GAO about the results of its investigation into the management of these types of documents by two agencies: the Department of Energy and the Department of Defense. As GAO will testify, neither of these departments has clear policies regarding the designations and neither has adequate oversight of their use.

I have been vocal in my criticism of the Republican Congress for failing to conduct meaningful oversight of the Bush Administration. The refusal of Congress to fulfill its constitutional oversight responsibilities undermines accountability. And it creates a climate in which secrecy flourishes. This hearing won't undo the consequences of years of neglect, but at least it is a step in the right direction.

Mr. Chairman, I thank you for holding this hearing on openness in government. I look forward to the testimony of today's witnesses.

Mr. SHAYS. At this time, the chair would recognize Mr. Kucinich, the ranking member of the committee.

Mr. KUCINICH. Thank you very much, Mr. Chairman. I might note to my good friend, Mr. Waxman, you just mentioned that they reclassified that information about dropping propaganda out of hot air balloons. I think the reason why they reclassified it is that they are still doing it here in Washington. [Laughter.]

I want to thank the chairman for holding the third subcommittee hearing on this important oversight issue, and I want to note that this hearing is being held during what American newspaper editors have declared as National Sunshine Week, but it may be that the administration's song will be, "The Sun Will Come Out Tomorrow," not today, so it is imperative that Congress exercises its oversight responsibility and that we hold Federal agencies accountable for the millions of classification and declassification decisions they exercise every day.

The results of our review can be measured through a variety of statistics, but in the end, we must ask two fundamental questions. First, do we still have an open government? And second, are we safer as a result of these classification decisions? I think the answer to both questions is no.

By any measure, the administration has been classifying documents at a dizzying pace. Under this administration, more agencies have been given authority to classify documents and over 50 new security designations, including "Sensitive But Unclassified" and "For Official Use Only" have been created. Over 4,000 Federal employees now have original classification authority, and nearly $8 billion a year is spent to classify documents, $8 billion. Meanwhile, declassification has slowed to a crawl.

But we must also look at what kind of information this administration is classifying. Is it sensitive, a threat to our national security if released to the public? According to researcher Matthew Aid, thousands of documents from the cold war era have been increasingly removed from the National Archives over the past 7 years and subsequently reclassified. Much of this trove consists of innocuous historical information from the cold war era and is being kept from the public's view. According to the Washington Post, even documents about the Cuban missile crisis, one of the most important events in our Nation's history, are still being denied to historians. It is well past the 25-year limit in which most Federal documents have to be declassified.

Declassification is an essential tool to watchdog the actions of our government. For example, documents declassified just last year concern Luis Posada Carriles, a CIA operative involved in the 1976 bombing of a Cubana Airlines flight that killed 73 passengers. They show the complicity and support our government gave to his violent acts. After escaping from a Venezuelan prison in 1985, Posada worked in El Salvador on the Iran-Contra program and he admitted to a string of hotel bombings in Havana and various assassination attempts of Fidel Castro.

Last year, Mr. Posada snuck into the United States and is attempting to seek asylum here. Despite requests from both Venezuela and Cuba to extradite him, the Department of Homeland Security has refused to deport him. In effect, the Bush administra-

tion—the Bush administration—is harboring an international terrorist, and documents released by the National Security Archives show the full extent of CIA involvement in those operations.

If this is how the administration treats so-called historical information, how do you think they treat materials that could inform public policy debates today or protect our Nation against terrorist threats? That is one of the reasons, Mr. Chairman, why I introduced a resolution of inquiry on the Dubai port deal. We want to know how it came about. Maybe the deal is dead, maybe it is not, but the public has a right to know how it came about in the first place and the only way you can do that is to get the public records.

In April 2004, only 1 day before Secretary Rice was forced to testify before the 9/11 Commission, the administration suddenly declassified a key memo from former Counterterrorism Chief Richard Clarke to Secretary Rice warning her about the al Qaeda threat and calling for a meeting of principal security heads. Mr. Clarke's memo had been written in January 2001, more than 9 months before the tragic attacks.

Let me give you another example. Last week, the Department of Justice released e-mails from David Kris, an Associate Deputy Attorney General with the knowledge of the administration's justifications for its domestic wiretapping program. Mr. Kris argues that the Department's arguments were weak, had a slightly after-the-fact quality to them, and even surmised that they reflected the Vice President's philosophy that the best defense is a good offense. Yet only following a Federal court order and a Freedom of Information lawsuit did the Justice Department search for and release unclassified documents that relate to justification of the eavesdropping program, and after 2½ months of searching, the Justice Department said it found only some e-mails and transcripts of public interviews with the Attorney General. The rest of the material apparently still remains classified.

Finally, a March 3rd Wall Street Journal editorial entitled, "Open the Iraq Files" highlights the fact that there are millions of documents captured in Iraq and Afghanistan, collectively referred to as the Harmony Program, which have now been classified. The Harmony Program supposedly contains information about Saddam Hussein's so-called weapons programs, about the Niger uranium connection, and even about Iraq's support of a terrorism program and lists of potential terrorists threats. These documents would undoubtedly better inform the American public and elected officials as we continue to debate our foreign policy in those parts of the world, yet you can bet they won't see any light of day anytime soon.

So our Nation is neither safer nor more open. We spend more and more each year to classify documents and declassify fewer and fewer Federal records. Moreover, the Government Accountability Office has told the Congress, and what journalists and historians report to us, is that implementation of classification policy is inconsistent. Training in classification procedures and Freedom of Information policies differ across Federal agencies. Review of classification decisions, supervision of officials, and cross-agency communication are sparse, at best.

Mr. Chairman, we need to take another look at the laws and regulations that guide classification policies. I believe the current sys-

tem is out of control. I hope we can work together in a bipartisan manner to reverse the momentum that we lost. Let us make sure sunshine is present throughout the Federal Government, not just for 1 week, but that it shines forth each and every day.

Thank you, and I want to welcome the witnesses, and I have, without objection, various documents that I want to submit into the record.

Mr. SHAYS. I thank the gentleman.

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

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

Hearing on "Drowning in a Sea of Faux Secrets: Policies on Handling of Classified and Sensitive Information"

March 14, 2006

Good afternoon. I'd like to thank the Chairman for holding the third Subcommittee hearing on this important oversight issue, and note that this hearing is being held during what American newspaper editors have declared as national "Sunshine Week."

It is imperative that Congress exercises its oversight responsibility and holds federal agencies accountable for the millions of classification and declassification decisions they exercise every day. The results of our review can be measured through a variety of statistics, but in the end, we must ask two fundamental questions: 1) Do we still have an open government?; and 2) Are we safer as a result of these classification decisions? I am disturbed to say that I believe the answers to both questions are clearly no.

By any measure, this Administration has been classifying documents at a dizzying pace. Under this Administration, more agencies have been given authority to classify documents, and over fifty new security designations, such as "Sensitive But Unclassified" and "For Official Use Only", have been created. Over 4,000 federal employees now have original classification authority, and nearly $8 billion a year is spent to classify documents. Meanwhile, declassification has slowed to a crawl.

But we must also look at what kind of information this Administration is classifying. Is all of it "sensitive" or a threat to our national security if released to the public? According to researcher Matthew Aid, thousands of documents from the Cold War era had been increasingly removed from the National Archives over the past seven years, and subsequently reclassified. Much of this trove consists of innocuous historical information ~~from the Cold War era, and is being kept from the public's view.~~ According to the Washington Post, even documents about the Cuban Missile crisis, one of the most important events in our nation's history, are still denied to historians, well past the 25-year limit in which most federal documents have to be declassified.

Declassification is an essential tool to watchdog the actions of our government. For example, documents declassified just last year concerning Luis Posada Carriles, a CIA operative involved in the 1976 bombing of a Cubana Airlines flight that killed 73 passengers, show the complicity and support our government gave to his violent acts. After escaping from a Venezuelan prison in 1985, Posada worked in El Salvador on the Iran-contra program under Lt. Col. Oliver North. He has admitted to a string of hotel bombings in Havana, and various assassination attempts of Fidel Castro.

Last year, Mr. Posada snuck into the U.S. and is attempting to seek asylum here. Despite requests by both Venezuela and Cuba to extrude him, the Department of Homeland Security has refused to deport him. In effect, the Bush Administration is harboring an international terrorist, and documents released by the National Security Archives show the full extent of CIA involvement in these anti-Castro operations.

If this is how the Administration treats so-called historical information, how do you think they treat materials that could inform public policy debates today or protect our nation against terrorist threats?

In April 2004, only one day before Secretary of State Rice was forced to testify before the 9-11 Commission, the Administration suddenly declassified a key memo from former counterterrorism chief, Richard Clarke, to Secretary Rice warning her about the al-Qaeda threat and calling for a meeting of principal security heads. Mr. Clarke's memo had been written in January of 2001, more than nine months before the tragic terrorist attacks.

Let me give you another example. Last week, the Department of Justice released email messages from David Kris, an associate deputy attorney general with knowledge of the Administration's justifications for its domestic wiretapping program. Mr. Kris argues that the Department's arguments were "weak," had a "slightly after-the-fact quality" to them, and even surmised that they reflected "the VP's philosophy that "the best defense is a good offense." Yet, only following a federal court order in a FOIA lawsuit did the Justice Department search for, and release unclassified documents that related to justification of the eavesdropping program. And after two and a half months of searching, the Justice Department said it found only some emails and transcripts of public interviews with the Attorney General. The rest of the material apparently still remains classified.

Finally a March 3 *Wall Street Journal* editorial titled "Open the Iraq Files" highlights the fact that there are millions of documents captured in Iraq and Afghanistan, collectively referred to as the "Harmony Program," which have now been classified. The Harmony Program supposedly contains information about Saddam Hussein's weapons programs, about the Niger-uranium connection, and even about Iraq's support of terrorism program, and lists of potential terrorist targets. These documents would undoubtedly better inform the American public and elected officials as we continue to debate our foreign policy in those parts of the world. Yet these won't see the light of day anytime soon either.

So, our nation is neither safer nor more open. We spend more and more each year to classify documents and declassify fewer and fewer federal records. Moreover, what GAO has told the Congress, and what journalists and historians report to us, it that implementation of classification policy is inconsistent. Training in classification procedures and FOIA policies differ across federal agencies. Review of classification decisions, supervision of officials, and cross-agency communication are sparse at best.

Mr. Chairman, we need to take another look at the laws and regulations that guide classification policy, for I believe the current system is out of control. I hope that we can work together in a bipartisan manner to reverse the momentum that we lost.

Let's make sure sunshine is present throughout the federal government not just for one week, but that it shines each and every day.

Thank you, and welcome to our witnesses testifying today.

[Insert March 12, 2006 *Washington Post* article into record]

[Place Posada documents in record]

[Place Clarke memo and Kris emails in record]

[Place March 3, 2006 Wall Street Journal editorial into record]

washingtonpost.com

Still Secret After All These Years

By Michael Dobbs
Sunday, March 12, 2006; B02

Advertisement

Government secrecy will not be an issue, I told myself optimistically as I began to research a history of the Cuban missile crisis.

After all, the classic showdown of the Cold War occurred more than four decades ago, well outside the 25-year period established by the administrations of both Bill Clinton and George W. Bush for the automatic release of everything but the most sensitive government documents. The Soviet Union has been consigned to the ash heap of history, and '60s-era defense technologies, such as the U-2 spy plane, are no longer considered secret.

How wrong I was.

It turns out that most government documents on the missile crisis -- including the principal Pentagon and State Department records collections -- are still classified. Hundreds of documents released to researchers a decade ago have since been withdrawn as part of a controversial -- itself secret -- reclassification program. And the backlog of Freedom of Information Act requests to the National Archives has grown to two, three or even five years.

Six months traveling across the country in pursuit of missile crisis records -- from the John F. Kennedy Library in Boston to the National Archives in College Park to the Air Force Historical Research Agency in Montgomery, Ala. -- spawns conflicting impressions. On the one hand, these institutions are part of a national treasure trove of archival riches. On the other, the system of declassifying government information has become so chaotic in recent years that it is difficult for outsiders, and even many insiders, to understand the logic behind it.

Thanks to the White House tapes declassified in 1996, I have eavesdropped on intimate conversations between President Kennedy and his aides as they struggled to respond to the deployment of Soviet rockets less than 100 miles from Key West. I have perused top-secret signals intelligence released by the National Security Agency, and page after page of U.S. invasion plans for Cuba, down to the gradient of the landing beaches and the Cuban "most wanted" list.

On the other hand, Air Force records describing the inadvertent penetration of Soviet air space by a U-2 at the very peak of the crisis are still secret. The files of former Kennedy military adviser Maxwell Taylor are full of withdrawal slips marked "Access restricted." An archival turf war between competing agencies has blocked access to the records of the State Department intelligence office.

The extent of the reclassification program only became clear late last month after a historian noticed that dozens of documents that he had previously copied from the National Archives had mysteriously disappeared from State Department boxes. The withdrawn records included several documents that had

already been published in official government histories, such as a 1948 CIA memo on using balloons to drop propaganda leaflets over Communist countries.

While the reclassification drive is intensely irritating to historians, an even bigger problem is the ripple effect such efforts have had on declassification. The routine declassification of government records has ground to a virtual standstill over the past few years because of the diversion of resources to reexamining previously released records. Documents that would have been released routinely a decade ago are trapped in a bureaucratic twilight zone.

A good example of this phenomenon are the thousands of pages of Secretary of State and Secretary of Defense records on the missile crisis transferred to the National Archives more than five years ago, but currently stored in confidential stacks. Archives officials told me that they will probably be able to release part of that collection in the next few months, but the bulk must go through an elaborate interagency screening process that could take several years.

It is instructive to compare the situation of Cuban missile crisis records with that of World War II records. The last great wartime secret -- the existence of the Enigma code-breaking machine -- was officially revealed in 1974, 29 years after the end of the war. By 1990, 45 years after the victory over Nazi Germany, the wartime records were almost completely accessible. An equivalent amount of time has passed since the missile crisis, but archival access is much more limited.

While the reclassification drive has accelerated under the Bush administration, particularly since 9/11, it actually began under Clinton. The initial impulse came from the Kyl-Lott amendment, passed by Congress in 1998 in response to a scandal involving the alleged leaking of nuclear secrets to China. The CIA and the Pentagon took advantage of the new climate to look for information that had supposedly been released without their consent, and demanded its withdrawal.

On March 2, the National Archives announced yet another initiative to respond to the flurry of bad publicity about reclassification -- this time to check whether documents have been improperly withdrawn from circulation. While the initiative has been welcomed by historians, it also carries dangers. A vast amount of energy, time and taxpayer money is being wasted reviewing and re-reviewing the same documents.

If the missile crisis is any guide, the whole laborious process could be greatly speeded up by better coordination between agencies, improved data management, and what one frustrated National Archives records officer terms the application of "a little common sense." Some agencies -- the Air Force is a prime example -- lack an effective system for tracking documents previously declassified under the Freedom of Information Act.

By contrast, the CIA, which is often accused of dragging its feet, has found a way to make declassified documents instantly available to all researchers. The agency has a public database that includes day-by-day intelligence analyses on the deployment of Soviet missiles in Cuba, based on reconnaissance flights by U-2s and low-level planes.

Archival work is a little like tackling a giant jigsaw puzzle. If you are patient enough, you can eventually make out the picture, even if many of the pieces are missing. In the case of the missile crisis, I have assembled enough of the puzzle to be confident that few, if any, of the missing pieces contain national security information that could be useful to an enemy -- the criterion established by both Bush and Clinton for continuing to classify more than 25-year-old secrets.

So why, if the puzzle is largely resolved, am I -- and other researchers -- making such a fuss? Because history is not just about the big picture. It is also about the small stuff, thousands upon thousands of individual acts of bravery and skill and, yes, foolishness. In order to make sense of the anguished White House debates between Kennedy and his advisers in October 1962, you need to understand how the Cold War was actually fought, by the generals, the spies, the reconnaissance pilots. It is the details that make history come alive -- and in far too many cases those details are still being hidden from us.

dobbspost@gmail.com

Michael Dobbs is a Washington Post reporter on leave to write a book about the Cuban missile crisis.

© 2006 The Washington Post Company

Ads by Google

Military College Credit
Your military training can count toward a degree. Online, anywhere.
www.universityofphoenix.com

Search military records
Find enlistment records, gravesites regimental histories and more.
Ancestry.com

Military Caps
Great Selection of Army, Navy, Air Force, Marine Caps at great prices.
www.CopShoes.com

~~SECRET~~ CIA HISTORICAL REVIEW PROGRAM RELEASE AS SANITIZED 1997 Rwk 5-27-97

CITE TDFR DB-315/06286-76

DIST 22 JUNE 1976

REPORT CLASS ~~S E C R E T~~--WARNING NOTICE-SENSITIVE INTELLLIGENCE SOURCES AND METHODS INVOLVED--NOT RELEASABLE TO FOREIGN NATIONALS--NOT RELEASABLE TO CONTRACTORS OR CONTRACTOR/CONSULTANTS

COUNTRY: *CUBA/PANAMA/DOMINICAN REPUBLIC

DOI: 21 JUNE 1976

SUBJECT: POSSIBLE PLANS OF CUBAN EXILE EXTREMISTS TO BLOW UP A CUBANA AIRLINER

ACQ: (22 JUNE 1976)

SOURCE: A BUSINESSMAN WITH CLOSE TIES TO THE CUBAN EXILE COMMUNTIY. HE IS A USUALLY RELIABLE REPORTER.

1. A CUBAN EXILE EXTREMIST GROUP, OF WHICH ORLANDO B O S C H IS A LEADER, PLANS TO PLACE A BOMB ON A CUBANA AIRLINE FLIGHT TRAVELLING BETWEEN PANAMA AND HAVANA. ORIGINAL PLANS FOR THIS OPERATION CALLED FOR TWO BOMBS BEING PLACED ON THE 21 JUNE 1976 CUBANA FLIGHT NUMBER 467, WHICH WAS SCHEDULED TO LEAVE PANAMA AT 11:15 A.M. LOCAL PANAMA TIME.

2. BOSCH IS CURRENTLY RESIDEING IN THE DOMINICAN REPUBLIC.

(SOURCE COMMENT: BOSCH WAS ARRESTED IN COSTA RICA IN FEBRUARY. IT IS NOT KNOWN WHEN HE WAS RELEASED.)

3. FIELD DISSEM: SENT TO [16-7,10] 56-8-11

~~S E C R E T~~

MICROFILM CARD - REPRODUCTION

/07 OBSOLETE PREVIOUS EDITIONS

IN 958679

TDFIR DB-315/06286-76

WARNING NOTICE
SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED

PAGE 2 OF 2 PAGES

~~SECRET~~
(classification)

FURTHER DISSEMINATION AND USE OF THIS INFORMATION SUBJECT TO CONTROLS STATED AT BEGINNING AND END OF REPORT.

REPORT CLASS ~~S E C R E T~~--WARNING NOTICE-SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED--NOT RELEASABLE TO FOREIGN NATIONALS--NOT RELEASABLE TO CONTRACTORS OR CONTRACTOR/CONSULTANTS.

CLASSIFIED BY RECORDED REPORTING OFFICER. XGDS-2.

ADVANCE COPY TRANSMITTED TO STATE DIA ARMY NAVY AIR JCS SWS NSA TREAS FAA SS/ID FBI CIA/OPSCENTER.

~~SECRET~~

APERTURE CARD REPRODUCTION

NARA MD DATE 1-19-05

SECRET

2-469-6

HQ0034 2830300

PP MM SJ

DE HQ

P 090650Z OCT 76

FM DIRECTOR

TO MIAMI PRIORITY

SAN JUAN PRIORITY

RUEBWJA/ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION

ATTN: INTERNAL SECURITY SECTION

ATTN: GENERAL CRIMES SECTION

RUEAIIA/DIRECTOR, CIA

RUEOGSA/FEDERAL AVIATION ADMINISTRATION

RUEHC/SECRETARY OF STATE

BT

S E C R E T

SECTION 1 OF 2

9/8/97
CLASSIFIED BY 5668-SLO/GCL
DECLASSIFY ON: 25X
(5668, SLO/GCL 8/25/98 JFK)

UNKNOWN SUBJECTS; SUSPECTED BOMBING OF CUBANA AIRLINES DC-8 NEAR BARBADOS, WEST INDIES, OCTOBER 6, 1976, NM - CUBA - WEST INDIES.

BY TELETYPE OCTOBER 8, 1976 LEGAT CARACAS ADVISED AS FOLLOWS.

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

Classified by 5668/SLO/GCL
Declassify on: OADR
7/14/95 5668/SLO/GCL #214326

(13)

SECRET

2-469

PAGE TWO S E C R E T

HERNAN RICARDO LOZANO IS A NEWS PHOTOGRAPHER AND FREE-LANCE REPORTER AFFILIATED WITH THE MAGAZINE "VISION," AND HE IS ALSO EMPLOYED AS AN INDUSTRIAL INVESTIGATOR BY INVESTIGACIONES COMERCIALES E INDUSTRIALES, C.A. (ICI), AN INDUSTRIAL SECURITY FIRM OPERATED BY LUIS POSADA, FORMER HEAD OF [redacted] (S) E

1B 1C

POSADA, A CUBAN EXILE WHO IS NOW A VENEZUELAN CITIZEN, IS STRONGLY ANTI-CASTRO AND WAS SUSPECTED OF HAVING BEEN THE MAIN SUPPORTER OF ORLANDO BOSCH AVILA DURING BOSCH'S PRESENCE IN VENEZUELA PRIOR TO HIS ARREST ON NOVEMBER 19, 1975. LEGAT BECAME ACQUAINTED WITH [redacted] (S) IN THE COURSE OF OFFICIAL BUSINESS DURING PERIOD [redacted] (S) E

1B 1C

HERNAN RICARDO LOZANO FIRST BECAME KNOWN TO LEGAT IN APPROXIMATELY JUNE, 1974, WHEN HE CONTACTED LEGAT FOR ASSISTANCE IN EXPEDITING THE PROCESSING OF A VISA TO THE U.S. THAT HAD BEEN REQUESTED FOR THE MINOR SON OF THE THEN [redacted] (S) E

1B 1C

LEGAT WAS LED TO BELIEVE RICARDO WAS AN ACTIVE MEMBER OF DISIP AND ASSISTANCE WAS PROVIDED THAT RESULTED IN THE PROMPT ISSUANCE OF A VISA TO THE [redacted] (S) CHILD. E

RICARDO RECONTACTED LEGAT A FEW WEEKS LATER TO EXPRESS HIS APPRECIATION FOR ASSISTANCE PREVIOUSLY RENDERED, AND LEGAT THEN BE-

RELEASED PER P.L.-102-526(JFK ACT)
NARA MD DATE 1·19·05

2-469

PAGE THREE S E C R E T

CAME AWARE RICARDO WAS MERELY AN AUXILIARY [redacted] (S), AND THAT HE WAS ACTUALLY IN THE PERSONAL SERVICE OF LUIS POSADA. RICARDO REVEALED HE WAS ALSO A NEWSPAPER REPORTER AND PHOTOGRAPHER AFFILIATED WITH THE MAGAZINE "VISION," AND INDICATED HE DEVOTED MOST OF HIS TIME RESEARCHING NEWS ARTICLES INTENDED TO DISCREDIT THE CASTRO GOVERNMENT. HE CLAIMED PARTIAL RESPONSIBILITY FOR A NEWSPAPER ARTICLE THAT APPEARED IN A CARACAS NEWSPAPER ABOUT THAT TIME, REVEALING THE PRESENCE OF CUBAN INTELLIGENCE OFFICERS IN CUBAN EMBASSY IN CARACAS.

RICARDO CONTACTED LEGAT APPROXIMATELY FOUR TIMES AFTER THE INITIAL VISIT, AND ON TWO OCCASIONS FURNISHED PHOTOGRAPHS AND BIOGRAPHICAL DATA ON MEMBERS OF THE CUBAN EMBASSY WHICH WERE OBVIOUSLY OBTAINED FROM [redacted] (S) DURING ONE VISIT, RICARDO SUGGESTED LEGAT MIGHT WISH TO MAKE SOME SUGGESTIONS REGARDING COURSES OF ACTION THAT MIGHT BE TAKEN AGAINST THE CUBAN EMBASSY IN CARACAS BY AN ANTI-CASTRO GROUP OF WHICH HE FORMED PART. LEGAT INFORMED RICARDO SUCH WAS NOT PART OF THE FUNCTION OF THE LEGAL ATTACHE'S OFFICE, AND THAT IN ANY EVENT, LEGAT PERSONALLY ABHORRED TERRORIST ACTIVITIES REGARDLESS OF WHOM THEY MIGHT BE DIRECTED AGAINST. LEGAT POINTED OUT TO RICARDO THAT THE U.S. GOVERNMENT WAS DOING EVERYTHING IT COULD TO PREVENT DISRUP-

SECRET

RELEASED PER P.L. 102-526(JFK ACT)
NARA MA DATE 1-19-05

2-469

PAGE FOUR S E C R E T

TIVE AND TERRORIST ACTIONS BY ANTI-CASTRO GROUPS IN THE US. RICARDO DID NOT AGAIN REPEAT THE SUGGESTION. (U)

LEGAT WAS SURPRISED BY APPEARANCE OF RICARDO AT AMERICAN EMBASSY ON SEPTEMBER 30, 1976. THE LAST CONTACT WITH RICARDO HAD BEEN EARLY IN DECEMBER, 1975, WHEN RICARDO TELEPHONED LEGAT AND INVITED HIM TO A LUNCH OF VENEZUELAN SPECIALTIES PREPARED DURING THE HOLIDAY SEASON. LEGAT DECLINED INVITATION, CITING A PREVIOUS ENGAGEMENT. (U)

ON SEPTEMBER 30, 1976, RICARDO INFORMED LEGAT HE HAD A PHOTOGRAPHIC ASSIGNMENT FOR "VISION" MAGAZINE IN JAMAICA AND WAS IN NEED OF A VISA TO THE US SINCE HE PLANNED A TWO-DAY STOPOVER IN PUERTO RICO

HE SAID HE HAD FIRST CONTACTED A TRAVEL AGENCY TO MAKE ARRANGEMENTS FOR THE VISA, BUT WAS TOLD THE PROCESS WOULD TAKE THREE DAYS, AND SINCE HE EXPECTED TO DEPART CARACAS ON OCTOBER 1, 1976, HE REQUESTED LEGAT'S ASSISTANCE IN EXPEDITING A VISA FOR HIM. AS LEGAT WAS OCCUPIED WITH OTHER MATTERS, HE ACCEPTED RICARDO'S PASSPORT AND VISA APPLICATION FORM, PROMISING TO LOOK IT OVER AND TO SUBSEQUENTLY ADVISE RICARDO OF ANY FURTHER REQUIREMENTS. IN REVIEWING THE PASSPORT AND APPLICATION FORM, LEGAT NOTED RICARDO HAD NOT PREVIOUSLY TRAVELED TO THE US. THE PASSPORT DID REFLECT HOWEVER THAT RICARDO HAD TRAVELED FROM CARACAS TO PORT-OF-SPAIN, TRINIDAD, ON AUGUST 29, (U)

SECRET

2-469

PAGE FIVE S E C R E T

1976, AND HAD RETURNED TO CARACAS ON SEPTEMBER 1, 1976. LEGAT RECALLED THAT THE BOMBING OF THE GUYANESE CONSULATE IN PORT-OF-SPAIN HAD OCCURRED AT APPROXIMATELY 10:15 AM ON SEPTEMBER 1, 1976, AND WONDERED IN VIEW OF RICARDO'S ASSOCIATION WITH LUIS POSADA, IF HIS PRESENCE THERE DURING THAT PERIOD WAS COINCIDENCE. (U)

ON THE HUNCH IT MIGHT BE OF POSSIBLE FUTURE INTEREST, LEGAT TOOK THE LIBERTY OF MAKING XEROX COPIES OF RICARDO'S PASSPORT AND VISA APPLICATION FORM. IN CONSULTING WITH CHIEF OF NONIMMIGRANT VISA SECTION, GLADYS LUJAN, LEGAT INFORMED HER HE WISHED NO SPECIAL CONSIDERATION FOR RICARDO, AND REQUESTED THE ISSUANCE OF A VISA TO HIM BE CONSIDERED ON ITS OWN MERITS. MRS. LUJAN STATED RICARDO WOULD NEED ONLY AN EMPLOYMENT LETTER INDICATING HE WAS GAINFULLY EMPLOYED IN VENEZUELA. (U)

WHEN RICARDO REAPPEARED AT EMBASSY ON AFTERNOON OF SEPTEMBER 30, 1976, HE WAS INFORMED OF REQUIREMENT OF A LETTER OF EMPLOYMENT, AND HE WAS INSTRUCTED TO GO DIRECTLY TO CONSULAR SECTION WITH HIS DOCUMENTS WHEN HE HAD THEM IN ORDER. HE INDICATED HE WOULD OBTAIN THE EMPLOYMENT LETTER AND WOULD RETURN TO THE CONSULARSECTION ON THE MORNING OF OCTOBER 1, 1976. (U)

ON THE MORNING OF OCTOBER 1, 1976, RICARDO AGAIN APPEARED AT THE

SECRET

NARA

2-469

PAGE SIX S E C R E T

RECEPTIONIST DESK IN THE LOBBY OF THE EMBASSY AND REQUESTED TO SEE LEGAT. LEGAT PROCEEDED TO LOBBY, WHERE RICARDO SAID HE HAD BEEN TOLD BY ONE OF THE VICE CONSULS HIS EMPLOYMENT LETTER WAS NOT EXPLICIT ENOUGH, AND WHEN HE INFORMED HER HE WAS ACQUAINED WITH LEGAT, THE VICE CONSUL SUGGESTED HE RECONTACT LEGAT AND ASK HIM TO SPEAK WITH HERJS RICARDO DISPLAYED A LETTER WRITTEN ON ICI LETTERHEAD STATIONERY AND SIGNED BY LUIS POSADA ATTESTING MERELY RICARDO WAS AN ICI EMPLOYEE. LEGAT THEN COMMUNICATED WITH VICE CONSUL WHO WISHED TO KNOW IF LEGAT BELIEVED RICARDO WOULD RETURN TO VENEZUELA AFTER HIS VISIT IN THE US, OR IF HE WAS LIKELY TO REMAIN THERE ILLEGALLY. LEGAT INFORMED THE VICE CONSUL HE HAD NO REASON TO BELIEVE RICARDO WOULD NOT RETURN TO CARACAS. THE VICE CONSUL INDICATED IN THAT CASE A VISA WOULD BE ISSUED TO RICARDO, AND HE WAS ASKED TO RETURN TO THE CONSULAR SECTION. UPON TAKING LEAVE OF LEGAT, RICARDO INDICATED HE MIGHT ALSO VISIT NEW YORK CITY BEFORE RETURNING TO CARACAS, AND MENTIONED IN PASSING THAT BESIDES JAMAICA, HE MIGHT ALSO BE VISITING BARBADOS IN CONNECTION WITH HIS PICTORIAL ASSIGNMENT FOR "VISION." RICARDO WAS NOT SEEN AFTER THAT. 3/4

BT

SECRET

2-469

PAGE SEVEN S E C R E T

IN A CONVERSATION WITH AN [redacted] (S) ON OCTOBER 1, 1976, E
LEGAT BROACHED THE SUBJECT OF RICARDO AND OF THE FAINT SUSPICION THAT
1B RICARDO MAY HAVE BEEN SOMEHOW INVOLVED IN THE BOMBING OF THE GUYANESE
1C CONSULATE IN PORT-OF-SPAIN. LEGAT ADMITTED THERE WAS NO SUBSTANTIVE
EVIDENCE OF RICARDO'S IMPLICATION, BUT THAT THE COINCIDENCE OF HIS
PRESENCE THERE AT THE APPROPRIATE TIME, COUPLED WITH HIS EMPLOYMENT
RELATIONSHIP WITH LUIS POSADA, HAD GIVEN LEGAT CAUSE TO WONDER.
THE [redacted] (S) RELATED [redacted] (S) HAD NO REASON TO BELIEVE RICARDO WAS E,
THE CALIBER OF INDIVIDUAL THAT WOULD BE UTILIZED IN SUCH AN OPERATION,
AND THAT RICARDO WAS NOT KNOW TO BE INVOLVED IN SUCH ACTIVITIES, IN
SPITE OF HIS ASSOCIATION WITH POSADA. (U)

ON OCTOBER 3, 1976, A CONFIDENTIAL SOURCE ABROAD ADVISED HE
HAD DISCOVERED THAT THE INDIVIDUAL ARRESTED IN TRINIDAD, AND WHO
IS IN POSSESSION OF THE VENEZUELAN PASSPORT ISSUED TO JOSE VAZQUEZ
GARCIA, IS ACTUALLY HERNAN RICARDO LOZANO. HE SAID HE DETERMINED
THAT RICARDO AND FREDDY LUGO, THE OTHER VENEZUELAN ARRESTED IN
TRINIDAD, HAD BEEN PART OF THE SUPPORT GROUP IN THE SABOTAGE
OPERATION AGAINST THE CUBANA AIRLINER IN BARBADOS. HE SAID THE
OPERATION HAD NOT GONE AS PLANNED BECAUSE IT WAS INTENDED THAT
THE BOMB SHOULD EXPLODE BEFORE THE AIRCRAFT TOOK OFF FROM BARBADOS.
THE SOURCE STATED THAT APPARENTLY THE TIMING MECHANISM ON THE BOMB
HAD NOT BEEN PROPERLY SET. (U)

SECRET

RELEASED PER P.L-102-526(JFK ACT)
NARA [illegible] DATE 5/4/05

Reproduced at the National Archives

October 18, 1976

DRAFT
SECRET
SENSITIVE

MR WARREN
CIA/DDO/WH

Ray,
Please have this checked for accuracy
filling in missing parts and facts.
Hal Saunders wants to be able
to assure the Secretary that the
memo has your full concurrence.
Noon deadline
Francis

To: The Secretary

From: INR - Harold H. Saunders

Castro's Allegations

In his speech of October 15, Fidel Castro made the following allegations concerning CIA involvement in the bombing and crash of a Cubana Airlines plane on October 6 off Barbados:

--"Well-informed Venezuelan sources" had communicated to the Cubans that Hernan Ricardo Lozano (one of the men arrested in Trinidad in connection with the bombing of the plane) was a CIA agent and had handled reports from the CIA many times.

--Hernan Ricardo is an associate of Felix Martinez Suarez, who is reputed to be a CIA agent in Venezuela.

--"The recruitment of citizens and the utilization of other countries' territories to conduct such acts are methods characteristic of the CIA. At the beginning we were uncertain whether the CIA had directly organized the sabotage or had carefully prepared it through its covert organization formed

CIA HAS NO OBJECTION TO DECLASSIFICATION AND/OR RELEASE OF CIA INFORMATION IN THIS DOCUMENT AS SANITIZED
Jm 41457

FOIA/PA NO
Classified by Secretary
Declassify on: OADR
1/26/96

2-2-73

RELEASED PER P.L-102-526(JFK ACT)
NARA DATE 5/4/05
Reproduced at the National Archives

by Cuban counterrevolutionaries. Now we decidedly believe the first assumption is correct. The CIA directly participated in the destruction of the Cubana aircraft in Barbados."

--The principal leaders of Cuban exile terrorist groups are closely linked through the CORU organization to CIA activities against Cuba.

In his speech, Castro did not make any specific allegations concerning a USG relationship with Orlando Bosch, or Luis Posada (two Cuban exile activists who were arrested by Venezuelan authorities in connection with the Cubana crash). However, the link with Bosch is implied since he is reported to be chief of CORU, the umbrella organization of Cuban exile terrorists.

Individuals Allegedly Involved

Hernan Ricardo Lozano

a. Involvement in the Crash: He was arrested in Trinidad on suspicion of having planted a bomb in the Cubana plane. Caracas radio announced on October 18 that he confessed to sabotaging the airliner. A [redacted] (S) source in Caracas reports that Ricardo may have been trained in the use of explosives and investigative techniques by Luis Posada. [redacted] (S)

IB per CIA

RELEASED PER P.L.-102-526(JFK ACT)
NARA DATE 5/4/05

Reproduced at the National Archives

[redacted]

[redacted] (S)

Ricardo, a Venezuelan citizen, is a photographer employed by Posada in his industrial security firm in Caracas. A [redacted] (S) source says that Ricardo is also a part time employee of the Venezuelan Intelligence Service (DISIP). He reportedly gathered photographic material on groups and individuals of interest to DISIP and the Venezuelan Government. He was hired by DISIP when Pasada was an official of that organization. The [redacted] (S) source says that the Venezuelan Government is concerned and would be faced with serious problems if these connections become public knowledge.

b: Relationship with US: [redacted] (S) The US Legal Attache in Caracas, Joseph Leo, says that he has had some dealings with Ricardo for help in expediting visa applications [redacted]

[redacted] (S) During one visit, Ricardo attempted to solicit suggestions from the Legal Attache on activities which might be directed against the Cuban Embassy by an anti-Castro group to which he belonged. Leo says he discouraged Ricardo, pointing out that the US Government was attempting to prevent disruptive and

RELEASED PER P.L-102-526(JFK ACT)
NARA DATE 5/4/05
Reproduced at the National Archives

terrorist activities by anti-Castro groups in the US, and Ricardo never repeated the suggestion.

Freddy Lugo

a. Involvement in the crash: Lugo was arrested in Trinidad with Ricardo on suspicion of having planted the bomb aboard the Cubana plane. A [redacted] (S) source alleges that Lugo apparently was only peripherally involved in the bombing and is not considered to be one of the leading participants.

1B pou CPA

Lugo, a Venezuelan citizen, is also a photographer employed by Posada's company. According to [redacted] (S) source, he also worked for DISIP under the same arrangements noted above for Ricardo.

b. Relationship with US: [redacted] (S) The name and phone number of US Legal Attache Leo were discovered in Lugo's address book when he was arrested in Trinidad. Leo says that he has had no contact with Lugo and speculates that his name and phone were furnished to Lugo by Posada.

Luis Posada Carriles

a. Involvement in Crash: Posada was arrested on October 14 in Venezuela along with Orlando Bosch and three others accused of conspiring to sabotage the plane. Posada, a Cuban exile who is now a Venezuelan citizen, is vehemently anti-Castro and is suspected of having been the main supporter of Bosch during the latter's stay in Venezuela prior to being

RELEASED PER P.L-102-526(JFK ACT)
NARA [illegible] DATE 5/4/05

Reproduced at the National Archives

SENSITIVE

arrested in November 1974. Posada was formerly chief of the counterintelligence division of the Venezuelan intelligence service, DISIP.

b. Relationship with US. [redacted] OIA

[redacted] When he lost his position in DISIP in [redacted] (S)

says: [redacted] 3/12/98

[redacted] declined to assist Posada on a visa matter. (S)

The US army attache has also used a Posada business partner (also a Cuban exile, whose name we do not have) as an informant (though not as an agent).

Our Legal Attache (Joseph Leo) became acquainted with Posada during the latter's employment [redacted] (S) and after his resignation, Posada continued to contact Leo on rare occasions, usually in order to obtain personal service in regard to visa requests for relatives and business associates, the last being Ricardo on ~~October 1, 1976~~ September 30, 1976 and October 1, 1976. Leo says he has seen Posada on about three occasions since 1973, the last being in June 1976 when Posada inquired if the FBI had interest in a Venezuelan who had hired two of his "operatives" as body guards. [redacted]

OIA Code Chart

RELEASED PER P.L-102-526(JFK ACT)
NARA DATE 5/4/05
Reproduced at the National Archives

Orlando Bosch

a. Involvement in Crash: As noted above, Bosch was arrested in Venezuela for alleged involvement in the Cubana crash. In late June, a CIA source reported that an exile group headed by Bosch planned to bomb a Cubana flight between Panama and Havana. An FBI source has alleged that one attempt was made but the bomb did not detonate. A second try occurred in Jamaica on July 9, but the bomb exploded before the suitcase in which it was carried was put aboard the plane.

According to [redacted] Venezuelan President Carlos Andres Perez is said to be sympathetic to Bosch and has permitted him to travel freely in the country and solicit funds with the understanding that Venezuela would not be used as a base of operations or place of refuge. Bosch reportedly promised not to engage in terrorist activity while in Venezuela and received a token $500 contribution from Perez. [redacted] reported that after Bosch's arrival in Caracas in September, he stated during a fund raising dinner that "Now that our organization has come out of the Letelier job looking good, we are going to try something else." A few days later, Posada allegedly said, "We are going to hit a Cuban airliner" and "Orlando (Bosch) has the details.".

b. Relationship with US. [redacted] The US is currently attempting to have Bosch deported from Venezuela

RELEASED PER P.L-102-526(JFK ACT)
NARA DATE 5/4/05
Reproduced at the National Archives

to the US, where he is subject to immediate imprisonment for parole violation.

Frank Castro

a. Involvement in Crash: Venezuelan officials reportedly believe that Castro, (head of the FLNC terrorist organization, a component group in CORU) is deeply involved in the crash, though we have no details of his supposed involvement. Frank Castro was in Venezuela in late September 1976 and in mid-October was back in Miami. Frank Castro has admitted to FBI agents that he met with Bosch in Caracas on September 26 or 27, but denies any personal knowledge of the bombing of the Cubana plane.

b. Relationship with US: [redacted] who is an American citizen with permanent residence in Santo Domingo.

Orlando Garcia and Ricardo Morales Navarrete

a. Involvement in Crash: Orlando Garcia is President Perez' security and intelligence advisor, and Morales is Garcia's deputy; both are Cuban exiles who are now Venezuelan citizens. [redacted] claims that Garcia was directed to protect and assist Bosch during his stay in Venezuela. [redacted] reported that Garcia and Posada met Bosch upon his arrival and escorted him to his hotel. Both Garcia and Morales reportedly attended the fund-raising dinner during which Bosch allegedly made the remark about the "Letelier job," and after the Cubana

RELEASED PER P.L-102-526(JFK ACT)
NARA DATE 5/4/05
Reproduced at the National Archives

crash Garcia may have made an effort to get Bosch out of Venezuela. It is possible, therefore that Garcia and/or Morales may have known in advance about the operation which led to the bombing of the plane.

b. Relationship with US:

Felix Martinez Suarez

a. Involvement in Crash: None, except by the alleged association with Ricardo, contained in Fidel Castro's charges.

b. Relationship with US: [redacted]

Castro's allegation regarding CORU: With regard to Castro's charge on CIA links with CORU, an FBI report of September 17 states that "a confidential source abroad" claims to have been told by Roberto Carballo (leader of the Association of Veterans of the Bay of Pigs, AVBC, one of the component organizations of CORU) that in July of this year Carballo and three other Cuban exiles had been approached by representatives

RELEASED PER P.L-102-526(JFK ACT)
NARA DATE 5/4/05
Reproduced at the National Archives

of the CIA who informed them that CIA was dissatisfied with all the acts of sabotage being carried out at random and ordered them to disassociate themselves from Bosch and CORU. The source alleged that during the week of September 12-18 Carballo and three other Cuban exiles were in Washington to confer with representatives of the CIA on plans to be carried out by the action arm of the AVBC, for which financing was to come from CIA. The FBI report concludes with a request that the CIA advise if it has "active operational interest in AVBC as described above."

CIA says that this report is false and the Agency has no active operational interest in the AVBC. According to CIA, a representative of a group of Cuban exiles did telephone into the Agency in September 1976 requesting contact for an unspecified reason, but the contact did not take place and the callers were discouraged from further attempts to telephone the Agency.

RELEASED PER P.L-102-526(JFK ACT)
NARA ___ DATE 5/4/05

Reproduced at the National Archives

9:30 AM

SECRET/SENSITIVE

October 19, 1976

Additional Questions (answers and comments needed by late morning, October 20)

Cuban Airlines

1. Has CIA had any relationship with Posada's investigative agency or any other business he may have had?

2. [redacted] (S) 23,4 24 10

1B per CIA

3. [redacted] (S) 24,4,2 8

4. Does the CIA believe that the source of TDFIR DB-315/10256 deliberately, delayed passing on Bosch's and Posada's remarks about hitting a Cuban plane until after the incidents?

5. Does the CIA have any additional relevant information on any of the people named in the draft memorandum, or any other information relating to the sabotage of the plane, which it has not yet disseminated in TDFIR form?

6. Would CIA please provide whatever information it has concerning Orlando Garcia and Ricardo Morales so that para b on page 8 of the draft memorandum can be completed?

FBI INFORMATION CONTAINED HEREIN IS UNCLASSIFIED DATE ___ BY ___

CIA HAS NO OBJECTION TO DECLASSIFICATION AND/OR RELEASE OF THIS DOCUMENT AS SANITIZED K 3/13/98

2-2173

NOT RECORDED
23 MAY 17 1977

CIA HAS NO OBJECTION TO DECLASSIFICATION AND/OR RELEASE OF CIA INFORMATION IN THIS DOCUMENT. AS SANITIZED JM 4/14/97

File

SECRET/SENSITIVE

70 MAY 19 1977

~~SECRET~~ CIA HISTORICAL REVIEW PROGRAM RELEASE AS SANITIZED 1997 Rwk 5-27-97

CITE TDRN DB-315/06286-76

DIST 22 JUNE 1976

REPORT CLASS ~~S E C R E T~~--WARNING NOTICE-SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED--NOT RELEASABLE TO FOREIGN NATIONALS--NOT RELEASABLE TO CONTRACTORS OR CONTRACTOR/CONSULTANTS

COUNTRY: *CUBA/PANAMA/DOMINICAN REPUBLIC

DOI: 21 JUNE 1976

SUBJECT: POSSIBLE PLANS OF CUBAN EXILE EXTREMISTS TO BLOW UP A CUBANA AIRLINER

ACQ: (22 JUNE 1976)

SOURCE: A BUSINESSMAN WITH CLOSE TIES TO THE CUBAN EXILE COMMUNTIY. HE IS A USUALLY RELIABLE REPORTER.

1. A CUBAN EXILE EXTREMIST GROUP, OF WHICH ORLANDO B O S C H IS A LEADER, PLANS TO PLACE A BOMB ON A CUBANA AIRLINE FLIGHT TRAVELLING BETWEEN PANAMA AND HAVANA. ORIGINAL PLANS FOR THIS OPERATION CALLED FOR TWO BOMBS BEING PLACED ON THE 21 JUNE 1976 CUBANA FLIGHT NUMBER 467, WHICH WAS SCHEDULED TO LEAVE PANAMA AT 11:15 A.M. LOCAL PANAMA TIME.

2. BOSCH IS CURRENTLY RESIDEING IN THE DOMINICAN REPUBLIC.

(SOURCE COMMENT: BOSCH WAS ARRESTED IN COSTA RICA IN FEBRUARY. IT IS NOT KNOWN WHEN HE WAS RELEASED.)

3. FIELD DISSEM: SENT TO [16-7,10] 56-8-11

~~S E C R E T~~

NOT TO BE CARD REPRODUCTIONS

.07 OBSOLETE PREVIOUS EDITIONS

IN 958679

TDFIR DB-315/06286-76

WARNING NOTICE
SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED

PAGE 2 OF 2 PAGES

~~SECRET~~
(classification)

FURTHER DISSEMINATION AND USE OF THIS INFORMATION SUBJECT TO CONTROLS STATED AT BEGINNING AND END OF REPORT.

REPORT CLASS ~~S E C R E T~~--WARNING NOTICE-SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED--NOT RELEASABLE TO FOREIGN NATIONALS--NOT RELEASABLE TO CONTRACTORS OR CONTRACTOR/CONSULTANTS.

CLASSIFIED BY RECORDED REPORTING OFFICER. XGDS-2.

ADVANCE COPY TRANSMITTED TO STATE DIA ARMY NAVY AIR JCS SWS NSA TREAS FAA SS/ID FBI CIA/OPSCENTER.

~~SECRET~~

APERTURE CARD REPRODUCTION

NARA mD DATE 1·19·05

2-469-6

HQ0034 2830800

PP MM SJ

DE HQ

P 090650Z OCT 76

FM DIRECTOR

TO MIAMI PRIORITY

SAN JUAN PRIORITY

RUEBWJA/ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION

ATTN: INTERNAL SECURITY SECTION

ATTN: GENERAL CRIMES SECTION

RUEAIIA/DIRECTOR, CIA

RUEOGBA/FEDERAL AVIATION ADMINISTRATION

RUEHC/SECRETARY OF STATE

BT

S E C R E T

SECTION 1 OF 2

9/8/97 CLASSIFIED BY 5668-SLO/Jude DECLASSIFY ON: 25X (5668 SLO/GCL 8/25/98 JFK) (JFK)

UNKNOWN SUBJECTS; SUSPECTED BOMBING OF CUBANA AIRLINES DC-8 NEAR BARBADOS, WEST INDIES, OCTOBER 6, 1976, NM - CUBA - WEST INDIES.

BY TELETYPE OCTOBER 8, 1976 LEGAT CARACAS ADVISED AS FOLLOWS.

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

~~Classified by: 5668/GCL~~ ~~Declassify on: OADR~~ ~~1/20/8~~ ~~7/14/85 SP6650/GCL #214,326~~

SECRET

2-469

PAGE TWO S E C R E T

HERNAN RICARDO LOZANO IS A NEWS PHOTOGRAPHER AND FREE-LANCE REPORTER AFFILIATED WITH THE MAGAZINE "VISION," AND HE IS ALSO EMPLOYED AS AN INDUSTRIAL INVESTIGATOR BY INVESTIGACIONES COMERCIALES E INDUSTRIALES, C.A. (ICI), AN INDUSTRIAL SECURITY FIRM OPERATED BY LUIS POSADA, FORMER HEAD OF [redacted] (S) E

1B 1C

POSADA, A CUBAN EXILE WHO IS NOW A VENEZUELAN CITIZEN, IS STRONGLY ANTI-CASTRO AND WAS SUSPECTED OF HAVING BEEN THE MAIN SUPPORTER OF ORLANDO BOSCH AVILA DURING BOSCH'S PRESENCE IN VENEZUELA PRIOR TO HIS ARREST ON NOVEMBER 19, 1975. LEGAT BECAME ACQUAINTED WITH [redacted] (S) IN A THE COURSE OF OFFICIAL BUSINESS DURING PERIOD [redacted] (S) E

1B 1C

HERNAN RICARDO LOZANO FIRST BECAME KNOWN TO LEGAT IN APPROXIMATELY JUNE, 1974, WHEN HE CONTACTED LEGAT FOR ASSISTANCE IN EXPEDITING THE PROCESSING OF A VISA TO THE U.S. THAT HAD BEEN REQUESTED FOR THE MINOR SON OF THE THEN [redacted] (S) E

1B 1C

LEGAT WAS LED TO BELIEVE RICARDO WAS AN ACTIVE MEMBER OF DISIP AND ASSISTANCE WAS PROVIDED THAT RESULTED IN THE PROMPT ISSUANCE OF A VISA TO THE [redacted] (S) CHILD. E

RICARDO RECONTACTED LEGAT A FEW WEEKS LATER TO EXPRESS HIS APPRECIATION FOR ASSISTANCE PREVIOUSLY RENDERED, AND LEGAT THEN BE-

RELEASED PER P.L-102-526(JFK ACT)
NARA MD DATE 1-19-05

2-469

PAGE THREE S E C R E T

CAME AWARE RICARDO WAS MERELY AN AUXILIARY [redacted] (S), AND THAT HE WAS ACTUALLY IN THE PERSONAL SERVICE OF LUIS POSADA. RICARDO REVEALED HE WAS ALSO A NEWSPAPER REPORTER AND PHOTOGRAPHER AFFILIATED WITH THE MAGAZINE "VISION," AND INDICATED HE DEVOTED MOST OF HIS TIME RESEARCHING NEWS ARTICLES INTENDED TO DISCREDIT THE CASTRO GOVERNMENT. HE CLAIMED PARTIAL RESPONSIBILITY FOR A NEWSPAPER ARTICLE THAT APPEARED IN A CARACAS NEWSPAPER ABOUT THAT TIME, REVEALING THE PRESENCE OF CUBAN INTELLIGENCE OFFICERS IN CUBAN EMBASSY IN CARACAS.

RICARDO CONTACTED LEGAT APPROXIMATELY FOUR TIMES AFTER THE INITIAL VISIT, AND ON TWO OCCASIONS FURNISHED PHOTOGRAPHS AND BIOGRAPHICAL DATA ON MEMBERS OF THE CUBAN EMBASSY WHICH WERE OBVIOUSLY OBTAINED FROM [redacted] (S) DURING ONE VISIT, RICARDO SUGGESTED LEGAT MIGHT WISH TO MAKE SOME SUGGESTIONS REGARDING COURSES OF ACTION THAT MIGHT BE TAKEN AGAINST THE CUBAN EMBASSY IN CARACAS BY AN ANTI-CASTRO GROUP OF WHICH HE FORMED PART. LEGAT INFORMED RICARDO SUCH WAS NOT PART OF THE FUNCTION OF THE LEGAL ATTACHE'S OFFICE, AND THAT IN ANY EVENT, LEGAT PERSONALLY ABHORRED TERRORIST ACTIVITIES REGARDLESS OF WHOM THEY MIGHT BE DIRECTED AGAINST. LEGAT POINTED OUT TO RICARDO THAT THE U.S. GOVERNMENT WAS DOING EVERYTHING IT COULD TO PREVENT DISRUP-

SECRET

RELEASED PER P.L. 102-526(JFK ACT)
NARA MDL DATE 1-18-05

2-469

PAGE FOUR S E C R E T

TIVE AND TERRORIST ACTIONS BY ANTI-CASTRO GROUPS IN THE US. RICARDO DID NOT AGAIN REPEAT THE SUGGESTION. (U)

LEGAT WAS SURPRISED BY APPEARANCE OF RICARDO AT AMERICAN EMBASSY ON SEPTEMBER 30, 1976. THE LAST CONTACT WITH RICARDO HAD BEEN EARLY IN DECEMBER, 1975, WHEN RICARDO TELEPHONED LEGAT AND INVITED HIM TO A LUNCH OF VENEZUELAN SPECIALTIES PREPARED DURING THE HOLIDAY SEASON. LEGAT DECLINED INVITATION, CITING A PREVIOUS ENGAGEMENT. (U)

ON SEPTEMBER 30, 1976, RICARDO INFORMED LEGAT HE HAD A PHOTOGRAPHIC ASSIGNMENT FOR "VISION" MAGAZINE IN JAMAICA AND WAS IN NEED OF A VISA TO THE US SINCE HE PLANNED A TWO-DAY STOPOVER IN PUERTO RICO

HE SAID HE HAD FIRST CONTACTED A TRAVEL AGENCY TO MAKE ARRANGEMENTS FOR THE VISA, BUT WAS TOLD THE PROCESS WOULD TAKE THREE DAYS, AND SINCE HE EXPECTED TO DEPART CARACAS ON OCTOBER 1, 1976, HE REQUESTED LEGAT'S ASSISTANCE IN EXPEDITING A VISA FOR HIM. AS LEGAT WAS OCCUPIED WITH OTHER MATTERS, HE ACCEPTED RICARDO'S PASSPORT AND VISA APPLICATION FORM, PROMISING TO LOOK IT OVER AND TO SUBSEQUENTLY ADVISE RICARDO OF ANY FURTHER REQUIREMENTS. IN REVIEWING THE PASSPORT AND APPLICATION FORM, LEGAT NOTED RICARDO HAD NOT PREVIOUSLY TRAVELED TO THE US. THE PASSPORT DID REFLECT HOWEVER THAT RICARDO HAD TRAVELED FROM CARACAS TO PORT-OF-SPAIN, TRINIDAD, ON AUGUST 29, (U)

SECRET

2-469

PAGE FIVE S E C R E T

1976, AND HAD RETURNED TO CARACAS ON SEPTEMBER 1, 1976. LEGAT RECALLED THAT THE BOMBING OF THE GUYANESE CONSULATE IN PORT-OF-SPAIN HAD OCCURRED AT APPROXIMATELY 10:15 AM ON SEPTEMBER 1, 1976, AND WONDERED IN VIEW OF RICARDO'S ASSOCIATION WITH LUIS POSADA, IF HIS PRESENCE THERE DURING THAT PERIOD WAS COINCIDENCE. (U)

ON THE HUNCH IT MIGHT BE OF POSSIBLE FUTURE INTEREST, LEGAT TOOK THE LIBERTY OF MAKING XEROX COPIES OF RICARDO'S PASSPORT AND VISA APPLICATION FORM. IN CONSULTING WITH CHIEF OF NONIMMIGRANT VISA SECTION, GLADYS LUJAN, LEGAT INFORMED HER HE WISHED NO SPECIAL CONSIDERATION FOR RICARDO, AND REQUESTED THE ISSUANCE OF A VISA TO HIM BE CONSIDERED ON ITS OWN MERITS. MRS. LUJAN STATED RICARDO WOULD NEED ONLY AN EMPLOYMENT LETTER INDICATING HE WAS GAINFULLY EMPLOYED IN VENEZUELA. (U)

WHEN RICARDO REAPPEARED AT EMBASSY ON AFTERNOON OF SEPTEMBER 30, 1976, HE WAS INFORMED OF REQUIREMENT OF A LETTER OF EMPLOYMENT, AND HE WAS INSTRUCTED TO GO DIRECTLY TO CONSULAR SECTION WITH HIS DOCUMENTS WHEN HE HAD THEM IN ORDER. HE INDICATED HE WOULD OBTAIN THE EMPLOYMENT LETTER AND WOULD RETURN TO THE CONSULARSECTION ON THE MORNING OF OCTOBER 1, 1976. (U)

ON THE MORNING OF OCTOBER 1, 1976, RICARDO AGAIN APPEARED AT THE

SECRET

NARA

2-469

PAGE SIX S E C R E T

RECEPTIONIST DESK IN THE LOBBY OF THE EMBASSY AND REQUESTED TO SEE LEGAT. LEGAT PROCEEDED TO LOBBY, WHERE RICARDO SAID HE HAD BEEN TOLD BY ONE OF THE VICE CONSULS HIS EMPLOYMENT LETTER WAS NOT EXPLICIT ENOUGH, AND WHEN HE INFORMED HER HE WAS ACQUAINED WITH LEGAT, THE VICE CONSUL SUGGESTED HE RECONTACT LEGAT AND ASK HIM TO SPEAK WITH HERJS RICARDO DISPLAYED A LETTER WRITTEN ON ICI LETTERHEAD STATIONERY AND SIGNED BY LUIS POSADA ATTESTING MERELY RICARDO WAS AN ICI EMPLOYEE. LEGAT THEN COMMUNICATED WITH VICE CONSUL WHO WISHED TO KNOW IF LEGAT BELIEVED RICARDO WOULD RETURN TO VENEZUELA AFTER HIS VISIT IN THE US, OR IF HE WAS LIKELY TO REMAIN THERE ILLEGALLY. LEGAT INFORMED THE VICE CONSUL HE HAD NO REASON TO BELIEVE RICARDO WOULD NOT RETURN TO CARACAS. THE VICE CONSUL INDICATED IN THAT CASE A VISA WOULD BE ISSUED TO RICARDO, AND HE WAS ASKED TO RETURN TO THE CONSULAR SECTION. UPON TAKING LEAVE OF LEGAT, RICARDO INDICATED HE MIGHT ALSO VISIT NEW YORK CITY BEFORE RETURNING TO CARACAS, AND MENTIONED IN PASSING THAT BESIDES JAMAICA, HE MIGHT ALSO BE VISITING BARBADOS IN CONNECTION WITH HIS PICTORIAL ASSIGNMENT FOR "VISION." RICARDO WAS NOT SEEN AFTER THAT. 3(4)

BT

SECRET

2-469

PAGE SEVEN S E C R E T

IN A CONVERSATION WITH AN [redacted] (S) ON OCTOBER 1, 1976, E
LEGAT BROACHED THE SUBJECT OF RICARDO AND OF THE FAINT SUSPICION THAT
1B RICARDO MAY HAVE BEEN SOMEHOW INVOLVED IN THE BOMBING OF THE GUYANESE
1C CONSULATE IN PORT-OF-SPAIN. LEGAT ADMITTED THERE WAS NO SUBSTANTIVE
EVIDENCE OF RICARDO'S IMPLICATION, BUT THAT THE COINCIDENCE OF HIS
PRESENCE THERE AT THE APPROPRIATE TIME, COUPLED WITH HIS EMPLOYMENT
RELATIONSHIP WITH LUIS POSADA, HAD GIVEN LEGAT CAUSE TO WONDER.
THE [redacted] (S) RELATED [redacted] (S) HAD NO REASON TO BELIEVE RICARDO WAS E,
THE CALIBER OF INDIVIDUAL THAT WOULD BE UTILIZED IN SUCH AN OPERATION,
AND THAT RICARDO WAS NOT KNOW TO BE INVOLVED IN SUCH ACTIVITIES, IN
SPITE OF HIS ASSOCIATION WITH POSADA. (U)

ON OCTOBER 8, 1976, A CONFIDENTIAL SOURCE ABROAD ADVISED HE
HAD DISCOVERED THAT THE INDIVIDUAL ARRESTED IN TRINIDAD, AND WHO
IS IN POSSESSION OF THE VENEZUELAN PASSPORT ISSUED TO JOSE VAZQUEZ
GARCIA, IS ACTUALLY HERNAN RICARDO LOZANO. HE SAID HE DETERMINED
THAT RICARDO AND FREDDY LUGO, THE OTHER VENEZUELAN ARRESTED IN
TRINIDAD, HAD BEEN PART OF THE SUPPORT GROUP IN THE SABOTAGE
OPERATION AGAINST THE CUBANA AIRLINER IN BARBADOS. HE SAID THE
OPERATION HAD NOT GONE AS PLANNED BECAUSE IT WAS INTENDED THAT
THE BOMB SHOULD EXPLODE BEFORE THE AIRCRAFT TOOK OFF FROM BARBADOS.
THE SOURCE STATED THAT APPARENTLY THE TIMING MECHANISM ON THE BOMB
HAD NOT BEEN PROPERLY SET. (U)

SECRET

INITIAL SA 13

RELEASED PER P.L-102-526(JFK ACT)
NARA [illegible] DATE 5/4/05

Reproduced at the National Archives

October 18, 1976

DRAFT

SECRET
SENSITIVE

MR WARREN
CIA/DDO/WH

Ray,
Please have this checked for accuracy & filling in missing parts and facts. Hoo'n deadline
Hal Saunders wants to be able to assure the Secretary that the memo has your full concurrence.
Francis

To: The Secretary

From: INR - Harold H. Saunders

Castro's Allegations

In his speech of October 15, Fidel Castro made the following allegations concerning CIA involvement in the bombing and crash of a Cubana Airlines plane on October 6 off Barbados:

--"Well-informed Venezuelan sources" had communicated to the Cubans that Hernan Ricardo Lozano (one of the men arrested in Trinidad in connection with the bombing of the plane) was a CIA agent and had handled reports from the CIA many times.

--Hernan Ricardo is an associate of Felix Martinez Suarez, who is reputed to be a CIA agent in Venezuela.

--"The recruitment of citizens and the utilization of other countries' territories to conduct such acts are methods characteristic of the CIA. At the beginning we were uncertain whether the CIA had directly organized the sabotage or had carefully prepared it through its covert organization formed

CIA HAS NO OBJECTION TO DECLASSIFICATION AND/OR RELEASE OF CIA INFORMATION IN THIS DOCUMENT AS SANITIZED JM 11997

EO INFO Classified by Same/Gen Declassify on: OADR

2-2173

RELEASED PER P.L-102-526(JFK ACT)
NARA DATE 5/4/05

Reproduced at the National Archives

by Cuban counterrevolutionaries. Now we decidedly believe the first assumption is correct. The CIA directly participated in the destruction of the Cubana aircraft in Barbados."

--The principal leaders of Cuban exile terrorist groups are closely linked through the CORU organization to CIA activities against Cuba.

In his speech, Castro did not make any specific allegations concerning a USG relationship with Orlando Bosch, or Luis Posada (two Cuban exile activists who were arrested by Venezuelan authorities in connection with the Cubana crash). However, the link with Bosch is implied since he is reported to be chief of CORU, the umbrella organization of Cuban exile terrorists.

Individuals Allegedly Involved

Hernan Ricardo Lozano

a. Involvement in the Crash: He was arrested in Trinidad on suspicion of having planted a bomb in the Cubana plane. Caracas radio announced on October 18 that he confessed to sabotaging the airliner. A [redacted] (5) source in Caracas reports that Ricardo may have been trained in the use of explosives and investigative techniques by Luis Posada. [redacted] (5)

1B per CIA

RELEASED PER P.L-102-526(JFK ACT)
NARA DATE 5/4/05
Reproduced at the National Archives

LB per CDA

[redacted]

[redacted] (S)

Ricardo, a Venezuelan citizen, is a photographer employed by Posada in his industrial security firm in Caracas. A [redacted] (S) source says that Ricardo is also a part time employee of the Venezuelan Intelligence Service (DISIP). He reportedly gathered photographic material on groups and individuals of interest to DISIP and the Venezuelan Government. He was hired by DISIP when Pasada was an official of that organization. The [redacted] (S) source says that the Venezuelan Government is concerned and would be faced with serious problems if these connections become public knowledge.

b: Relationship with US: [redacted]

[redacted] (S) The US Legal Attache in Caracas, Joseph Leo, says that he has had some dealings with Ricardo for help in expediting visa applications [redacted]

4 [redacted]

[redacted] (S) During one visit, Ricardo attempted to solicit suggestions from the Legal Attache on activities which might be directed against the Cuban Embassy by an anti-Castro group to which he belonged. Leo says he discouraged Ricardo, pointing out that the US Government was attempting to prevent disruptive and

RELEASED PER P.L.-102-526(JFK ACT)
NARA DATE 5/4/05

Reproduced at the National Archives

terrorist activities by anti-Castro groups in the US, and Ricardo never repeated the suggestion.

Freddy Lugo

a. Involvement in the crash: Lugo was arrested in Trinidad with Ricardo on suspicion of having planted the bomb aboard the Cubana plane. A [redacted] (S) source alleges that Lugo apparently was only peripherally involved in the bombing and is not considered to be one of the leading participants.

1B per CPA

Lugo, a Venezuelan citizen, is also a photographer employed by Posada's company. According to [redacted] (S) source, he also worked for DISIP under the same arrangements noted above for Ricardo.

b. Relationship with US: [redacted] (S) The name and phone number of US Legal Attache Leo were discovered in Lugo's address book when he was arrested in Trinidad. Leo says that he has had no contact with Lugo and speculates that his name and phone were furnished to Lugo by Posada.

Luis Posada Carriles

a. Involvement in Crash: Posada was arrested on October 14 in Venezuela along with Orlando Bosch and three others accused of conspiring to sabotage the plane. Posada, a Cuban exile who is now a Venezuelan citizen, is vehemently anti-Castro and is suspected of having been the main supporter of Bosch during the latter's stay in Venezuela prior to being

RELEASED PER P.L-102-526(JFK ACT)
NARA DATE 5/9/05
Reproduced at the National Archives

SENSITIVE

- 5 -

arrested in November 1974. Posada was formerly chief of the counterintelligence division of the Venezuelan intelligence service, DISIP.

b. Relationship with US. [redacted]

[redacted] When he lost his position in DISIP [redacted] says [redacted] declined to assist Posada on a visa matter. [redacted]

The US army attache has also used a Posada business partner (also a Cuban exile, whose name we do not have) as an informant (though not as an agent).

Our Legal Attache (Joseph Leo) became acquainted with Posada during the latter's employment [redacted] and after his resignation, Posada continued to contact Leo on rare occasions, usually in order to obtain personal service in regard to visa requests for relatives and business associates, the last being Ricardo on ~~October 1, 1976~~ September 30, 1976 and October 1, 1976. Leo says he has seen Posada on about three occasions since 1973, the last being in June 1976 when Posada inquired if the FBI had interest in a Venezuelan who had hired two of his "operatives" as body guards.

RELEASED PER P.L-102-526(JFK ACT)
NARA DATE 5/4/05
Reproduced at the National Archives

Orlando Bosch

a. Involvement in Crash: As noted above, Bosch was arrested in Venezuela for alleged involvement in the Cubana crash. In late June, a CIA source reported that an exile group headed by Bosch planned to bomb a Cubana flight between Panama and Havana. An FBI source has alleged that one attempt was made but the bomb did not detonate. A second try occurred in Jamaica on July 9, but the bomb exploded before the suitcase in which it was carried was put aboard the plane.

According to [redacted] Venezuelan President Carlos Andres Perez is said to be sympathetic to Bosch and has permitted him to travel freely in the country and solicit funds with the understanding that Venezuela would not be used as a base of operations or place of refuge. Bosch reportedly promised not to engage in terrorist activity while in Venezuela and received a token $500 contribution from Perez. [redacted] reported that after Bosch's arrival in Caracas in September, he stated during a fund raising dinner that "Now that our organization has come out of the Letelier job looking good, we are going to try something else." A few days later, Posada allegedly said, "We are going to hit a Cuban airliner" and "Orlando (Bosch) has the details.".

IB per CIA

b. Relationship with US. [redacted] The US is currently attempting to have Bosch deported from Venezuela

RELEASED PER P.L-102-526(JFK ACT)
NARA DATE 5/4/05
Reproduced at the National Archives

to the US, where he is subject to immediate imprisonment for parole violation.

Frank Castro

a. Involvement in Crash: Venezuelan officials reportedly believe that Castro, (head of the FLNC terrorist organization, a component group in CORU) is deeply involved in the crash, though we have no details of his supposed involvement. Frank Castro was in Venezuela in late September 1976 and in mid-October was back in Miami. Frank Castro has admitted to FBI agents that he met with Bosch in Caracas on September 26 or 27, but denies any personal knowledge of the bombing of the Cubana plane.

b. Relationship with US: [redacted] who is an American citizen with permanent residence in Santo Domingo.

Orlando Garcia and Ricardo Morales Navarrete

a. Involvement in Crash: Orlando Garcia is President Perez' security and intelligence advisor, and Morales is Garcia's deputy; both are Cuban exiles who are now Venezuelan citizens. [redacted] claims that Garcia was directed to protect and assist Bosch during his stay in Venezuela. [redacted] reported that Garcia and Posada met Bosch upon his arrival and escorted him to his hotel. Both Garcia and Morales reportedly attended the fund-raising dinner during which Bosch allegedly made the remark about the "Letelier job," and after the Cubana

RELEASED PER P.L-102-526(JFK ACT)
NARA DATE 5/4/05
Reproduced at the National Archives

crash Garcia may have made an effort to get Bosch out of Venezuela. It is possible, therefore that Garcia and/or Morales may have known in advance about the operation which led to the bombing of the plane.

b. Relationship with US:

Felix Martinez Suarez

a. Involvement in Crash: None, except by the alleged association with Ricardo, contained in Fidel Castro's charges.

b. Relationship with US: [redacted]

18 per CIA

Castro's allegation regarding CORU: With regard to Castro's charge on CIA links with CORU, an FBI report of September 17 states that "a confidential source abroad" claims to have been told by Roberto Carballo (leader of the Association of Veterans of the Bay of Pigs, AVBC, one of the component organizations of CORU) that in July of this year Carballo and three other Cuban exiles had been approached by representatives

RELEASED PER P.L. 102-526(JFK ACT)
NARA dt DATE 5/4/05
Reproduced at the National Archives

of the CIA who informed them that CIA was dissatisfied with all the acts of sabotage being carried out at random and ordered them to disassociate themselves from Bosch and CORU. The source alleged that during the week of September 12-18 Carballo and three other Cuban exiles were in Washington to confer with representatives of the CIA on plans to be carried out by the action arm of the AVBC, for which financing was to come from CIA. The FBI report concludes with a request that the CIA advise if it has "active operational interest in AVBC as described above."

CIA says that this report is false and the Agency has no active operational interest in the AVBC. According to CIA, a representative of a group of Cuban exiles did telephone into the Agency in September 1976 requesting contact for an unspecified reason, but the contact did not take place and the callers were discouraged from further attempts to telephone the Agency.

RELEASED PER P.L-102-526(JFK ACT)
NARA [illegible] DATE 5/4/05

Reproduced at the National Archives

9:30 AM Call Lynn advised OK with chg 10-20-76 [illegible]

SECRET/SENSITIVE

October 19, 1976

Additional Questions (answers and comments needed by late morning, October 20)

Cuban aircraft

1. Has CIA had any relationship with Posada's investigative agency or any other business he may have had?

1B per CIA

2. [redacted] (S) 28,4 24 10

3. [redacted] (S) 24,4,2 8

4. Does the CIA believe that the source of TDFIR DB-315/10256 deliberately, delayed passing on Bosch's and Posada's remarks about hitting a Cuban plane until after the incidents?

5. Does the CIA have any additional relevant information on any of the people named in the draft memorandum, or any other information relating to the sabotage of the plane, which it has not yet disseminated in TDFIR form?

6. Would CIA please provide whatever information it has concerning Orlando Garcia and Ricardo Morales so that para b on page 8 of the draft memorandum can be completed?

CIA HAS NO OBJECTION TO DECLASSIFICATION AND/OR RELEASE OF THIS DOCUMENT AS SANITIZED. 3/13/98
2-2173
NOT RECORDED
MAY 17 1977
2-2173
CIA HAS NO OBJECTION TO DECLASSIFICATION AND/OR RELEASE OF CIA INFORMATION IN THIS DOCUMENT. AS SANITIZED JM 4/14/97
FBI INFORMATION CONTAINED HEREIN IS UNCLASSIFIED DATE [illegible] BY [illegible]

File [illegible] 6-88

SECRET/SENSITIVE

70 MAY 19 1977

RELEASED PER P.L-102-526(JFK ACT)
NARA ___ DATE 5/4/05

Reproduced at the National Archive

MM093S 3080105
PP HI WF
DE MM
P 020105Z NOV 76FM MIAMI (2-469) (P)
TO DIRECTOR PRIORITY
WASHINGTON FIELD PRIORITY
BT
S E C R E T
~~SECTION 1 OF 2~~
NO FOREIGN DISSEMINATION
UNSUBS; BOMBING OF CUBANA AIRLINES DC-8 NEAR BARBADOS, WEST INDIES, OCTOBER 6, 1976. NEUTRALITY MATTERS- CUBA - WEST INDIES. ~~(MIAMI FILE 2-469)~~
~~CHILBOM, PEO- MURDER; ZIB. UOJ. (MIAMI FILE 185-76).~~

ON NOVEMBER 1, 1976, A CONFIDENTIAL SOURCE WHO HAS FURNISHED RELIABLE INFORMATION IN THE PAST ADVISED THAT ON OCTOBER 23-24, 1976, RICARDO MORALES NAVARRETE, COMISARIO IN CHARGE OF SECTION D54, A COUNTERINTELLIGENCE SECTION OF DISIP (VENEZUELAN INTELLIGENCE SERVICE), FURNISHED THE FOLLOWING INFORMATION TO SOURCE:

SOME PLANS REGARDING THE BOMBING OF A CUBANA AIRLINES AIRPLANE WERE DISCUSSED AT THE BAR IN THE ANAUCO HILTON HOTEL IN CARACAS, VENEZUELA, AT WHICH MEETING FRANK CASTRO,

RELEASED PER P.L-102-526(JFK ACT)
NARA DATE 5/4/05
Reproduced at the National Archives

GUSTAVO CASTILLO, LUIS POSADA CARRILES AND MORALES NAVARRETE WERE PRESENT. THIS MEETING TOOK PLACE SOMETIME BEFORE THE BOMBING OF THE CUBANA AIRLINES DC-8 NEAR BARBADOS ON OCTOBER 6, 1976.

FRANK CASTRO IS A LEADER OF CORU, THE ANTI-CASTRO TERRORIST ORGANIZATION WHICH HAS TAKEN CREDIT FOR SEVERAL BOMBINGS. GUSTAVO CASTILLO IS ONE OF THREE PERSONS INVOLVED IN THE ATTEMPTED KIDNAPING OF THE CUBAN CONSUL IN MERIDA YUCATAN ON JULY 23, 1976, AT WHICH TIME THE CONSUL'S BODYGUARD WAS SLAIN. ORESTES RUIZ HERNANDEZ AND GASPAR JIMENEZ WERE APPREHENDED BY MEXICAN AUTHORITIES BUT CASTILLO EVADED CAPTURE. LUIS POSADA CARRILES HAS BEEN ARRESTED BY VENEZUELAN AUTHORITIES IN CONNECTION WITH THE CUBANA AIRLINES DC-8 BOMBING.

MORALES NAVARRETE TOLD THE SOURCE THAT ANOTHER MEETING TO PLAN THE BOMBING OF A CUBANA AIRLINER TOOK PLACE IN THE APARTMENT OF MORALES NAVARRETE IN THE ANUCO HILTON. THIS MEETING WAS ALSO PRIOR TO THE BOMBING OF THE CUBANA AIRLINER ON OCTOBER 6, 1976. PRESENT AT THIS MEETING WERE MORALES NAVARRETE,

RELEASED PER P.L-102-526(JFK ACT)
NARA DATE 5/4/05
Reproduced at the National Archives

POSADA CARRILES AND FRANK CASTRO. ACCORDING TO MORALES NAVARRETE, AT THIS MEETING THERE WAS SOME DISAGREEMENT AS TO WHO WOULD TAKE PART IN THE VARIOUS PHASES OF THE OPERATION, AND WHO WOULD CLAIM CREDIT FOR THE BOMBING. FRANK CASTRO SAID THE FLNC (NATIONAL LIBERATION FRONT OF CUBA) WOULD TAKE CREDIT.

THE FLNC IS AN ANTI-CASTRO TERRORIST ORGANIZATION WHICH HAS TAKEN CREDIT FOR SEVERAL BOMBINGS.

MORALES NAVARRETE SAID THAT AFTER THIS MEETING HE HAD NOTHING MORE TO DO WITH THIS MATTER. HE ADDED THAT AFTER THE CABANA AIRLINER BOMBING ON OCTOBER 6, 1976, FRANK CASTRO DID NOT WANT THE FLNC TO CLAIM CREDIT AS HE WAS AFRAID OF REPRISALS BY THE CUBAN GOVERMNENT.

MORALES NAVARRETE SAID THAT THE GROUP INVOLVED HAD PREVIOUSLY ATTMEPTED TO BOMB A CUBANA AIRLINER IN PANAMA AND IN JAMAICA.

MORALES NAVARRETE SAID THAT SOME PEOPLE IN THE VENEZUELAN GOVERNMENT ARE INVOLVED IN THIS AIRPLANE BOMBING, AND THAT IF POSADA CARRILES TALKS, THEN MORALES NAVARRETE AND OTHERS IN

RELEASED PER P.L-102-526(JFK ACT)
NARA DATE 5/4/05
Reproduced at the National Archives

THE VENEZUELAN GOVERNMENT WILL "GO DOWN THE TUBE". HE SAID THAT IF PEOPLE START TALKING "WE'LL HAVE OUR OWN WATERGATE".

MORALES NAVARRETE SAID THAT AFTER THE CUBANA AIRLINER CRASH, HERNAN RICARDO LOZANO TELEPHONED ORLANDO BOSCH FROM TRINIDAD STATING " A BUS WITH 73 DOGS WENT OFF A CLIFF AND ALL GOT KILLED". BOSCH, KNOWING THAT MANY PHONE CALLS ARE TAPPED BY THE VENEZUELAN GOVERNMENT, PRETENDED HE DID NOT KNOW WHAT HERNAN RICARDO LOZANO WAS TALKING ABOUT.

SOURCE SAID THAT IN A CONVERSATION WITH ORLANDO GARCIA VASQUEZ, MINISTER COUNSELLOR ON SECURITY MATTERS TO VENEZUELAN PRESIDENT CARLOS ANDRES PEREZ, GARCIA VASQUEZ TOLD SOURCE THAT SHORTLY AFTER THE CUBANA CRASH, GRACIA VASQUEZ TALKED TO CARLOS FABRI, THE BOMB EXPERT FOR DISIP. GARCIA VASQUEZ TOLD FABRI THAT HE WOULD HAVE TO TESTIFY AT ANY TRIAL IN THIS MATTER REGARDING BOMBS AND THEIR COMPONENTS. ACCORDING TO GARCIA VASQUEZ, FABRI BECAME VERY NERVOUS AND GARCIA VASQUEZ TOLD SOURCE HE BELIEVES THAT FABRI EITHER MADE THE BOMB FOR THIS CUBANA BOMBING, INSTRUCTED PERSONS ON HOW TO MAKE IT , OR AT LEAST HAD PRIOR KNOWLEDGE OF THE BOMBING.

NARA Jt DATE 5/4/05

GARCIA VASQUEZ MENTIONED THAT THE BOMB ON THE CUBANA AIRLINER WAS ACTIVATED BY A "LAPICERO" (TIME PENCIL).

SOURCE SAID THAT HE ALSO CONVERSED WITH A MEMBER OF THE VENEZUELAN POLICIA TECNICA JUDICIAL (JUDICIAL TECHNICAL POLICE) (PTJ) IN CARACAS. THIS MEMBER, WHOSE NAME SOURCE DOES NOT RECALL, BUT WHO HAS A POLISH NAME, SAID THAT AFTER THE CUBANA AIRLINER CRASHED, THE PTJ KNEW WHO WAS INVOLVED AND THEREFORE WANTED TO HANDLE THE INVESTIGATION. HOWEVER, THE PTJ WAS DENIED THE INVESTIGATION AND DISIP TOOK OVER THE MATTER "TO COVER IT UP". THIS PTJ MEMBER ALSO TOLD SOURCE THAT IF CARLOS FABRI DID NOT MAKE THE BOMB, THEN HE AT LEAST HAD PRIOR KNOWLEDGE OF THE MATTER.

SOURCE SAID THAT FABRI AND POSADA CARILLES ARE GOOD FRIENDS AND THAT FABRI AND POSADA HAD ACTUALLY BEEN ARRESTED A COUPLE OF YEARS AGO BY VENEZUELAN AUTHORITIES AFTER IT WAS LEARNED THEY PORVIDED FALSE DOCUMENTATION AND EXPLOSIVES TO DR. ORLANDO BOSCH AVILA IN VENEZUELA AT THAT TIME.

NARA [illegible] DATE 5/4/05

DR. ORLANDO BOSCH AVILA IS A FUGIVE FROM THE U.S., LEADER OF CORU, AND IS IN CUSTODY IN VENEZUELA IN CONNECTION WITH THIS CUBANA AIRLINES BOMBING.

MORALES NAVARRETE TOLD SOURCE THAT ORLANDO BOSCH SAID THAT GUILLERMO NOVO VISITED CHILE IN EARLY 1975 AT WHICH TIME HE VISITED BOSCH. DURING THIS PERIOD, GUILLERMO NOVO MAKE CONTACT WITH AN ULTRA-RIGHTWING ORGANIZATION KNOWN AS "PATRIA Y LIBERTAD" (FATHERLAND AND LIBERTY). BOSCH SAID THAT ORLANDO LETELIER'S DEATH WAS THE RESULT OF AN AGREEMENT BETWEEN GILLERMO NOVO AND THE "PATRIA Y LIBERTAD" ORGANIZATION. MORALES NAVARRETE SAID THAT SOME MEMBERS OF "PATRIA Y LIBERTAD" ARE ALSO MEMBERS OF "DINA", A CHILEAN INTELLIGENCE SERVICE. SOURCE WAS UNABLE TO LEARN FURTHER INFORMATION REGARDING THIS MATTER.

MORALES NAVARRETE ALSO TOLD SOURCE THAT GUSTAVO CASTILLO AND MEMBERS OF HIS GROUP ARE RESPONSIBLE FOR THE FOLLOWING BOMBINGS IN THE MIAMI, FLORIDA AREA: BOMBING OF THE DOMINICAN CONSULATE ON OCTOBER 6, 1975, BOMBING OF THE DOMINICAN AIRLINES TICKET OFFICE ON OCTOBER 20, 1975; BOMBINGS AT THE BROWARD COUNTY COURT HOUSE ON OCTOBER 10, 1975; AND ATTEMPTED BOMBING OF A

RELEASED PER E.O. 12958 (NARA)
NARA [illegible] DATE 5/4/05

BAHAMASAIR AIRLINER AT MIAMI INTERNATIONAL AIRPORT ON NOVEMBER 27, 1975. ACCORDING TO MORALES NAVARRETE, THE ORGANIZATION "YOUTH OF THE STAR", WHICH CLAIMED CREDIT FOR THESE BOMBINGS, IS COMPOSED OF GUSTAVO CASTILLO, GASPAR JIMENEZ, ORESTES RUIZ HERNANDEZ, DUNEY PEREZ ALAMO AND RACIEL RODRIGUEZ GONZALEZ WHO IS THE YOUNGER BROTHER OF REINOL RODRIGUEZ, FLNC MEMBER WHO RESIDES IN SAN JUAN, PUERTO RICO. THIS GROUP IS GENERALLY INDEPENDENT EVEN THOUGH MEMBERS WILL ACCOMPLISH TERRORIST ACTS FOR THE FLNC OR OTHER CUBAN TERRORIST GROUPS.

SOURCE ADVISED THAT ON OCTOBER 27, 1976, THE VENEZUELAN GOVERNMENT ISSUED SOME TYPE OF NEWS RELEASE STATING THAT THERE IS NO RICARDO MORALES NAVARRETE IN DISP. SINCE THAT TIME, SOURCE HAS TELEPHONED NAVARRETE TO HIS OFFICE AND TO HIS APARTMENT AT THE ANAUCO HILTON IN CARACAS. PERSONS ANSWERING THE PHONE STATE THAT THEY KNOW OF NO RICARDO MORALES NAVARRETE NOR DO THEY KNOW OF COMISARIO MOISES (A CODE NAME FOR MORALES NAVARRETE). SOURCE SAID THAT MORALES NAVARRETE TELEPHONED HIS GIRL FRIEND IN MIAMI, FLORIDA, TELLING HER NOT TO PHONE HIM AS "HE DOES NOT

NARA Art DATE 5/4/05

PAGE EIGHT ~~MM 2 469 S E C R E T~~

"EXIST". MORALES NAVARRETE SAID HE WOULD TELEPHONE HER INSTEAD. MOST OF THE ABOVE INFORMATION WAS TOLD IN STRICT CONFIDENCE TO SOURCE AND DIVULGENCE OF THIS INFORMATION WOULD IMMEDIATELY PINPOINT THE SOURCE WHO REQUESTED THAT THIS INFORMATION NOT BE DIVULGED OUTSIDE THE U. S. GOVERNMENT. THEREFORE, NO ACTION SHOULD BE TAKEN ON THE ABOVE INFORMATION WHICH COULD COMPROMISE THE SOURCE.

~~CLASSIFIED BY 6080 CHAN REASON: FCIM II 1-2 4 5 DECLASSIFY ON: INDEFINITE~~
Administrative Data to Legals Only
ADMINISTRATIVE.

SOURCE IS RAUL DIAZ, ORGANIZED CRIME BUREAU, DADE COUNTY PUBLIC SAFETY DEPARTMENT, WHO TRAVELED TO VENEZUELA ON OCTOBER 22, 1976, IN AN ATTEMPT TO CONVINCE MORALES NAVARRETE TO TESTIFY IN THE NOVEMBER 15, 1976 STATE TRIAL OF ROLANDO OTERO FOR NINE BOMBINGS IN MIAMI, INCLUDING THAT OF THE MIAMI FBI OFFICE.

NARA [illegible] DATE 5/4/05

DIAZ SAID THAT MORALES NAVARRETE SAID THAT THE FLORIDA STATE ATTORNEY'S OFFICE SHOULD REQUEST THE VENEZUELAN GOVERNMENT, THROUGH THE U.S. DEPARTMENT OF STATE, TO HAVE MORALES SO TESTIFY.

RAUL DIAZ REQUESTED THAT HE NOT BE REVEALED AS THE SOURCE OF THIS INFORMATION, AND AS SET OUT IN THE DETAILS, THIS INFORMATION SHOULD NOT BE REVEALED OUTSIDE THE U.S. GOVERNMENT. IT IS NOTED THAT RAUL DIAZ IS A FRIEND OF MORALES NAVARRETE.

REGARDING PATRIA Y LIBERTAD, THE MIAMI OFFICE OPENDED A CASE ON OCTOBER 3, 1973, ENTITLED "PATRIA Y LIBERTAD, IS-CUBA (MIAMI FILE 105-21705)(BUFILE 105-258678)". THIS CASE WAS OPENED WHEN AN INFORMANT OF THE MIAMI OFFICE ADVISED THAT WHEN AN ANTI-CASTRO ORGANIZATION NAMED DIRECTORIO REVOLUCIONARIO WAS DISSOLVED IN MIAMI, SOME OF ITS MEMBERS ATTEMPTED TO ORGANIZE A NEW GOUP, PATRIA Y LIBERTAD, WHICH WAS TO BE HEADED BY ALDO VERA SERAFIN. (IT IS NOTED THAT VERA SERAFIN WAS ASSASSINATED IN SAN JUAN, PUERTO RICO ON OCTOBER 25, 1976). THIS CASE WAS CLOSED IN MARCH, 1975, AS INVESTIGATION REVEALED THAT THIS OPGANIZATION WAS NEVER FORMED. REGARDING BOMBINGS

RELEASED
NARA Art DATE 5/4/05

PAGE TEN ~~MM 2 ACG S E C R E T~~

COMMITTED BY GUSTAVO CASTILLO AND OTHERS IN THE MIAMI AREA, AS MENTIONED BY MORALES NAVARRETE, THE MIAMI OFFICE IS CONDUCTING INVESTIGATION REGARDING THIS AND THE BUREAU WILL BE ADVISED UNDER APPROPRIATE CASE CAPTIONS.

BUREAU IS REQUESTED TO FURNISH ABOVE INFORMATION TO LEGAT, CARACAS.

~~BT~~

~~WRS HOLD~~

Administrative Data to Legat only.

EFA145VV

CO RUFBI

DE RUEAIIA #4262 2871804

ZNY SSSSS

O 131649Z OCT 76

FM CIA

TO FEDERAL BUREAU OF IN//INTELLIGENCE DIVISION

BT

S E C R E T. CITE CIA 926816.

S E C R E T--WARNING NOTICE-SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED--NOT RELEASABLE TO FOREIGN NATIONALS--NOT RELEASABLE TO CONTRACTORS OR CONTRACTOR/CONSULTANTS

OCT 13 1976

TELETYPE

Asst. Dir.:
Adm. Serv.
Ext. Affairs
Fin. & Pers.
Gen. Inv.
Ident.
Intell.
Laboratory
Legal Coun.
Plan & Insp.
Rec. Mgmt.
Spec. Inv.
Training
Telephone Rm.
Director Sec'y

SUBJECT: TRACES ON PERSONS INVOLVED IN 6 OCT 1976 CUBANA CRASH

CIRA-295-76

CIRA-294-76 REFERENCE

FBI INFORMATION CONTAINED HEREIN IS UNCLASSIFIED DATE 4/8/94 BY SPE MAC/GCL (JFK)

FOLLOWING IS CORRECTED VERSION OF CIA 926531:

[By Teletype 10/13/76 NS CIA Advised That]

6 OCT 19 1976

1. THIS AGENCY HAS CONDUCTED AN INVESTIGATION OF THE NAMES OF PERSONS SUSPECTED OF INVOLVEMENT IN THE 6 OCTOBER 1976 CRASH OF THE CUBANA AIRLINES FLIGHT OFF THE COAST OF BARBADOS. -WE HAVE NO CIA TRACES ON HERNAN RICARDO L O Z A N O, AKA HERNAN R I C A R D O

[By D-73 to MIA, SJ; Legal Attaché Caracas, Venezuela MAC-7565 GCS; DAL-NE 10/15/76]

[By Teletype 10/13/76 CIA Advised NS FOLLOWS:]

1. THIS AGENCY HAS CONDUCTED AN INVESTIGATION OF THE NAMES OF PERSONS SUSPECTED OF INVOLVEMENT IN THE 6 OCTOBER 1976 CRASH OF THE CUBANA AIRLINES FLIGHT OFF THE COAST OF BARBADOS. -WE HAVE NO CIA TRACES ON HERNAN RICARDO L O Z A N O, AKA HERNAN R I C A R D O

PAGE 2 ~~RUFAIIA 4262 S E C R E T~~

LOZANO, ALIAS JOSE V A Z Q U E Z GARCIA; FREDDY L U G O;
OR E. S E A L Y.

2 WE HAVE DETERMINED THAT [redacted] HAS BEEN MENTIONED [redacted] (S)
[redacted] (S)(U)

K 3/20/98

BOTH LUGO'S AND LOZANO'S EMPLOYER IN CARACAS IS LUIS P O S A D A CARRILES, FORMER HEAD OF THE COUNTERINTELLIGENCE DIVISION OF THE DIRECTORATE FOR THE SERVICES OF INTELLIGENCE AND PREVENTION (DISIP), THE VENEZUELAN CIVILIAN SECURITY SERVICE. [redacted] IS A [redacted]. HE LOST HIS POSITION [redacted] AS A RESULT OF A CHANGE IN [redacted] HE UNSUCCESSFULLY [redacted] REGARDING A VISA PROBLEM. (S)

3. CLASSIFIED BY RECORDED REPORTING OFFICER. EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF E.O. 11652 EXEMPTION CATEGORY

PAGE 3 ~~RUFAIIA 4262 S E C R E T~~

~~5(B).~~ IMPOSSIBLE TO DETERMINE DATE OF AUTOMATIC DECLASSIFICATION.

SECRET

CIA HAS NO OBJECTION TO
DECLASSIFICATION AND/OR
RELEASE OF CIA INFORMATION
IN THIS DOCUMENT. JM 10-6-97

2-469-27

HQ002876 2901795
RR MM SJ
DE HQ
R 151342Z OCT 76
FM DIRECTOR
TO MIAMI ROUTINE
SAN JUAN ROUTINE
TO RUEBNJA/DEPUTY ATTORNEY GENERAL
ATTN: ANALYSIS AND EVALUATION UNIT
RUEBNJA/ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION
ATTN: INTERNAL SECURITY SECTION
ATTN: GENERAL CRIMES SECTION
BT
S E C R E T/C O R R E C T E D COPY
UNKNOWN SUBJECTS; SUSPECTED BOMBING OF CUBANA AIRLINES DC-8 NEAR BARBADOS, WEST INDIES, OCTOBER 6, 1976; NEUTRALITY MATTERS - CUBA - WEST INDIES.

DECLASSIFIED BY 5668 SUD/MSB
ON 4-15-98 (JFK)

9/8/97
CLASSIFIED BY 5668-SUD/MCK
DECLASSIFY ON: 25X (1) (JFK)

BY TELETYPE OCTOBER 13, 1976 CIA ADVISED AS FOLLOWS:

1. THIS AGENCY HAS CONDUCTED AN INVESTIGATION OF THE NAMES OF PERSONS SUSPECTED OF INVOLVEMENT IN THE 6 OCTOBER 1976 CRASH OF THE CUBANA AIRLINES FLIGHT OFF THE COAST OF BARBADOS. WE HAVE NO CIA TRACES ON VERNON RICARDO L[illegible], [illegible] HERNAN R[illegible] A R D O LOZANO, [illegible] OR L. [illegible] A L Y. (U)

1:35 PM 10-16-76

Classified by Secretone
Declassify on: OADR 6/30/85
1/14/85

THE INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

SECRET

REPRODUCED AT THE NATIONAL ARCHIVES

RELEASED PER P.L. 102-526(JFK ACT)
NARA MM DATE 1-19-05

2-469

PAGE TWO DE RUEHFB 4395 S E C R E T SECRET

2. WE HAVE DETERMINED THAT THIS AGENCY HAD A RELATIONSHIP WITH ONE PERSON WHOSE NAME HAS BEEN MENTIONED IN CONNECTION WITH THE REPORTED BOMBING (U)

BOTH LUGO'S AND LOZANO'S EMPLOYER IN CARACAS IS LUIS P O S A D A CARILES, FORMER HEAD OF THE COUNTERINTELLIGENCE DIVISION OF THE DIRECTORATE FOR THE SERVICES OF INTELLIGENCE AND PREVENTION (DISIP), THE VENEZUELAN CIVILIAN SECURITY SERVICE. POSADA IS A FORMER AGENT OF CIA. HE WAS AMICABLY TERMINATED IN JULY 1967 BUT CONTACT WAS RE-ESTABLISHED IN OCTOBER 1967. HE LOST HIS POSITION WITH DISIP IN MARCH 1974 AS A RESULT OF A CHANGE IN THE VENEZUELAN GOVERNMENT AND WAS AMICABLY TERMINATED. WE CONTINUED OCCASIONAL CONTACT WITH HIM. HIS LAST REPORTED CONTACT WITH US WAS IN JUNE 1975 WHEN HE UNSUCCESSFULLY SOUGHT ASSISTANCE REGARDING A VISA PROBLEM. (U)

3. CLASSIFIED BY RECORDED REPORTING OFFICER. EXCEPT FROM GENERAL DECLASSIFICATION SCHEDULE OF E.O. 11652 EXEMPTION CATEGORY IMPOSSIBLE TO DETERMINE DATE OF AUTOMATIC DECLASSIFICATION.

LEGATS MEXICO CITY, CARACAS AND BUENOS AIRES ADVISED SEPARATELY.

BT

2901711 MM 1

Reproduced at the National Archive

2-469

CIA HAS NO OBJECTION TO
DECLASSIFICATION AND/OR
RELEASE OF CIA INFORMATION
IN THIS DOCUMENT. JM 10-6-97

105-6335-320 CIA, Wash., D. C. Letter to Dir. 6-7-66. Re: Raul Federicao ANDRE Llano. The files of this Agency were searched with respect to the names contained in ANDRE's letter of 10 January 1965.

b. LUIS POZADA. Probably identifiable with Luis Clemente Faustino POSADA Carriles who has been of operational interest to this Agency since April 1965. According to information dated 13 January 1965 from a young Cuban emigre with good access to Cuban activist groups and whose reporting has been generally reliable in the past, Luis Clemente POSADA Carriles was a member of the crew of a motor launch which was to be used January 1965 by the Junta Revolucionaria Cubana (JURE, Cuban Revolutionary Junta--an anti-Castro group) to infiltrate JURE leader Manuel RAY Rivero into Cuba. At the time of the report, the crew was in the Dominican Republic. The attempt to infiltrate RAY into Cuba was postponed due to mechanical difficulties with the launch; the crew was given leave to go to Miami. According to information dated September 1964, Subject was granted visa to the Dominican Republic. This office has no information to indicate that Subject travels to Santo Domingo and/or has been infiltrated into Cuba.

per CIA
DECLASSIFIED BY 5668 SUD/HSR
ON 4-15-98 (JFK)

SECRET

(10)

2-469

105-10983-36

OPTIONAL FORM NO. 10
MAY 1962 EDITION
GSA GEN. REG. NO. 27
5010-107-02

UNITED STATES GOVERNMENT

Memorandum

JM 10-6-97
SLD/KSE
4-15-98
(JFK)

TO : SAC, MIAMI

DATE: 7/18/66

FROM : SA JOHN E. MCHUGH

9/8/97
CLASSIFIED BY 56168-SLD/mk
DECLASSIFY ON: 25X
(SLD 5/0/GCL 8/25/98 -JFK)
(JFK)

SUBJECT: [redacted] (S) - CUBA (S)

1B
1C

On 7/14/66, [redacted] advised that he was personally acquainted with MITCHELL WER BEL and had spent considerable time with WER BEL in [redacted] He stated that he has heard WER BEL on occasions introduce himself as ALEX WILSON.

[redacted] advised that he was personally acquainted with LUIS POSADA, in whom CIA has an operational interest. He advised that POSADA is receiving approximately $300 per month from CIA.

He further indicated that three anti-CASTRO organizations, namely the 30th of November, RECE and Comandos-L, were attempting to establish a base in the Dominican Republic and form a military alliance there of the three organizations for action against FIDEL CASTRO. LUIS POSADA has been approached to accept the position as military head of this alliance. POSADA formerly held a commission in the U. S. Army and allegedly was in a ranger battalion. According to [redacted] because of this, POSADA was selected to head the group. POSADA was interested in having [redacted] assist him in the Dominican Republic inasmuch as [redacted] had spent considerable time aboard the [redacted] a boat that was operated by another anti-CASTRO group [redacted]URE.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
EXCEPT WHERE SHOWN
OTHERWISE

Classified by [illegible]
Declassify on: OADR 6/21/83
1/14/85 SPA/BJA/GCL #211,326

SECRET

INITIALS
SA 19

MEMORANDUM FOR: Deputy Director of Security
(Investigations and Support)

DATE: 17 April 1972 amc

SUBJECT : C#
SO# 319235
201# 300985

ATTACHMENTS (IF ANY): One copy of the PRQ Part I.

CHIEF, CI/OA

CIA HISTORICAL REVIEW PROGRAM
RELEASE AS SANITIZED
1998

COPY 2413

SECRET

GROUP 1
Excluded from automatic downgrading and declassification

(40)

Part I of III

RELEASED PER P.L-102-526(JFK ACT)
NARA MN DATE 9/29/05

Reproduced at the National Archives

319 235
1-G
21 Jan 1972 tsm

BIOGRAPHICAL DATA

NAME:	POSADA Carriles, Luis Clemente
AKAS:	CARRILES, Luis Clemente POSADA Carriles, Bambi CARRILES, Bambi POSADA Carriles, Julian CARRILES, Julian
BIRTH:	15 Feb 1928, Cienfuegos, Cuba
CITIZENSHIP:	Cuban - Alien Reg. #12 419 708
ADDRESS:	Edf. Mayflower, Apt. 24, Ave., San Juan Bosco, Caracas, Venezuela - Present Permanent: Miami, Fla.
MARITAL STATUS:	POSADA, Nieves Elina nee GONZALEZ Leyva; b. 13 Dec 1935, Cienfuegos, Cuba; Add. Same as subject; Married on 13 Aug 1963, Columbus, Ga.; Alien Reg. #12 443 942 EX-SPOUSE: POSADA, Maria Concepcion; nee CASTANEDA Napoles; b. 13 Jul 1932, Cardenas, Cuba; Add. 6540 Seville St., Apt. C, Huntington Beach, Calif.; Married on 03 Nov 1955, Cardenas, Cuba; Divorced on 23 Jun 1963 in Chicago, Ill.
CHILDREN:	POSADA, Jorge Luis; b. 1966, Miami, Fla.
PARENTS:	POSADA Gonzales, Luis; b. 1903, Cienfuegos, Cuba; Add. #4110 Ave. 56, Cienfuegos, Cuba POSADA, Dolores nee CARRILES Vega; b. 1908, Cienfuegos, Cuba; Add. Same as above
BROTHERS & SISTER:	POSADA Carriles, Roberto; b. 1931, Cienfuegos, Cuba; Add. Havana, Cuba POSADA Carriles, Raul; b. 1934, Cienfuegos, Cuba; Add. Havana, Cuba POSADA Carriles, Maria Conchita; b. 1939, Cienfuegos, Cuba; Add. Cuba
MILITARY:	Feb 1963-Mar 1964: U.S.Army, #C-2312445
EMPLOYMENT:	Present: Min. of Internal Relations, Caracas, Venezuela

RELEASED PER P.L-102-526(JFK ACT)
NARA MN DATE 4/29/05
Reproduced at the National Archives

ATTACHMENT PRQ PART I HVCA-18757

DATE	PLACE	PURPOSE
1956	Miami, Florida	Tourist
1961	Mexico	Political exile
Feb 1961	Miami, Florida	Political exile
April 1961	Guatemala	Invasion (Cuba)
May 1961	Miami, Florida	Invasion (Cuba)
1964	Dominican Republic	Cuban Affairs
1964	Puerto Rico	Cuban Affairs
1964	Dominican Republic	Cuban Affairs
1964	Miami, Florida	
Oct 1967	Venezuela	Work
Oct 1967	Miami, Florida	
Oct 1967	Venezuela	Work
1968	Miami, Florida	Tourist
1969	Miami, Florida	Tourist
Mar 1970	Miami, Florida	Reentry Permit
1970	Trinidad, Tobago	Revolution--business
Jun 1970	Bogota	Business
1970	Bogota	Business
May 1971	Aruba	Business
April 1971	Lima, Peru	Business
April 1971	Argentina	Business
April 1971	Brazil	Business
Oct 1971	Portugal	Business
Oct 1971	Rome	Business
Nov 1971	Vienna	Business
Nov 1971	Rome	Business
Dec 1971	Miami, Florida	Business
Dec 1971	Puerto Rico	Tourist

RELEASED PER P.L.-102-526(JFK ACT)
NARA DATE 4/28/05

Reproduced at the National Archives

DECODED COPY SECRET

AIRGRAM CABLEGRAM RADIO TELETYPE

DECLASSIFICATION AND/OR RELEASE OF CIA INFORMATION IN THIS DOCUMENT

SECRET

URGENT

TO DIRECTOR

FROM LEGAT MEXICO CITY

LUIS POSADA CARRILES, AS-CUBA

DIAZ, MEXICO, ADVISED BY SECRET MEMORANDUM DATED JUL DAST, NOT TO BE FURTHER DISSEMINATED WITHOUT PRIOR APPROVAL OF ISSUING OFFICE, ENTITLED INTENTION OF CUBAN REPRESENTATIVE IN EXILE (RECE) TO BLOW UP A CUBAN OR SOVIET VESSEL IN VERACRUZ, MEXICO. (X)(X)(U)

A CUBAN REFUGEE WHO IS ASSOCIATED WITH CUBAN ACTIVISTS IN THE MIAMI AREA AND WHO HAS FURNISHED RELIABLE INFORMATION IN THE PAST ADVISED THAT LUIS POSADA CARRILES STATED ON JUNE 25 LAST THAT JORGE MASFERRER OF THE RECE HAD PAID HIM $5,000 TO COVER THE EXPENSES OF A DEMOLITION OPERATION IN MEXICO. POSADA SAID HE WAS PLANNING TO PLACE LIMPET MINES ON EITHER A CUBAN OR SOVIET VESSEL IN THE HARBOR OF VERACRUZ, MEXICO AND HAD 100 POUNDS OF C-4 EXPLOSIVES AND DETONATORS. POSADA SAID HE WAS PREPARING CERTAIN PAPERS TO SHOW HE IS PUERTO RICAN TO ENABLE HIM TO OBTAIN VISA FOR ENTRY INTO MEXICO. (X)(X)(U)

FOR INFORMATION OF BUREAU AND MIAMI. REC

HENRY J. JOHNSON

RECEIVED: 11:27 AM

TRD GC: MR. BRENNAN

JUL 15 1965

SECRET

If the intelligence contained in the above message is to be disseminated outside the Bureau, it is suggested it be paraphrased in order to protect the Bureau's cryptographic systems.

RELEASED PER P.L.-102-526(JFK ACT)
NARA [illegible] DATE 4/28/05

Reproduced at the National Archives

UNITED STATES DEPARTMENT OF JUSTICE

FEDERAL BUREAU OF INVESTIGATION

In Reply, Please Refer to
File No.

~~SECRET~~

Miami, Florida
July 13, 1965

105-8280

CIA HAS NO OBJECTION TO
DECLASSIFICATION AND/OR,
RELEASE OF CIA INFORMATION
IN THIS DOCUMENT, KP 2-9-98

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
EXCEPT WHERE SHOWN
OTHERWISE

~~S E C R E T~~

8/8/94
#21,326 SOB MACIGAT (JFK)
Classified by MULTIPLE SOURCES
Declassify on: OADR
4/2/85

RE: CUBAN REPRESENTATION IN EXILE (RECE);
INTERNAL SECURITY - CUBA;
NEUTRALITY MATTERS.

DECLASSIFIED BY 5668 SLD/LSB
ON 4-16-98 (JFK)

MM T-1, another Government agency which conducts intelligence investigations, on June 17, 1965, advised information had been received from a Cuban refugee with contacts among Cuban exile activists, and this refugee's previous reporting has proved to be fairly reliable. The information from this source is as follows: (~~S~~)(X)(U)

On June 11, 1965, a Cuban exile, proficient in demolition and the use of explosives, gave instructions in these subjects to three Cubans about to be infiltrated into Havana, Cuba, under the auspices of the Cuban Representation in Exile (RECE) (~~S~~)(X)(U)

In connection with this instruction, Jorge Mas Canosa, an official of RECE, residing in Miami, proposed to the demolition expert that he travel to Spain, Mexico, and other Latin American countries at RECE's expense and place bombs in Communist installations such as embassies and information service libraries. Mas said that in May, 1965, one of RECE's agents had placed a bomb in the Soviet Library in Mexico City, which bomb exploded and caused a furor. On this agent's return to Miami, he was not bothered by U. S. authorities, although his activities were common (~~S~~)(X)(U)

~~S E C R E T~~

CIA INFO CLASSIFIED PER
ITS 8/5/94 LTR.
9/83 [illegible] #21,326 4/27/9[illegible]

~~GROUP 1~~
~~Excluded from automatic downgrading and declassification.~~

SEE REVERSE
SIDE FOR
CLASSIFICATION
ACTION

31

~~SECRET~~

RELEASED PER P.L-102-526(JFK ACT)
NARA DATE 4/28/05

Reproduced at the National Archives

SECRET

RE: CUBAN REPRESENTATION IN EXILE (RECE).

knowledge in exile circles. Mas interpreted this to mean U. S. tacit approval to the operation. (U)

It is noted that "The Miami Herald," a daily newspaper published in Miami, Florida, on May 22, 1965, reported that two homemade bombs were thrown into a building occupied by the Mexican-Russian Cultural Relations Institute in Mexico City on May 21, 1965. Mexican police said they found a Cuban flag at the scene. Aldo Rosado Tuero, General Coordinator for Movimiento Nacionalista Cristiano (MNC), claimed that five commandos from his group in Mexico City did the bombing.

"The Miami Herald," on July 11, 1965, contained an article stating two Mexicans were in jail in Mexico City as accomplices of a Cuban-American in a Miami based plot to bomb leftist installations throughout Latin America.

The police said that Manuel de la Isla Paulin, Daniel Ituarte, and Henry Agueros Garces are members of a group which is affiliated with the Miami Cuban refugee National Christian Movement. De la Isla admitted taking part with Agueros in the May, 1965, attack on the Mexican-Russian Cultural Relations Institute in Mexico City.

MM T-1, on July 2, 1965, stated that a Cuban refugee who was associated with Cuban activists in Miami, and who has furnished reliable information in the past, stated that Luis Posada Carriles, on June 25, 1965, said that Jorge Mas Canosa paid him $5,000.00 to cover the expenses of a demolition operation in Mexico. (U)

SECRET

UNCLASSIFIED PER CIA'S 7/5/91 LTR. 9503 #211,326 4/29/95

RELEASED PER P.L-102-526(JFK ACT)
NARA DATE 4/28/05

Reproduced at the National Archiv

SECRET

RE: CUBAN REPRESENTATION IN EXILE (RECE).

Posada said he was planning to place limpet mines on either a Cuban or Soviet vessel in the harbor of Veracruz, Mexico, and had 100 pounds of C-4 explosives and detonators. Posada said he was preparing certain papers to show he is a Puerto Rican to enable him to obtain a visa for entry into Mexico. (U)

Immigration and Naturalization Service (INS) records, at Miami, Florida, on November 14, 1961, under INS Number A12 419 708, reflect that Luis Clemente Posada Carriles entered the United States at Miami from Cuba on April 28, 1961. He resided at 1761 S. W. 5th Street, Miami Fl. Posada's INS file reflected the following information:

Race	White
Sex	Male
Born	February 15, 1928, Cienfuegos, Cuba
Employment	Supervisor, Firestone Rubber Company.
Marital Status	Married
Wife	Concepcion Castaneda Napoles.

MM T-1, on September 6, 1961, stated that the Unidad Revolucionaria, an anti-Castro organization, planned to select infiltration teams from its commando group known as the Black Falcons. The teams would be given special training, and Luis Poveda Carriles was selected as one of the participants. No further background information was available concerning Poveda. (U)

On June 23, 1964, Luis Posada, at Polk City, Florida, gave a signed statement to the FBI, stating the following:

SECRET

CIA UNCLASSIFIED PER ITS 9/5/91 LTR. 9803 #211,326 4/29/92

RELEASED PER P.L-102-526(JFK ACT)
NARA DATE 4/28/05

Reproduced at the Nationa

S E C R E T

RE: CUBAN REPRESENTATION IN EXILE (RECE)

He was then 36 years of age, served in the U. S. Army one year, and resided at 750 N. W. 15th Street, Miami. He had joined Junta Revolucionaria Cubana, an anti-Castro organization known as JURE. About three months before, he went to Polk City, Florida, and with other JURE members, built a military training camp on property belonging to Mr. Weir Williams. After that military training courses in guerrilla warfare were given, and three groups of eight men each were trained. He explained the purpose of the training was for guerrilla warfare in Cuba, and they planned to be in Cuba by May 20, 1964, but the plan failed.

Posada continued that he had not been told they had the support of the U. S. Government, but they did believe they had U. S. Government tolerance by the very fact they had not been bothered by anyone while they conducted their military training activities.

On June 25, 1965, Weir P. Williams stated that he had not been contacted by the U. S. Government to allow these Cubans to use his property, but was led to believe it was in accord with the Government's desire. He said that the uniforms, boots and equipment appeared to be U. S. Government issue, and on one occasion the Sheriff of Polk County, Florida, told Williams he had checked with the Federal Government and verified it was operating with U. S. Government approval.

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

S E C R E T

RELEASED PER P.L-102-526(JFK ACT)
NARA DATE 4/28/05

Reproduced at the National Archives

UNITED STATES DEPARTMENT OF JUSTICE

FEDERAL BUREAU OF INVESTIGATION

SECRET

In Reply, Please Refer to
File No.

DECLASSIFIED 5668 SLD/KSR
BY 6-27-98 (JFK)

~~SECRET~~

2-380

Miami, Florida
May 17, 1965

Classified by
Declassify on: OADR

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
EXCEPT WHERE SHOWN
OTHERWISE

RE: ROBERTO ALEJOS ARZU;
LUIS SIERRA LOPEZ
NEUTRALITY MATTERS
INTERNAL SECURITY - GUATEMALA

It is noted that ROBERTO ALEJOS ARZU, 180 Palm Drive, Palm Island, Miami Beach, Florida, is a wealthy Guatemalan national and has been conspiring to overthrow the Government of Guatemala.

On May 6, 1965, Mr. ALLEN S. YARBOROUGH, U. S. Customs Agent, Miami, Florida, furnished the following information: (U)

All information from Customs was declassified per Customs on 11-24-97

LUIS SIERRA LOPEZ, a Cuban exile associated with ALEJOS, was arrested by Mexican authorities in Tapachula, Mexico, on April 29, 1965. SIERRA was subsequently released and arrived in Miami, Florida, on May 2, 1965, where he was met by ALEJOS and LUIS POSADA, another Cuban exile associated with ALEJOS. (U)

As a result of a series of conferences held by Mr. YARBOROUGH with SIERRA and POSADA and other exiles associated with ALEJOS, the following munitions were surrendered to U. S. Customs agents on May 4, 1965:

1 .30 cal. machine gun, M-1919A4
1 .30 cal. machine gun, M-1919A4
1 Browning Automatic Rifle
1 Flame Thrower w/tanks and gun
1 Portable Flame Thrower Gun, No. M-2A1

(U)

SEE REVERSE
SIDE FOR
CLASSIFICATION
ACTION

~~SECRET~~
~~Group 1~~
~~Excluded from automatic downgrading and declassification~~

SECRET

ENCLOSURE

SECRET

RE: ROBERT ALEJOS ARZU;
LUIS SIERRA LOPEZ

1 Carbine .30 cal. M-1 short stock, without trigger mechanisms
1 Carbine .30 cal. M-1 short stock
3 Carbines .30 cal. M-1, long stock (no serial Nos.)
1 Carbine .30 cal. M-1 long stock, Serial No. 2888
1 .30 cal. barrel (packed)
1 Thompson .45 cal. submachine gun, 1928 model
1 Pistol, .45 cal. Colt automatic
10 .45 cal. M-3 Grease guns
1 Rocket Launcher, 3.5", M-20 (Bazooka)
2 Mortar, 60 MM, M-5, tripod, base plate, barrel
1 Electric blasting machine, U. S. Army 10 cap.
2 Mount, tripod, .30 cal. M-2
2 Mount, bipod, .30 cal. M-2
15 Garand Rifles, M-1

Ammunition

1500 rounds M-2 30.06 ball linked armor piercing
3240 rounds M-2 30.06 ball
700 rounds carbine .30 cal. ball
100 rounds pistol, .38 cal. (ball)
400 rounds .45 cal. (ball)
100 rounds .50 cal. (ball)
5 rounds 12 gauge shotgun shells
3 Flares, Marine
1 Ammunition belt for BAR
11 Bandaleers - empty
43 Clips - BAR
108 Clips - .45 cal. M-3 Grease gun
1 Clip (round) - .45 cal. Thompson, 1928 Model submachine gun

(b)(4)

SECRET

SECRET

RE: ROBERT ALEJOS ARZU;
LUIS SIERRA LOPEZ

26 Clips - .45 cal. pistol
28 Grenade adapters, M-1 Garand rifle
1 Pistol holster, .45 cal. Colt
1 Pistol holster, .38 cal.
5 Trigger Mechanisms, .30 cal. M-2 carbine conversion
24 Pistol Belts
6 Cartridge Belts

32 Blocks C-4 ($2\frac{1}{2}$ lbs. each) 80 lbs.
12 Blocks C-3 ($2\frac{1}{4}$ lbs. each) 28 lbs.
24 Blocks TNT (1 lb. each) 24 lbs.
8 Blocks Pinolite (1 lb. each) 8 lbs.
2 cans Napalm (3 gal. each) 6 gals.
16 rockets Bazooka (3.5 inch dia. H.E.)
44 sticks Dynamite (Military) 1 - lb. each 44 lbs.
46 rounds 57 MM Mortar Shells
51 M-21 Hand Grenades (fragmentation)
3 Tear gas Grenades
6 Rifle Grenades
5 rolls Orange-wax fuse clover brand - Total of 170 feet
20 each Fuse lighters
2 each Heavy duty primers (1 lb. each)
1 box Fuse Lighter Primers (100 each)
53 Blasting caps
1 roll Detonating wire - approx. 1/4 mile

1 Ammunition Bag, M-1 Garand Rifle
1 Satchel, tool bag
7 Gun Slings
1 Val-Pac suitcase for clothes

SECRET

NARA DATE

SECRET

RE: ROBERT ALEJOS ARZU;
LUIS SIERRA LOPEZ

26 Pairs Coveralls - Air Force type
1 Poncho
40 Suspenders, web, for carrying field packs
1 12 gauge Winchester semi-auto. shotgun

Mr. YARBOROUGH said that as a result of investigation, interviews, and intelligence information, it was ascertained that the following individuals have been in some way involved in ALEJOS' conspiracy:

LUIS SIERRA LOPEZ
LUIS POSADA CARRILES
AMADO CANTILLO HUGUET
EUGENIO AGUILERA FRUTOS
BERNADO BOSCH RODRIGUEZ
HIPOLITO MARTINEZ TERRERO
VICTOR VASQUEZ
JOSE RONDON
RAMON ESCARDA RUBIO
JOSE SALAZAR JARDON
JOSE F. VERNIER (VERRIER)
JESUS MARTINEZ
ANTONIO CONSTANZO CONSTANCE PALAU
ANTONIO PEREZ BASULTO
HORACIO SOTOLONGO GARCIA
BLAS ERNESTO MARTINEZ DOMINGUEZ
GASTON CAMPITRUZ SILVA
GUILLERMO RODRIGUEZ
JUAN HERNANDEZ
ROLANDO MARIN GONZALEZ
LORETO SANTIAGO GUIJARRO
GERADO MARTINEZ

foreign

SECRET

RELEASED PER P.L-102-526(JFK ACT)
NARA DATE 5/4/05

Reproduced at the National Archives

MESSAGE RELAY

Transmit in [X] Plaintext [X] Immediate Date 10/8/76
[X] Cipher [ ] Urgent
[ ] Nitel

From: Director, FBI

To: SAC Miami
SAC San Juan

Mexico City
Buenos Aires

To: RUEADWW [X] The President [ ] The Vice President [ ] White House Situation Room

RUEBAAA [X] Attorney General [X] Deputy Attorney General
[X] Attn: Analysis and Evaluation Unit

RUEBWAA [ ] Assistant Attorney General, Civil Rights Division

RUEBWAA [X] Assistant Attorney General, Criminal Division
[X] Attn: General Crimes Section

RUEAGNC [ ] Drug Enforcement Administration

RUEBWAA [X] Immigration and Naturalization Service

RUEBWAA [ ] 1009 Marshall Street

RUEBQUA [ ] Department of the Air Force (AFOSI)

RUEAGII [ ] Department of the Army

RUEADIA [X] Director, DIA

RUEBGAA [X] Commandant, U.S. Coast Guard

RUEKCIA [X] Director, Defense Intelligence Agency

RUEBGTN [ ] Bureau of Research and Development, Administration

RUEGCBA [X] Postal Service Administration

RUEBARE/ [ ] Naval Investigative Service

RUEADSA/ [ ] U.S. Postal Service

RUEBSB/ [X] U.S. Secret Service (USN)

RUEHC [X] Secretary of State

RUEBQIA/ [ ] Department of Defense
Attn: Director, Security

RUEATRA [X] Department of Treasury
[X] Attn: U.S. Customs

Classified by Scelfano 6/9/83
Declassify on: OADR

COMMUNICATIONS SECTION

OCT 08 1976

TELETYPE

OCT 10 1976

OCT 16 1976

SECRET

SECRET

FEDERAL BUREAU OF INVESTIGATION
COMMUNICATIONS SECTION
OCT 07 1976
TELETYPE

~~O 072345Z OCT 76~~
~~RL CARACAS (2-0)~~
~~TO DIRECTOR IMMEDIATE AM 100-07~~
~~BT~~
~~S E C R E T~~

Cubana Airlines

UNSUBS; SUSPECTED BOMBING OF CUBANA AIRLINES DC-8 NEAR BARBADOS, WEST INDIES, OCTOBER 6, 1976, AM - CUBA - WEST INDIES.

By teletype 10/7/76, LEGAT CARACAS ADVISED AS FOLLOWS:

CUBANA AIRLINES FLIGHT 455, DC-8 AIRCRAFT LEASED BY CUBANA FROM AIR CANADA, CRASHED IN THE CARIBBEAN SEA OFF THE COAST OF BARBADOS AT ABOUT 1:45 PM ON OCTOBER 6, 1976, SHORTLY AFTER TAKEOFF FROM SEAWELL AIRPORT, BARBADOS, EN ROUTE TO HAVANA, CUBA, VIA KINGSTON, JAMAICA. NO SURVIVORS REPORTED AMONG THE 78 PERSONS ABOARD THE PLANE.

ACCORDING TO AMERICAN EMBASSY, BRIDGETOWN, BARBADOS, PILOT REPORTED TO SEAWELL AIRPORT TOWER SHORTLY BEFORE CRASH THAT AN EXPLOSION HAD OCCURRED ABOARD THE PLANE. FLIGHT LOG RECOVERED AFTER CRASH NOTED POWER FAILURE IN NUMBER FOUR ENGINE, BUT NO MENTION OF EXPLOSION. AIRPORT OFFICIAL AT BARBADOS REPORTEDLY INFORMED THAT PILOT TOLD TOWER THERE HAD BEEN EXPLOSION IN ONE OF THE REAR LAVATORIES OF THE PLANE.

STATE DEPT. INFO (PARA 2 - END) IS UNCLASSIFIED PER DOS AUTHORITY 4/29/96.

AMERICAN EMBASSY, PORT OF SPAIN, TRINIDAD, ADVISED ON OCTOBER 7, 1976, AS FOLLOWS:

"TRINIDAD AND TOBAGO POLICE ARE HOLDING TWO VENEZUELAN

SECRET

~~END PAGE ONE~~

~~CARBON COPY DO NOT FILE~~

2

SECRET

~~END CAPTION SECRET~~

TELEGRAMS WHOM THEY BELIEVE MAY BE CONNECTED WITH THE CUBANA AIRLINE CRASH OCTOBER 6 OFF BARBADOS. TWO SUSPECTS ARE:

"A. JOSE VAZQUEZ GARCIA - HOLDER OF VENEZUELAN PASSPORT 720733 (THIS IS THE PERFERATED NUMBER--NUMBER WRITTEN IN THE PASSPORT IS 3140806), ISSUED ON JUNE 6, 1976, IN CARACAS. BORN DECEMBER 9, 1950 IN CARACAS. HOLDS VENEZUELAN ID CEDULA V 3140806.

"B. FREDDY (NOT FEDERICO) LUGO - HOLDER OF VENEZUELAN PASSPORT 006543 (THIS IS THE PERFERATED NUMBER--NUMBER WRITTEN IN THE PASSPORT IS 2123,051), ISSUED JULY 6, 1976, IN CARACAS. SINGLE. BORN OCTOBER 17, 1942. GAVE RESIDENCE AS CARACAS AND OCCUPATION AS JOURNALIST. HOLDS ID CEDULA VO 2123051. CARRIES OFFICIAL PRESS CARD NO 152 OF CIRCULO DE REPORTEROS GRAFICOS DE VENEZUELA. LUGO ALSO HAD IN HIS POSSESSION TOURIST CARD FOR COLOMBIA DATED JULY 15, 1976. THIS GAVE PERMANENT ADDRESS AD URB URDANETA VERDA 24, CARACAS.

"THESE TWO VENEZUELANS ARRIVED IN TRINIDAD FROM CARACAS ON PANAM 443 EARLY MORNING HOURS WEDNESDAY, OCTOBER 6. CHECKED INTO HOLIDAY INN AT 0200 HOURS. HOTEL REGISTRATION MADE IN NAMES OF

~~END PAGE TWO~~

STATE DEPT. INFO (ALL PARAS) IS UNCLASSIFIED PER DOS AUTHORITY 8/26/96

SECRET

~~PAGE TWO S E C R E T~~

JOSE GARCIA/FREDDY PEREZ. HOME ADDRESS GIVEN AS URB CRISTO REY NO 61, VALENCIA, VENEZUELA. HAD LUGGAGE WHEN CHECKED INTO HOTEL.

"VENEZUELANS CHECKED OUT OF HOLIDAY INN ABOUT 0600 OCTOBER 6 WITH LUGGAGE AND WERE SEEN AT PIARCO AIRPORT. BOARDED GUYANA FLIGHT AT 1150 OCTOBER 6 TO BARBADOS.

"RETURNED FROM BARBADOS TO TRINIDAD ON SAME DAY ON BWIA FLIGHT AT 2155 AND CHECKED INTO HOLIDAY INN AT 2360 WITHOUT SUITCASES. REGISTRATION IN NAME OF GUSTAVO GARCIA, RESIDENCE BOGOTA, COLOMBIA. THEY CLAIMED THE SUITCASES HAD BEEN STOLEN, BUT THEY HAVE MADE NO REPORT OF STOLEN SUITCASES EITHER TO AIRLINE OR BARBADOS OR TRINIDAD POLICE.

"AMONG DOCUMENTS IN HANDS OF POLICE IS BOARDING PASS OF E. SEALY FOR DIFFERENT BWIA FLIGHT. POLICE CHECKING THIS OUT. THIS THEY BELIEVE COULD BE TRINIDAD ACCOMPLICE.

"OF INTEREST IS FACT BOTH PASSPORTS FAIRLY NEW. THEREFORE DIFFICULT TRACE PAST TRAVEL. HOWEVER, PASSPORT OF FREDDY LUGO DID HAVE STAMP SHOWING ENTRY AT BARBADOS ON JULY 9. (NOTE: THE BOMBS WHICH WENT OFF AT THE BWIA OFFICE AND AT THE GENERAL MANAGER'S CAR AND YACHT IN BRIDGETOWN, BARBADOS, TOOK PLACE ON 10 AND 11 JULY 1976.)

~~END PAGE THREE~~

STATE DEPT. INFO (ALL PARAS.) IS UNCLASSIFIED PER DOS AUTHORITY 8/28/96

SECRET

4

SECRET

~~PAGE FOUR SECRET~~

"PAGE IN POSSESSION OF LIGO APPARENTLY FROM ADDRESS BOOK WITH LETTER "S" ON IT CITED FOLLOWING: EMBASSY AMERICAN 2346111-1371 ATT JOSEPH LEO 33/9 11.

"TRINIDAD AND TOBAGO POLICE ARE FINGERPRINTING BOTH SUSPECTS AND COPYING ALL DOCUMENTS IN THEIR POSSESSION.

"TRINIDAD AND TOBAGO POLICE REQUEST URGENTLY ANY INFORMATION OF THESE PERSONS, PARTICULARLY ANY CRIMINAL RECORDS. NO OBJECTION TO LEGATT CONTACTING LOCAL POLICE/SECURITY SERVICES. POLICE REQUEST AT LEAST INTERIM REPLY BEFORE 1700 LOCAL TIME. PLEASE SEND REPLY REACT IMMEDIATE.

"POLICE WOULD LIKE TO KNOW IF ANYONE FROM LEGATT OFFICE PLANS TO COME TO TRINIDAD ON THIS CASE, OR HOW YOUR WOULD LIKE TO RECEIVE COPIES OF FINGERPRINTS, ETC."

[redacted] 4

[redacted] (S)

ON OCTOBER 7, 1976, A CONFIDENTIAL SOURCE ABROAD ADVISED THAT (S)

END PAGE FOUR

SECRET

SECRET

~~PAGE FIVE OAR 2-9 S E C R E T~~

FREDDY LUGO IS A VENEZUELEN NEWSMAN WHO IS ALSO EMPLOYED AS AN INVESTIGATOR BY LUIS POSADA, [redacted] (S) CARACAS. HE RESIGNED FROM HIS POSITION [redacted] (S) IN 1973 [redacted] (S) POSADA IS A CUBAN EXILE WHO IS KNOWN FOR HIS ANTI-CASTRO ACTIVITIES, AND HE REPORTEDLY ASSISTED ORLANDO BOSCH AVILA IN 1976, SHORTLY BEFORE BOSCH WAS ARRESTED BY VENEZUELAN AUTHORITIES. (S)

LEGAT BECAME ACQUAINTED WITH POSADA WHILE THE LATTER WAS [redacted] (S) AND AFTER HIS RESIGNATION, POSADA CONTINUED TO CONTACT LEGAT ON RARE OCCASIONS, USUALLY IN ORDER TO OBTAIN PERSONALIZED SERVICE IN CONNECTION WITH VISA REQUESTS. IN VIEW OF LUGO'S EMPLOYMENT BY POSADA, LEGAT ASSUMES HIS NAME AND TELEPHONE NUMBER WERE FURNISHED TO LUGO BY POSADA. LEGAT ESTIMATES HE HAS SEEN POSADA IN PERSON ON PERHAPS THREE OCCASIONS SINCE 1973, THE LAST TIME BEING ON JUNE 10, 1976, WHEN POSADA VISITED LEGAT OFFICE TO INQUIRE IF FBI HAD INTEREST IN CARLO BORDONI (BUFILE 29-[illegible], ORFILE 29-[illegible]). INFORMED IN THE AFFIRMATIVE, POSADA REVEALED BORDONI HAD HIRED TWO OF HIS OPERATIVES AS ARMED BODY GUARDS AT HIS HOME. THAT INFORMATION WAS SUBSEQUENTLY PASSED BY LEGAT TO [redacted] WHO WERE INVOLVED IN THE ARREST ACTION AGAINST BORDONI. (S) (S)

~~END PAGE FIVE~~

SECRET

SECRET

~~PAGE SIX CAR C O S E C R E T~~

POSADA MORE OFTEN REFERRED TO LEGAT RELATIVES AND ASSOCIATES SEEKING ADVICE REGARDING VISAS, THE LAST BEING ONE OF HIS EMPLOYEES, HERNAN RICARDO LOZANO, WHO SOUGHT A VISA TO TRAVEL TO SAN JUAN, PUERTO RICO, ON OCTOBER 1, 1976. LEGAT WILL PROVIDE ADDITIONAL INFO DEVELOPED REGARDING RICARDO IN A SUBSEQUENT COMMUNICATION. (S)

ON OCTOBER 7, 1976, THE CONFIDENTIAL SOURCE FURTHER ADVISED THAT IN VIEW OF THE ARREST OF VAZQUEZ AND LUGO IN TRINIDAD, THE [redacted] B
[redacted] (S)(U) WAS ARRANGING FOR LUIS POSADA AND ORLAND BOSCH AVILA TO LEAVE [VENEZUELA] (S)(U) AS SOON AS POSSIBLE. THE SOURCE ALL BUT ADMITTED THAT POSADA AND BOSCH HAD ENGINEERED THE BOMBING OF THE AIRLINE, AND HE PROMISED TO FURNISH FURTHER DETAILS ON OCTOBER 8, 1976. (S)

~~CLASSIFIED BY 4420, ADD. EXEMPTIONS B AND A, INDEFINITE.~~

ADMIN TO FIELD AND LEGATS ONLY

ADMINISTRATIVE: CONFIDENTIAL SOURCE IS [redacted] A
[redacted] CARACAS, A-B
VENEZUELA. (S)(U)

FROM STATEMENTS OF [redacted] IT APPEARS ALMOST CERTAIN THAT THE A
[redacted] WAS PRIVY TO THE ACTIVITIES OF POSADA AND B
BOSCH AND THAT IT NOW WILL ATTEMPT TO DISASSOCIATE ITSELF FROM THEM FOR FEAR OF RETALIATION BY THE CUBAN GOVERNMENT. (S)(U)

IN

ADMIN TO FIELD AND LEGATS ONLY

SECRET

INITIAL 7WD

RELEASED PER P.L-102-526(JFK ACT)
NARA DATE 5/4/05

Reproduced at the National Archive

WMO938 3080105
PP HI WF
DE MM
P 020105Z NOV 76FM MIAMI (2-469) (P)
TO DIRECTOR PRIORITY
WASHINGTON FIELD PRIORITY
BT
S E C R E T
~~SECTION 1 OF 2~~
NO FOREIGN DISSEMINATION
UNSUBS; BOMBING OF CUBANA AIRLINES DC-8 NEAR BARBADOS, WEST INDIES, OCTOBER 6, 1976. NEUTRALITY MATTERS- CUBA - WEST INDIES. ~~(MIAMI FILE 2-469)~~
~~CHILBOM, PFO- MURDER; EID. OOJ. (MIAMI FILE 185-76).~~

ON NOVEMBER 1, 1976, A CONFIDENTIAL SOURCE WHO HAS FURNISHED RELIABLE INFORMATION IN THE PAST ADVISED THAT ON OCTOBER 23-24, 1976, RICARDO MORALES NAVARRETE, COMISARIO IN CHARGE OF SECTION D54, A COUNTERINTELLIGENCE SECTION OF DISIP (VENEZUELAN INTELLIGENCE SERVICE), FURNISHED THE FOLLOWING INFORMATION TO SOURCE:

SOME PLANS REGARDING THE BOMBING OF A CUBANA AIRLINES AIRPLANE WERE DISCUSSED AT THE BAR IN THE ANAUCO HILTON HOTEL IN CARACAS, VENEZUELA, AT WHICH MEETING FRANK CASTRO,

RELEASED PER P.L-102-526(JFK ACT)
NARA DATE 5/4/05
Reproduced at the National Archives

GUSTAVO CASTILLO, LUIS POSADA CARRILES AND MORALES NAVARRETE WERE PRESENT. THIS MEETING TOOK PLACE SOMETIME BEFORE THE BOMBING OF THE CUBANA AIRLINES DC-8 NEAR BARBADOS ON OCTOBER 6, 1976.

FRANK CASTRO IS A LEADER OF CORU, THE ANTI-CASTRO TERRORIST ORGANIZATION WHICH HAS TAKEN CREDIT FOR SEVERAL BOMBINGS. GUSTAVO CASTILLO IS ONE OF THREE PERSONS INVOLVED IN THE ATTEMPTED KIDNAPING OF THE CUBAN CONSUL IN MERIDA YUCATAN ON JULY 23, 1976, AT WHICH TIME THE CONSUL'S BODYGUARD WAS SLAIN. ORESTES RUIZ HERNANDEZ AND GASPAR JIMENEZ WERE APPREHENDED BY MEXICAN AUTHORITIES BUT CASTILLO EVADED CAPTURE. LUIS POSADA CARRILES HAS BEEN ARRESTED BY VENEZUELAN AUTHORITIES IN CONNECTION WITH THE CUBANA AIRLINES DC-8 BOMBING.

MORALES NAVARRETE TOLD THE SOURCE THAT ANOTHER MEETING TO PLAN THE BOMBING OF A CUBANA AIRLINER TOOK PLACE IN THE APARTMENT OF MORALES NAVARRETE IN THE ANUCO HILTON. THIS MEETING WAS ALSO PRIOR TO THE BOMBING OF THE CUBANA AIRLINER ON OCTOBER 6, 1976. PRESENT AT THIS MEETING WERE MORALES NAVARRETE,

RELEASED PER P.L.-102-526(JFK ACT)
NARA DATE 5/4/05
Reproduced at the National Archives

POSADA CARRILES AND FRANK CASTRO. ACCORDING TO MORALES NAVARRETE, AT THIS MEETING THERE WAS SOME DISAGREEMENT AS TO WHO WOULD TAKE PART IN THE VARIOUS PHASES OF THE OPERATION, AND WHO WOULD CLAIM CREDIT FOR THE BOMBING. FRANK CASTRO SAID THE FLNC (NATIONAL LIBERATION FRONT OF CUBA) WOULD TAKE CREDIT.

THE FLNC IS AN ANTI-CASTRO TERRORIST ORGANIZATION WHICH HAS TAKEN CREDIT FOR SEVERAL BOMBINGS.

MORALES NAVARRETE SAID THAT AFTER THIS MEETING HE HAD NOTHING MORE TO DO WITH THIS MATTER. HE ADDED THAT AFTER THE CABANA AIRLINER BOMBING ON OCTOBER 6, 1976, FRANK CASTRO DID NOT WANT THE FLNC TO CLAIM CREDIT AS HE WAS AFRAID OF REPRISALS BY THE CUBAN GOVERMNENT.

MORALES NAVARRETE SAID THAT THE GROUP INVOLVED HAD PREVIOUSLY ATTMEPTED TO BOMB A CUBANA AIRLINER IN PANAMA AND IN JAMAICA.

MORALES NAVARRETE SAID THAT SOME PEOPLE IN THE VENEZUELAN GOVERNMENT ARE INVOLVED IN THIS AIRPLANE BOMBING, AND THAT IF POSADA CARRILES TALKS, THEN MORALES NAVARRETE AND OTHERS IN

RELEASED PER P.L-102-526(JFK ACT)
NARA at DATE 5/4/05
Reproduced at the National Archives

THE VENEZUELAN GOVERNMENT WILL "GO DOWN THE TUBE". HE SAID THAT IF PEOPLE START TALKING "WE'LL HAVE OUR OWN WATERGATE".

MORALES NAVARRETE SAID THAT AFTER THE CUBANA AIRLINER CRASH, HERNAN RICARDO LOZANO TELEPHONED ORLANDO BOSCH FROM TRINIDAD STATING " A BUS WITH 73 DOGS WENT OFF A CLIFF AND ALL GOT KILLED". BOSCH, KNOWING THAT MANY PHONE CALLS ARE TAPPED BY THE VENEZUELAN GOVERNMENT, PRETENDED HE DID NOT KNOW WHAT HERNAN RICARDO LOZANO WAS TALKING ABOUT.

SOURCE SAID THAT IN A CONVERSATION WITH ORLANDO GARCIA VASQUEZ, MINISTER COUNSELLOR ON SECURITY MATTERS TO VENEZUELAN PRESIDENT CARLOS ANDRES PEREZ, GARCIA VASQUEZ TOLD SOURCE THAT SHORTLY AFTER THE CUBANA CRASH, GRACIA VASQUEZ TALKED TO CARLOS FABRI, THE BOMB EXPERT FOR DISIP. GARCIA VASQUEZ TOLD FABRI THAT HE WOULD HAVE TO TESTIFY AT ANY TRIAL IN THIS MATTER REGARDING BOMBS AND THEIR COMPONENTS. ACCORDING TO GARCIA VASQUEZ, FABRI BECAME VERY NERVOUS AND GARCIA VASQUEZ TOLD SOURCE HE BELIEVES THAT FABRI EITHER MADE THE BOMB FOR THIS CUBANA BOMBING, INSTRUCTED PERSONS ON HOW TO MAKE IT , OR AT LEAST HAD PRIOR KNOWLEDGE OF THE BOMBING.

NARA dt DATE 5/4/05

GARCIA VASQUEZ MENTIONED THAT THE BOMB ON THE CUBANA AIRLINER WAS ACTIVATED BY A "LAPICERO" (TIME PENCIL).

SOURCE SAID THAT HE ALSO CONVERSED WITH A MEMBER OF THE VENEZUELAN POLICIA TECNICA JUDICIAL (JUDICIAL TECHNICAL POLICE) (PTJ) IN CARACAS. THIS MEMBER, WHOSE NAME SOURCE DOES NOT RECALL, BUT WHO HAS A POLISH NAME, SAID THAT AFTER THE CUBANA AIRLINER CRASHED, THE PTJ KNEW WHO WAS INVOLVED AND THEREFORE WANTED TO HANDLE THE INVESTIGATION. HOWEVER, THE PTJ WAS DENIED THE INVESTIGATION AND DISIP TOOK OVER THE MATTER "TO COVER IT UP". THIS PTJ MEMBER ALSO TOLD SOURCE THAT IF CARLOS FABRI DID NOT MAKE THE BOMB, THEN HE AT LEAST HAD PRIOR KNOWLEDGE OF THE MATTER.

SOURCE SAID THAT FABRI AND POSADA CARILLES ARE GOOD FRIENDS AND THAT FABRI AND POSADA HAD ACTUALLY BEEN ARRESTED A COUPLE OF YEARS AGO BY VENEZUELAN AUTHORITIES AFTER IT WAS LEARNED THEY PORVIDED FALSE DOCUMENTATION AND EXPLOSIVES TO DR. ORLANDO BOSCH AVILA IN VENEZUELA AT THAT TIME.

NARA [illegible] DATE 5/4/05

DR. ORLANDO BOSCH AVILA IS A FUGIVE FROM THE U.S., LEADER OF CORU, AND IS IN CUSTODY IN VENEZUELA IN CONNECTION WITH THIS CUBANA AIRLINES BOMBING.

MORALES NAVARRETE TOLD SOURCE THAT ORLANDO BOSCH SAID THAT GUILLERMO NOVO VISITED CHILE IN EARLY 1975 AT WHICH TIME HE VISITED BOSCH. DURING THIS PERIOD, GUILLERMO NOVO MAKE CONTACT WITH AN ULTRA-RIGHTWING ORGANIZATION KNOWN AS "PATRIA Y LIBERTAD" (FATHERLAND AND LIBERTY). BOSCH SAID THAT ORLANDO LETELIER'S DEATH WAS THE RESULT OF AN AGREEMENT BETWEEN GILLERMO NOVO AND THE "PATRIA Y LIBERTAD" ORGANIZATION. MORALES NAVARRETE SAID THAT SOME MEMBERS OF "PATRIA Y LIBERTAD" ARE ALSO MEMBERS OF "DINA", A CHILEAN INTELLIGENCE SERVICE. SOURCE WAS UNABLE TO LEARN FURTHER INFORMATION REGARDING THIS MATTER.

MORALES NAVARRETE ALSO TOLD SOURCE THAT GUSTAVO CASTILLO AND MEMBERS OF HIS GROUP ARE RESPONSIBLE FOR THE FOLLOWING BOMBINGS IN THE MIAMI, FLORIDA AREA: BOMBING OF THE DOMINICAN CONSULATE ON OCTOBER 6, 1975, BOMBING OF THE DOMINICAN AIRLINES TICKET OFFICE ON OCTOBER 20, 1975; BOMBINGS AT THE BROWARD COUNTY COURT HOUSE ON OCTOBER 10, 1975; AND ATTEMPTED BOMBING OF A

RELEASED PER E.O. 12958 (AS AMENDED)
NARA [illegible] DATE 5/4/05

BAHAMASAIR AIRLINER AT MIAMI INTERNATIONAL AIRPORT ON NOVEMBER 27, 1975. ACCORDING TO MORALES NAVARRETE, THE ORGANIZATION "YOUTH OF THE STAR", WHICH CLAIMED CREDIT FOR THESE BOMBINGS, IS COMPOSED OF GUSTAVO CASTILLO, GASPAR JIMENEZ, ORESTES RUIZ HERNANDEZ, DUNEY PEREZ ALAMO AND RACIEL RODRIGUEZ GONZALEZ WHO IS THE YOUNGER BROTHER OF REINOL RODRIGUEZ, FLNC MEMBER WHO RESIDES IN SAN JUAN, PUERTO RICO. THIS GROUP IS GENERALLY INDEPENDENT EVEN THOUGH MEMBERS WILL ACCOMPLISH TERRORIST ACTS FOR THE FLNC OR OTHER CUBAN TERRORIST GROUPS.

SOURCE ADVISED THAT ON OCTOBER 27, 1976, THE VENEZUELAN GOVERNMENT ISSUED SOME TYPE OF NEWS RELEASE STATING THAT THERE IS NO RICARDO MORALES NAVARRETE IN DISP. SINCE THAT TIME, SOURCE HAS TELEPHONED NAVARRETE TO HIS OFFICE AND TO HIS APARTMENT AT THE ANAUCO HILTON IN CARACAS. PERSONS ANSWERING THE PHONE STATE THAT THEY KNOW OF NO RICARDO MORALES NAVARRETE NOR DO THEY KNOW OF COMISARIO MOISES (A CODE NAME FOR MORALES NAVARRETE). SOURCE SAID THAT MORALES NAVARRETE TELEPHONED HIS GIRL FRIEND IN MIAMI, FLORIDA, TELLING HER NOT TO PHONE HIM AS "HE DOES NOT

NARA Art DATE 5/4/05

PAGE EIGHT ~~MM 2 469 S E C R E T~~

EXIST". MORALES NAVARRETE SAID HE WOULD TELEPHONE HER INSTEAD. MOST OF THE ABOVE INFORMATION WAS TOLD IN STRICT CONFIDENCE TO SOURCE AND DIVULGENCE OF THIS INFORMATION WOULD IMMEDIATELY PINPOINT THE SOURCE WHO REQUESTED THAT THIS INFORMATION NOT BE DIVULGED OUTSIDE THE U. S. GOVERNMENT. THEREFORE, NO ACTION SHOULD BE TAKEN ON THE ABOVE INFORMATION WHICH COULD COMPROMISE THE SOURCE.

~~CLASSIFIED BY 6090 OHM NOT E.O. 5 INDEFINITE.~~
Administrative Data to Legals Only
ADMINISTRATIVE.

SOURCE IS RAUL DIAZ, ORGANIZED CRIME BUREAU, DADE COUNTY PUBLIC SAFETY DEPARTMENT, WHO TRAVELED TO VENEZUELA ON OCTOBER 22, 1976, IN AN ATTEMPT TO CONVINCE MORALES NAVARRETE TO TESTIFY IN THE NOVEMBER 15, 1976 STATE TRIAL OF ROLANDO OTERO FOR NINE BOMBINGS IN MIAMI, INCLUDING THAT OF THE MIAMI FBI OFFICE.

NARA DATE 5/9/05

DIAZ SAID THAT MORALES NAVARRETE SAID THAT THE FLORIDA STATE ATTORNEY'S OFFICE SHOULD REQUEST THE VENEZUELAN GOVERNMENT, THROUGH THE U.S. DEPARTMENT OF STATE, TO HAVE MORALES SO TESTIFY.

RAUL DIAZ REQUESTED THAT HE NOT BE REVEALED AS THE SOURCE OF THIS INFORMATION, AND AS SET OUT IN THE DETAILS, THIS INFORMATION SHOULD NOT BE REVEALED OUTSIDE THE U.S. GOVERNMENT. IT IS NOTED THAT RAUL DIAZ IS A FRIEND OF MORALES NAVARRETE.

REGARDING PATRIA Y LIBERTAD, THE MIAMI OFFICE OPENDED A CASE ON OCTOBER 3, 1973, ENTITLED "PATRIA Y LIBERTAD, IS-CUBA (MIAMI FILE 105-21705)(BUFILE 105-258678)". THIS CASE WAS OPENED WHEN AN INFORMANT OF THE MIAMI OFFICE ADVISED THAT WHEN AN ANTI-CASTRO ORGANIZATION NAMED DIRECTORIO REVOLUCIONARIO WAS DISSOLVED IN MIAMI, SOME OF ITS MEMBERS ATTEMPTED TO ORGANIZE A NEW GOUP, PATRIA Y LIBERTAD, WHICH WAS TO BE HEADED BY ALDO VERA SERAFIN. (IT IS NOTED THAT VERA SERAFIN WAS ASSASSINATED IN SAN JUAN, PUERTO RICO ON OCTOBER 25, 1976). THIS CASE WAS CLOSED IN MARCH, 1975, AS INVESTIGATION REVEALED THAT THIS OPGANIZATION WAS NEVER FORMED. REGARDING BOMBINGS

RELEASED UNDER THE JFK ACT
NARA [illegible] DATE 5/4/05

COMMITTED BY GUSTAVO CASTILLO AND OTHERS IN THE MIAMI AREA, AS MENTIONED BY MORALES NAVARRETE, THE MIAMI OFFICE IS CONDUCTING INVESTIGATION REGARDING THIS AND THE BUREAU WILL BE ADVISED UNDER APPROPRIATE CASE CAPTIONS.

BUREAU IS REQUESTED TO FURNISH ABOVE INFORMATION TO LEGAT, CARACAS.

~~HE~~
~~WFS RCLD~~

Administrative Data to Legat only.

FEDERAL BUREAU OF INVESTIGATION
COMMUNICATIONS SECTION

NOV 03 1976

TELETYPE

~~P 031930Z NOV 76~~
~~TM CARACAS (2-9) (P)~~
~~TO DIRECTOR PRIORITY NR 807-03~~
~~BT~~
~~E F T O~~

IN SUBS; SUSPECTED BOMBING OF CUBANA AIRLINES DC-8 NEAR BARBADOS, WEST INDIES, OCTOBER 6, 1976; NM - CUBA - WEST INDIES.

~~RECAPTEL NOVEMBER 2, 1976.~~

ARREST WARRANTS WERE ISSUED ON NOVEMBER 2, 1976, FOR HERNAN RICARDO LOZANO, FREDDY LUGO, ORLANDO BOSCH AVILA, AND LUIS POSADA CARRILES BY INVESTIGATING JUDGE DELIA ESTABA FOLLOWING THE COMPLETION OF HER PRELIMINARY INVESTIGATION. THE FOUR HAVE BEEN CHARGED WITH "QUALIFIED HOMICIDE" AND THE USE AND MANUFACTURE OF WEAPONS OF WAR. THEY WILL CONTINUE TO BE HELD IN CUSTODY BY VENEZUELAN AUTHORITIES. JUDGE ESTABA TOLD NEWSMEN ON NOVEMBER 2, 1976, THAT THE COURT HAD SUFFICIENT EVIDENCE TO PROSECUTE.

SUSPECTS HERMES ROJAS PERALTA, OLEG GUETON RODRIGUEZ, WILLIAM WOLFE FIGUEREDO AND FRANCISCO NUNEZ VALLEJO HAVE BEEN RELEASED CONDITIONALLY, PENDING FURTHER INVESTIGATION. GOLFREDO MANCINI PEREZ AND CELSA MARY TOLEDO ALEMAN WERE ABSOLVED COMPLETELY AND HAVE BEEN RELEASED UNCONDITIONALLY.

RECEIVED

MMO859 0242206

FEDERAL BUREAU OF INVESTIGATION
COMMUNICATIONS SECTION

JAN 24 1977

TELETYPE

PP HI NK NY

DE MM

P 242206Z JAN 77

FM MIAMI (2-471) P

TO DIRECTOR (105-304390) PRIORITY

SAN JUAN (2-63) (VIA WASHINGTON) PRIORITY

NEWARK PRIORITY

NEW YORK PRIORITY

BT

S E C R E T

(Main ed. info. from 105-285035)

WM

B: O/H/W MAYANA CUBA, MARIANO, CUBA
SOC. SEC. # 163-86-2900 ALIEN REG. # A25014897
RESIDED 5 W. 1ST. AVE. MIAMI, FLA.

LOC: ELA: FOREIGN

FRANCISCO E. NUNEZ;
SYLA GUERVO;
EULALIO FRANCISCO CASTRO DIAZ, aka
FRANK CASTRO

NEUTRALITY MATTERS - CUBA (ANTI CASTRO);
FOREIGN AGENTS REGISTRATION ACT;
EXPLOSIVE AND INCENDIARY DEVICES
OO: MM 99-549

DECLASSIFIED ON 2-23-00 BY SP1CLK/gac

COORDINATION OF UNITED REVOLUTIONARY ORGANIZATIONS (CORU), NEUTRALITY MATTERS - CUBA, ANTI-CASTRO.

CORU IS AN ORGANIZATION COMPOSED OF FIVE ANTI-CASTRO TERRORIST ORGANIZATIONS HEADED BY DR. ORLANDO BOSCH WHO IS INCARCERATED IN CARACAS, VENEZUELA.

ON JANUARY 21, 1977, A CONFIDENTIAL SOURCE WHO HAS FURNISHED RELIABLE INFORMATION IN THE PAST ADVISED AS FOLLOWS:

FRANCISCO E. NUNEZ, CARACAS, VENEZUELA, CONSIDERED A TOP ECHELON MEMBER OF CORU, IS PRESENTLY IN MIAMI. NUNEZ HAS

Assoc. Dir.
Dep. AD Adm.
Dep. AD Inv.
Asst. Dir.:
Adm. Serv.
Ext. Affairs
Fin. & Pers.
Gen. Inv.
Ident.
Intell.
Legal Coun.
Plan. & Insp.
Rec. Mgt.
S. & T. Serv.
Spec. Inv.
Training
Telephone Rm.
Director's Sec'y

ORIGINAL FILED IN 105-304390-199

FEB 15 1977

REC-108

DE-15

SEP 1 - 1977

0003993

NR-2268-1

PAGE TWO MM 2-471 S E C R E T

STATED THAT HE IS COOPERATING WITH ORLANDO GARCIA VAZQUEZ, CHIEF OF DISIP IN CARACAS, VENEZUELA. HE CONFIDED THAT HE WAS IN MIAMI CARRYING OUT INSTRUCTIONS FOR THE "PEOPLE IN VENEZUELA". (SOURCE CONCLUDED THAT HE MEANT GARCIA VAZQUEZ). NUNEZ HAS STATED THAT THE "PEOPLE IN VENEZUELA" WANT TWO IMMEDIATE MISSIONS CARRIED OUT FROM MIAMI. ONE SHOULD BE A DRAMATIC MISSION THAT WOULD CAUSE MAXIMUM PUBLICITY AND THE OTHER WOULD BE LESS DRAMATIC, BUT ENOUGH TO KEEP THE PUBLICITY GOING. THE DRAMATIC MISSION SHOULD BE A NAVAL OPERATION AGAINST CUBAN SHIPPING ENTERPRISES, WHICH SHOULD RESULT IN A MAXIMUM NUMBER OF CUBAN NATIONALS KILLED. THE LESS DRAMATIC ACTION SHOULD BE A BOMBING OF A CONSULATE, EMBASSY, OR THE LIKE OF ANY COUNTRY HAVING RELATIONS WITH CUBA. THE LATTER SHOULD CAUSE NO INJURIES. NUNEZ ADVISED THAT THE MISSIONS WOULD TAKE AWAY THE "PRESSURE" FROM ORLANDO BOSCH AND SPECIFICALLY FROM THE REPUBLIC OF VENEZUELA. THE VENEZUELANS WERE INTERESTED IN PROSECUTING LUIS POSADA CARRILES TO THE

PAGE THREE MM 2-471 S E C R E T

FULLEST. HOWEVER, A VERY SERIOUS PROBLEM WAS ARISING IN THAT THE WIFE OF HERNAN RICARDO WAS DESTITUTE AND NO ONE WAS FINANCIALLY HELPING HER. THIS COULD CAUSE RICARDO TO START TALKING INVOLVING OTHERS IN THE BOMBING OF THE CUBANA AIRLINES ON OCTOBER 6, 1976 IN WHICH 73 PEOPLE PERISHED.

CLASSIFIED BY 7129, XGDS, 2&3, INDEFINITE - NO FOREIGN DISSEMINATION.

ADMINISTRATIVE

B THE CONFIDENTIAL SOURCE IS [redacted]

THE FOLLOWING IS A COMPLETE DEBRIEFING OF THE SOURCE ON JANUARY 21, 1977:

B [redacted] FRANCISCO E. NUNEZ, CARACAS, VENEZUELA, A TOP ECHELON MEMBER OF CORU IN VENEZUELA. NUNEZ [redacted] ALL AS A RESULT OF EVENTS IN VENEZUELA AFTER THE OCTOBER 6, 1976 CUBANA AIRLINES

PAGE FOUR MM 2-471 SECRET

CRASH. A FANTASTIC AMOUNT OF PRESSURE AND POLICE HARASSMENT HAS CAUSED HIM AND HIS FAMILY TO INCUR PROBLEMS THAT HE HAD NOT PREVIOUSLY ANTICIPATED. NUNEZ [redacted]

B [redacted] HE CONFIDED THAT HE IS A COOPERATING SOURCE FOR ORLANDO GARCIA VAZQUEZ, DISIP CHIEF IN CARACAS, VENEZUELA. NUNEZ CONFIDED THAT HE WAS IN MIAMI CARRYING OUT INSTRUCTIONS FOR THE "PEOPLE IN VENEZUELA", (SOURCE CONCLUDES THAT HE MEANT ORLANDO GARCIA VAZQUEZ), AND IN RETURN FOR THESE ACTS HE WAS GOING TO REMOVE HIMSELF FROM ANY FURTHER ANTI-CASTRO ACTIVITIES. HE SAID HE SPENT TOO MUCH MONEY ALREADY IN ADDITION TO DEVELOPING HEALTH PROBLEMS.

B NUNEZ [redacted] THAT THE "PEOPLE IN VENEZUELA" WANT TWO IMMEDIATE MISSIONS FROM MIAMI. ONE SHOULD BE VERY DRAMATIC THAT WOULD CAUSE MAXIMUM PUBLICITY, AND ONE NOT

B AS DRAMATIC, BUT THAT WOULD KEEP PUBLICITY GOING. [redacted]

PAGE FIVE MM 2-471 S E C R E T

[redacted] WHICH SHOULD BE A NAVAL ATTACK ON CUBAN SHIPPING IN WHICH A MAXIMUM NUMBER OF REPUBLIC OF CUBA PERSONNEL SHOULD BE KILLED. THE LESSER MISSION WOULD BE AN ESTABLISHMENT BOMBING SUCH AS A CONSULATE, EMBASSY, OR THE LIKE OF ANY COUNTRY HAVING RELATIONS WITH CUBA. NUNEZ WENT ON TO SAY THAT FUNDS WERE AVAILABLE AND THE MISSIONS SHOULD BE CARRIED OUT VERY SOON. IN ADDITION, NUNEZ HAD INSTRUCTIONS TO IMMEDIATELY LOCATE FRANK CASTRO WHO COULD CARRY OUT THE LESS DRAMATIC MISSION.

B [redacted] THAT THE MISSIONS WOULD TAKE AWAY THE PRESSURE FROM DR. ORLANDO BOSCH AND SPECIFICALLY FROM VENEZUELA. THE VENEZUELANS WERE INTERESTED IN PROSECUTING LUIS POSADA CARRILES TO THE FULLEST AND THAT DR. ORLANDO BOSCH MAY BE ABLE TO EXTRICATE HIMSELF FROM PROSECUTION. HOWEVER, A VERY SERIOUS PROBLEM WAS ARISING IN THAT THE WIFE OF HERNAN RICARDO WAS DESTITUTE AND NO ONE WAS FINANCIALLY HELPING HER. RICARDO COULD START TALKING INVOLVING OTHERS IN THE CUBANA AIRLINES INCIDENT. NUNEZ EXPRESSED DISAPPOINTMENT

PAGE SIX MM 2-47I S E K R E T

WITH DR. BOSCH IN THAT HE FEELS THAT BOSCH HAD ACTED IN VERY BAD FAITH CONCERNING THE CUBANA AIRLINES BOMBING. THE PLANE WAS TO HAVE BEEN SABOTAGED ON THE GROUND AND NOT IN THE AIR. HE DID NOT ELABORATE FURTHER ON THIS.

B [redacted] NUNEZ THAT HE COULD TELL THE "PEOPLE IN VENEZUELA" [redacted] ANY NAVAL OPERATIONS AGAINST CUBA IN BEHALF OF DR. ORLANDO BOSCH OR FOR THE BENEFIT OF THE VENEZUELAN GOVERNMENT.

NUNEZ ADVISED ALSO THAT RICARDO MORALES NAVARRETE HAS BEEN REPLACED IN DISIP BY MARIO JIMENEZ ROJO, ANOTHER CUBAN EXILE LIVING IN VENEZUELA. NUNEZ ALSO ADVISED THAT HE HAD DELIVERED AN AMOUNT OF MONEY TO SYLA CUERVO, OWNER OF STANDARD SERVICE STATION, 5688 W. FLAGLER STREET, MIAMI, FLORIDA. SOURCE ADVISED THAT CUERVO IS AN ANTI-CASTRO ACTIVIST.

THE BUREAU IS REQUESTED TO ADVISE INTERESTED AGENCIES.

PAGE SEVEN MM 2-471 S E C R E T

AND ALSO TO FURNISH THE SOURCE'S FULL DEBRIEFING TO LEGATS, CARACAS, MEXICO CITY, AND BUENOS AIRES.

MIAMI WILL CONTINUE CONTACTS WITH SOURCE FOR ANY FURTHER DEVELOPMENTS, AND ALL INTERESTED OFFICES WILL BE PROMPTLY ADVISED.

BT

#

HOLD

UNITED STATES DEPARTMENT OF JUSTICE

FEDERAL BUREAU OF INVESTIGATION

In Reply, Please Refer to File No.

Miami, Florida

2-471

August 16, 1978

DECLASSIFIED BY 5668/SLO/JC ON 8/491 86-0132

~~CONFIDENTIAL~~

COORDINACION DE ORGANIZACIONES REVOLUCIONARIAS UNIDAS
(COORDINATION OF UNITED REVOLUTIONARY ORGANIZATIONS)
(CORU)
NEUTRALITY MATTERS - CUBA (ANTI-CASTRO)

Classified by
Declassify on: OADR

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

Coordinacion de Organizaciones Revolucionarias Unidas (Coordination of United Revolutionary Organizations) (CORU) is an anti-Castro terrorist umbrella organization integrated by 5 anti-Castro groups which united in the Dominican Republic on June 11,1976, under the leadership of Dr. ORLANDO BOSCH. The 5 anti-Castro terrorist groups represented at the June 11, 1976 meeting were Accion Cubana, Cuban Nationalist Movement, Cuban National Liberation Front, Association of the Veterans of the Bay of Pigs Brigade 2506 and the 17th of April Movement.

Accion Cubana is a group headed by ORLANDO BOSCH AVILA, a Cuban exile medical doctor previously tried and acquitted in Federal Court, Miami, on extortion charges. In 1968, he was convicted in a Federal Court for ship bombings and sentenced to 10 years imprisonment and paroled in December, 1972. In June, 1974, BOSCH admitted having sent package bombs to Cuban Embassies in Lima, Peru, Madrid, Spain, Ottawa, Canada, and Buenos Aires, Argentina. BOSCH is presently in jail in Caracas, Venezuela, held in connection with an investigation by that government of the October 6, 1976 bombing of a Cubana Airlines plane wherein 73 persons were killed.

Classified by
Declassify on: OADR

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE.

Sources whose identities are concealed herein have furnished reliable information in the past except where otherwise noted.

~~CONFIDENTIAL~~
Classified by 6034
Exempt from GDS, Category 2
Date of Declassification: Indefinite

105-304390-5741

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

ENCLOSURE

0002935

SECRET

RE: CORU

~~CONFIDENTIAL~~

The Cuban Nationalist Movement is a right wing organization which claimed credit for acts of violence in the United States and Canada during the mid-1960s.

Cuban National Liberation Front is a Cuban exile terrorist organization which was formed on October, 1973, when several leaders from different groups participated in a sea attack against a Government of Cuba fishing boat. FLNC has claimed credit for about 25 acts of terrorism.

Association of the Veterans of the Bay of Pigs Brigade 2506 is comprised of participants in the Bay of Pigs invasion of Cuba in 1961. The organization has approximately 1,500 members, most of whom are inactive.

The 17th of April Movement is an off-shoot of Brigade 2506 which is presently inactive.

On May 5, 1977, MM T-1, who has furnished reliable information in the past, advised as follows: b)(u)

There has been a lot of talk among the Cuban exiles who are associated with CORU concerning missions, by Cuban exiles, against Cuba and/or countries maintaining trade relations with Cuba. These Cuban exiles have noted that in 17 years of attemptin to topple FIDEL CASTRO from power in Cuba, with various types of missions, they have all been unsuccessful in weakening CASTRO's hold on Cuba. In addition, financial support for the Cuban exiles has become a problem. This has been brought about by a concern among the Cuban exile community that to contribute to terrorist groups will automatically associate them with terrorism in the eyes of law enforcement agencies.

Some of the Cuban exile activists that have actually carried out missions have temporarily stopped operations in order to re-examine their capability, penetration of activist groups by law enforcement, and resources. This is in addition

~~CONFIDENTIAL~~

SECRET

SECRET

RE: CORU ~~CONFIDENTIAL~~

to the posture of the United States towards normalization of relations with communist Cuba, which may give Cuban exiles an opportunity to carry out missions against CASTRO from within Cuba. Some Cuban exiles feel that this may provide a more successful method of bringing down the FIDEL CASTRO communist regime in Cuba.

On May 5, 1977, MM T-2, who has furnished reliable information in the past, advised as follows: (U)

Cuban exiles within CORU have been having serious discussions on what course of action to take in their struggle to bring about the downfall of FIDEL CASTRO from power in Cuba. The source believes that the desire to free Cuba from communism has not diminished, but that the Cuban exiles are taking a new look at the new U.S.-Cuba position. Some of the Cuban exiles are openly talking about taking destructive actions within Cuba itself. They are also talking about having the opportunity, in the near future, of carrying out missions against FIDEL CASTRO's government in a more direct way such as Cuban freight ships which may dock in U.S. ports. (U)

On May 13, 1977, MM T-3, who has furnished reliable information in the past, advised as follows: (U)

On May 11, 1977, members of the Coordination of United Revolutionary Organizations (CORU) reportedly met at ORLANDO "BEBO" ACOSTA's sporting goods store, Casa de Los Deportes, Miami, Florida. FRANK CASTRO stated to those present that new operational cells must be formed by CORU to carry forward the anti-Castro fight. He noted that the CORU would be coming out with a press release in the very near future making the United States and Cuba responsible for any anti-Castro action carried out by CORU. He said that this was due to the United States provoking the Cuban exile community by opening avenues of economic benefit to Cuba, such as strong congressional moves to ease trade and tourist travel restrictions.

FRANK CASTRO stated that intelligence was presently being gathered in Merida, Yucatan, Mexico, the intermediate point of a proposed tourist flight route between the United

~~CONFIDENTIAL~~ SECRET

SECRET

RE: CORU

~~CONFIDENTIAL~~

States and Havana. He stated that the flight would be a Mexican airliner from the United States to Merida to Havana. He stated that this aircraft must be sabotaged to cause fear for anyone attempting to travel to Cuba as a tourist. FRANK CASTRO stressed that for the present CORU will prohibit any act or mission within the United States and Puerto Rico. He was very emphatic in stating that all operations must be outside of the boundaries of the United States.

Fla Cuba

On May 12, 1977, FRANK CASTRO allegedly indicated that the Cuban Nationalists Movement was being reintegrated into CORU, but without FELIPE RIVERO DIAZ. He stated that Brigade 2506 would be reintegrated into CORU by Wednesday, May 18, 1977.

On August 2, 1977, MM T-4 advised CORU recently had a meeting in Miami at ROIG Military Academy on 7th Street, wherein the following people attended: (U)

Fla Cuba

GASPAR JIMENEZ, JOSE GOLMENARES, TONY CALATAYUD, and other members of CORU.

The purpose of the meeting was to raise funds to send to Mexico for a jail break attempt for ORESTES RUIZ.

Up to this point money has been collected through a campaign headed by Dr. MODESTO MORA, MARTIANO ORTA, and JOAQUIN FONTANA. These people are all Cuban exile medical doctors. $1,000 has been raised by them and sent to the Dominican Republic to FRANK CASTRO to be later used in the proposed jail break.

On August 23, 1977, MM T-3 advised that Dr. AURELIO ECHEZARRETA and other CORU members recently went to see the president of Venezuela to obtain the release of Dr. ORLANDO BOSCH from civilian tribunals to the Military Court which "effectively" leaves BOSCH without defense in that normal legal procedures do not apply to the military. (U)

Cuba Fla

Dr. BOSCH wants war declared against Venezuela and wants CORU to make all Venezuelan interests its targets.

~~CONFIDENTIAL~~

SECRET

SECRET

RE: CORU

CONFIDENTIAL

MM T-3 advised that a person named "PEPE", a friend of GUSTAVO VILLOLDO, very high ranking CORU member, visits Dr. ORLANDO BOSCH regularly and brings instructions from BOSCH to FRANK CASTRO and other CORU elements in Miami. MM T-3 described "PEPE" as a white male, 5'6", 42-43 years old, brown eyes, short dark hair, medium to strong frame, no mustache.

On August 22, 1977, MM T-2 advised that "PEPE", friend of VILLOLDO, described above, is JOSE "PEPE" GOMEZ. GOMEZ has an import-export type business which involves Miami, Santo Domingo and Caracas. GOMEZ is also in the fishing and fish processing business from Santo Domingo to Caracas to Miami. Source does not know how extensive this business is.

MM T-2 advise that JOSE "PEPE" GOMEZ is a very close friend of ORLANDO BOSCH as well as many other Cuban exile activists in Miami and Caracas. "PEPE" does bring letters and messages from BOSCH to people in Miami and "PEPE" does visit with BOSCH often.

On September 30, 1977, MM T-5 advised reliable newspaper sources in Miami received direct information from Venezuela, giving the form, means and reasons why Dr. ORLANDO BOSCH went to Caracas on September 8, 1976. The following is a summary of this information:

In August, 1976, Dr. ORLANDO BOSCH passed through Maiquetias Airport, Caracas, coming from Curacao, enroute Chile. At the airport he was interviewed by a commission from the Venezuelan Government.

Once in Chile, Dr. ORLANDO BOSCH worked with JOSE "PEPE" FIGUERES FERRAR, ex-president of Costa Rica, and FIGUERES got him a false passport under the name of HECTOR EMILIO BALANGO. Using this passport, Dr. BOSCH went from Chile to Costa Rica.

For unknown reasons, the Costa Rican Government arrested Dr. ORLANDO BOSCH, and later, they agreed to set him free, on the condition that he leave the country. For this purpose, he was given another false passport in the name of LUIS PANIAGUA.

CONFIDENTIAL

SECRET

0002939

SECRET

RE: CORU

~~CONFIDENTIAL~~

From Costa Rica, traveling under the name of LUIS PANIAGUA, Dr. ORLANDO BOSCH went to Santo Domingo, where he received a telephone call from Venezuela during which a government official requested him to come to Caracas, where they urgently needed to talk to him.

Dr. ORLANDO BOSCH went to Nicaragua, where he received two more calls from Venezuela, urging him to come to Caracas as soon as possible.

On September 8, 1976, Dr. ORLANDO BOSCH arrived at Maiquetias Airport, Caracas, where he was met at the airport by POSADA, ORLANDO GARCIA, and RICARDO MORALES NAVARRETE. All are members of the Presidential Police Security Organization in Venezuela.

That same night, all the above-mentioned men dined at La Hacienda Restaurant. Dr. ORLANDO BOSCH was staying at the Caracas Hilton, Room 12-S. At the same time, two Venezuelan government employees were staying in Rooms 8-N and 5-Q of the same hotel.

Under these circumstances, Dr. ORLANDO BOSCH, through these members of the Venezuelan government, received the following proposition:

he would receive adequate police protection in Venezuela

he would be provided with a weapon for his personal defense

he would be permitted to collect funds in Venezuela for the cause of Cuba

they would try to get him an interview on October 10, 1977, with a top level person in the Venezuelan government. (ORLANDO BOSCH later said the interview was to be with President CARLOS ANDRES PEREZ)

~~CONFIDENTIAL~~

SECRET

SECRET

RE: CORU

CONFIDENTIAL

In exchange for all this, Dr. ORLANDO BOSCH promised to stop terrorism by his group in Venezuela, Costa Rica and Colombia, but not Panama. They tried to include Panama among these countries, and they added to the list of countries which could be attacked the name of Guyana. (U)

After that, the Cubana plane was sabotaged, and seventy-some people were killed. Dr. BOSCH was arrested and charged with the crime. He is presently in the Carcel Modelo in Caracas. (U)

[On October 14, 1977, MM T-1] advised as follows: (U)

One of the individuals who took boats to be used by ARMANDO LOPEZ ESTRADA's group in a raid against Cuba advised that aforementioned group had planned an important operation in Washington, D.C., or New York. This operation was cancelled because of law enforcement pressure and due to the arrest of PEDRO GIL. CORU members feel that LOPEZ ESTRADA has made himself too visible, attracting too much law enforcement interest.

VEN Cuba FIA

LOPEZ ESTRADA was requested to explain his actions by a CORU committee. His answers were not adequate and some have concluded that he may be an informant. They know that someone within the inner circle of the cell has informed.

CORU has decided to maintain a low profile. They will not conduct any additional terrorist attacks in the near future.

E

[On November 7, 1977, MM T-6 advised that [redacted] are having very serious problems with Dr. ORLANDO BOSCH in Venezuela. BOSCH has been very arbitrary and demanding and continuously makes statements and issues conclusions on what at best is mere speculation, all of which has been most detrimental not only to BOSCH's cause and the other three jailed persons, but also to the anti-Castro exile community. In addition, the problem exists that if BOSCH is released in January, 1978, where could he go. The U.S. does not want him, the Dominican Republic does not want him, and Venezuela has to deport him. [redacted] admitted that this was quite a dilemma and was further complicated by BOSCH's inordinate declarations. (U)

E

SECRET

CONFIDENTIAL

SECRET

RE: CORU

~~CONFIDENTIAL~~

MM T-6 stated that the Cuban exiles have excellent conditions which are favorable to topple FIDEL CASTRO of Cuba. He stated that among the excellent conditions which are now evident are: (1) the Angola and African problem that CASTRO has which has resulted in deaths and capture of many Cubans has caused questioning within the Republic of Cuba as to why these Cubans are being sacrificed abroad; (2) Cuba's economy and sugar prices have deteriorated; (3) an apparent shifting posture of U.S. policy towards Cuba, and the fact that FIDEL CASTRO has been in power too long, which historically speaking is detrimental to any leader. He noted that new people with new ambitions come along who make use of and play on a population which has been promised bright futures and those promises have not been fulfilled.

On November 30, 1977, MM T-3 advised as follows:

FRANK CASTRO, the present leader of CORU, has become active again in reorganizing CORU. He is anticipating that Dr. ORLANDO BOSCH, the incarcerated head of CORU, will be released from jail in Caracas, Venezuela, in the very near future.

F/A Cuba

MM T-3 advised that FRANK CASTRO has received the backing of Dr. CRISTOBAL GONZALEZ MAYO, leader of a Miami Cuban exile confederation of professionals which calls itself "Confederacion de Profesionales Cubanos en el Exilio". Dr. GONZALEZ MAYO agreed to have his organization support CORU with money and political influence.

F/A Cuba

MM T-3 further reported that FRANK CASTRO has secured information regarding international commercial ship movement from TEOFILO BABUN, owner of Antillean Marine Shipping Corporation, Miami. This information shows when ships are in port, in the United States and abroad, when they are due to depart port, what their home port is, and the country to which they belong.

FRANK CASTRO has reportedly stated that CORU needs to plant magnetic type bombs on communist country ships in four different ports, and on simultaneous dates of departure. Further,

~~CONFIDENTIAL~~

SECRET

RE: CORU ~~CONFIDENTIAL~~

such devices should have 24 hour delay activators causing explosions well after the victim ship leaves port. This would increase chances for the destruction of any evidence.

MM T-3 stated that Dr. ORLANDO BOSCH is scheduled to be released in January, 1978. The source advised that he assumes that FRANK CASTRO would want the ship bombing operations to take place soon after the release in order to capitalize on an anticipated publicity momentum that BOSCH's release could cause. (U)

Cuban B. APPROX. 1935

MM T-3 advised on December 19, 1977, that Dr. CARLOS F. DOMINICIS is a dentist, age approximately 43, ~~white male~~, Cuban, 5'6", 180 pounds, dark complected, black hair, brown eyes, business address 4912 Bergenline Avenue, Room 15, West New York, New Jersey, 07093, telephone number 201-865-4177, residing possibly at 73 Ferry Street, Newark, New Jersey 07105, telephone 201-589-8222. Source advised that DOMINICIS is now the Secretary of CORU, North Zone, which includes Washington, D.C., Newark and New York City, and other cities north of Washington, D.C. DOMINICIS is the mail organizer for CORU in that area. DOMINICIS possesses a 40-foot power boat located in West New York near a river, which will be transported to Miami, Florida, in the near future to be utilized as a mother ship for various operations by CORU. The boat is to be transported via trailer from West New York to Miami. DOMINICIS was observed driving a two-door, 1977 Chrysler Cordova, further description unrecalled. DOMINICIS will travel from Newark, New Jersey, to Miami, Florida, on approximately December 25, 1977, via automobile and will meet with FRANK CASTRO and other individuals connected in anti-Castro activities in the Miami, Florida area. (U)

Farrel B. APPROX. 1933

MM T-3 advised that HARRY "the Cop" FARREL, white male, grey hair, fair complexion, approximately 45 years old, operates Farrel Dental Supply and was a formulator of the old "Plan Torriente". FARREL has been designated Treasurer of the CORU organization in the North Zone. (U)

DC
NY
NJ

~~CONFIDENTIAL~~

SECRET

RE: CORU

~~CONFIDENTIAL~~

~~B. APPROX.~~

MM T-3 advised that JOSE TEXEIRO, white male, Cuban, newspaperman, has been designated as CORU's Propaganda Chief in the North Zone.

B. APPROX. 1938

"El Chino" ESQUIVEL, white male, Cuban, age approximately 40, was selected by CORU to form military cells for various activities. ESQUIVEL, with the CORU North Zone, is to report directly to FRANCISCO "FRANK" CASTRO, from Miami, Florida. ESQUIVEL will have two groups of cells, one group to engage in activities and operations in the North American Continent, while the second group of cells will operate outside the U.S. on a world-wide basis.

On December 30, 1977, MM T-2, who has furnished reliable information in the past, advised as follows:

On December 29, 1977, FRANK CASTRO flew to Freeport, Bahamas, aboard his Aerocommander aircraft. With him were the following: (1) PORFIRIO BONET, co-owner with FRANK CASTRO of Bonet Travel Agency, Miami; (2) RAFAEL VILLAVERDE, Director, Little Havana Community Center, Miami; (3) LILIA ESTEVEZ, girlfriend of VILLAVERDE, date of birth April 14, 1953, employed at Little Havana Community Center, Miami; (4) MARTHA MASSON, date of birth January 5, 1949, resides 971 West Flagler, Miami, Immigration and Naturalization Service (INS) Number A12 539 609, reported by MM T-2 as being the secretary to ROBERTO CARBALLO, present President of Brigade 2506, in a new business venture that CARBALLO is in which involves exports and imports of unknown products.

MM T-2 advised that FRANK CASTRO confided that he did not place any of the three bombs (referring to the bombings of Venezuelan establishments in Miami, New York and the placing of a device in San Juan). He stated that he was now stopping the bombings. He stated that it was now up to Venezuela to negotiate the release of Dr. ORLANDO BOSCH and LUIS POSADA CARRILES, also known as "Bambi". He stated that the Venezuelans wanted him (FRANK CASTRO) to meet with a General GARCIA in Caracas, Venezuela, on or about January 5, 1978. FRANK CASTRO

~~CONFIDENTIAL~~

SECRET

SECRET

RE: CORU

~~CONFIDENTIAL~~

stated that he would not go, but would probably send RAFAEL VILLAVERDE. However, the go-between is RICARDO MORALES NAVARRETE and he and VILLAVERDE had a very serious falling out and do not speak to each other. (U)

MM T-2 further advised that FRANK CASTRO appears very pleased and strongly believes that Venezuela will react in a positive way to releasing BOSCH and CARRILES. He confided that he considers the release of CARRILES as more important than BOSCH's release. He feels that BOSCH's ability to collect large amounts of money is no longer of primary importance in that new funding has been established. (U)

On December 31, 1977, MM T-3 advised that FRANK CASTRO had advised ORLANDO "BEBO" ACOSTA, REINOL RODRIGUEZ, of Puerto Rico, RAUL CABRERA, and others that RICARDO MORALES NAVARRETE, reportedly, was trying to obtain explosive materials to retaliate against those he suspects of being responsible for the recent December, 1977, violent actions taken against Venezuelan interests. RICARDO MORALES NAVARRETE is presently in Miami, Florida. (U)

On January 10, 1978, MM T-4 advised that a young action oriented cell under the control of FRANCISCO "FRANK" CASTRO of the CORU organization were responsible for the bombing incident that occurred at Viasa Airlines, Miami Beach, Florida, on December 23, 1977. The young CORU cell is made up of ALVIN ROSS DIAZ and RACIEL RODRIGUEZ. Source advised that DIAZ and RODRIGUEZ along with CASTRO have met in the restaurant called Cordova located in the Portofino Shopping Center at 87th Avenue, S.W. 8th Street, Miami, Florida. Source advised that MARIA EUGENIA VIDANA (sister of ANGELINA VIDANA) and MONO MORALES are allegedly connected with RODRIGUEZ and DIAZ. (U)

Cuba

On January 13, 1978, MM T-4 advised that ALFREDO MENOCAL was currently in Union City, New Jersey, along with GUILLERMO NOVO SAMPOL and FELIX EGUES and attempting to organize action cells for the organization CORU. MENOCAL, NOVO and (U)

~~CONFIDENTIAL~~

SECRET

0002945

SECRET

RE: CORU ~~CONFIDENTIAL~~

EGUES are organizing the cells for military action in the U.S. and against the country of Venezuela in view of their desire to have ORLANDO BOSCH released.

In connection with the organizing of cells, ALFREDO MENOCAL, FRANK CASTRO, ORLANDO ATIENZA, RAFAEL RODRIGUEZ, RAMON RODRIGUEZ, and GUILLERMO NOVO-SAMPOL are organizing a trip to the State of California in order to organize these cells.

In connection with the above activity, CORU will set up front organizations in various areas of the U.S. and secret cells will be formed within the front organizations and the cells will carry out military actions desired by CORU. Source advised that the following front organizations are being set up:

Organizaciones Revolucionarias de Puerto Rico in San Juan, Puerto Rico; Asemblea Coordinadora de la Dignidad in the area of Miami, Florida; Federacion de Organizaciones Cubanas de Illinois (F.O.C.I.) located in Chicago, Illinois; Bloque de Organizaciones Revolucionarias Cubanas de New York, New Jersey (North Zone).

Source reiterated that individual charged with organizing secret cells with the above front organizations is ALFREDO MENOCAL.

Source advised that Dr. ANGEL ALVAREZ currently employed as an attorney by the City of Miami, Miami, Florida, and a close friend of RAFAEL VILLAVERDE is engaged in financing activities for the CORU organization.

Source advised that CORU will continue attempts to organize secret cells in the Miami, Florida area, Chicago, Illinois, San Juan, Puerto Rico, as well as the states of New York, New Jersey, California and Texas.

On January 25, 1978, MM T-3 advised that FRANCISCO "FRANK" CASTRO had called an emergency meeting attended by CASTRO,

~~CONFIDENTIAL~~ SECRET

SECRET

RE: CORU

~~CONFIDENTIAL~~

ORLANDO "BEBO" ACOSTA and others, at the Cordoba Restaurant, Miami, Florida. FRANK CASTRO appeared agitated and distressed regarding the arrest on January 23, 1978, of GASPAR JIMENEZ and GUSTAVO CASTILLO, on extradition warrants for extradition to Mexico. (CASTRO advised that HUMBERTO LOPEZ, SR., and LUIS CRESPO would be attending an annual dinner held at the Club Martiana in San Juan, Puerto Rico. The dinner would be held on January 28, 1978, to celebrate the "Seneca Martiana".) CASTRO advised that he could not permit JIMENEZ and CASTILLO to be extradited to Mexico due to fears that JIMENEZ and CASTILLO might be extradited from Mexico to the country of Cuba. CASTRO said that the Federal Government of Mexico had previously unofficially promised not to extradite GASPAR JIMENEZ and GUSTAVO CASTILLO through a Cuban source in Mexico City, Mexico. CASTRO advised that upon return of LOPEZ, CRESPO and other Cubans, from San Juan the next week, he (CASTRO) will give an all out "green light" to all terrorist organizations and individuals to attack Mexican property and government officials to include Mexican Embassies and AeroMexico Airlines everywhere. Source advised that on the evening of January 24, 1978, a committee was established to aid JIMENEZ and CASTILLO. ANTONIO MUNIZ was established as head of the committee called "Comite Por Derechos Humanos" (Committee for Human Rights). CASTRO advised that one of the purposes of the violence is to hurt the Mexican tourism trade and force Mexico to withdraw extradition of CASTILLO and JIMENEZ.

On April 18, 1978, MM T-3 advised that a meeting (U) is being proposed to occur in the near future, possibly the weekend of April 22, through April 24, 1978, to occur at Sarasota, Florida. The meeting will be attended by the following CORU individuals: Bahamas CA

Cuba VEN FIA

FRANK CASTRO, CORU Chief from Miami, Florida;
REINOL RODRIGUEZ, CORU Chief from San Juan, Puerto Rico;
SECUNDINO CARRERAS, Assistant CORU Chief, San Juan, Puerto Rico;
ORLANDO "BEBO" ACOSTA, CORU, Miami, Florida; Orlando Acosta
SIXTO ARCE, CORU, Miami, Florida;
ANTONIO "TONY" MUNIZ, CORU, Miami, Florida; Antonio Muniz
RAFAEL PEREZ ORESTE, CORU, Miami, Florida;
ROGELIO LOPEZ AVALO, CORU, Miami, Florida

~~CONFIDENTIAL~~

SECRET

0002947

SECRET

RE: CORU ~~CONFIDENTIAL~~

Source advised that ROGELIO LOPEZ AVALO was placed in charge of security and is responsible for obtaining lodging for the above individuals. It is also proposed that the above people arrived in Sarasota, Florida, at different times and different dates before the meeting. Source advised that CORU will discuss the following subjects at the meeting:

(1) Current conflict between FRANK CASTRO and LUIS CRESPO (CORU, Miami, Florida), and proposals to settle current differences. (2) Will discuss CORU membership including active organizations within CORU. (3) Will discuss future military strategy. (4) Will discuss plans or possibilities of a future conference to be attended by two delegates from all anti-Castro organizations throughout the U.S.

[MM T-3 advised that] on Monday, April 17, 1978, Dr. CARLOS F. DOMINICIS, CORU leader in the New York area, had arrived in Miami, Florida, at approximately 3 A.M. and had furnished $1,100 in cash to ORLANDO "BEBO" ACOSTA to finance military action. DOMINICIS had previously mailed ACOSTA $1,000 in cash, which ACOSTA received on April 13, 1978. Source advised that DOMINICIS advised that he had attended a conference in Chicago sponsored by the Federacion de Organizaciones Cubanas de Illinois (FOCI). DOMINICIS advised that approximately 12 days prior, DOMINICIS had been approached by one Korean and one Spanish individual claiming to be delegates of Reverend Moon and had offered financial aid to FOCI and its anti-Castro activity. DOMINICIS advised that he had discussed the financial aid being offered by Reverend Moon with FRANK CASTRO and ORLANDO ACOSTA and DOMINICIS was told by CASTRO and ACOSTA to go ahead and receive financial aid offered by the delegates of Reverend Moon. DOMINICIS advised that CORU is being proposed as the possible military arm of FOCI.

[MM T-3 advised on May 23, 1978, that] JUAN PEREZ FRANCO of the Brigade 2506 and NESTOR IZQUIERDO, Brigade 2506, said that the Brigade reportedly will be integrated into the CORU in the near future. FRANCO will be the Brigade's delegate to CORU while IZQUIERDO will be the Military Chief. Source advised that the Brigade 2506 has been discussing the possibility of

~~CONFIDENTIAL~~ SECRET

SECRET

RE: CORU ~~CONFIDENTIAL~~

reactivating "Ejercito Secreto" under the leadership of RAMIRO DE LA FE. The Brigade 2506 is discussing possibility of reactivating "M-17" or will utilize "M-17" as a pseudonym to take credit for future military actions. Regarding pseudonyms, source advised that pseudonym "Omega Seven" has been utilized by CNM in the New York-New Jersey area in the past. The term "Omega Seven" was originated by JOSE TENRIERO and GUILLERMO NOVO. Pseudonym "ELAC" (Ejercito Latino Americano Anticommunista), was originated by REINOL RODRIGUEZ, CORU Chief of San Juan, Puerto Rico. Pseudonym of "Jovenes de Las Estrella" (Youth of the Star), has been utilized by SIXTO ARCE, CORU member from Miami, Florida. The pseudonym "Pedro Luis Boitel" was possibly originated by ANTONIO MUNIZ, CORU member from Miami, Florida, while the pseudonym "El Condor" was originated by FRANK CASTRO, CORU Chief from Miami, Florida.

MM T-3 advised that OSVALDO BENCOMO, CORU Military Chief in San Juan, Puerto Rico, allegedly admitted placing a bomb approximately six months ago at a Venezuelan tourist office, San Juan, Puerto Rico. BENCOMO did not furnish additional details concerning this situation other than it was connected with a bombing incident surrounding Venezuelan office in the New York City area at about the same time. BENCOMO reportedly is the man in charge of military actions for the CORU organization in Puerto Rico.

REINOL RODRIGUEZ, CORU Chief, San Juan, Puerto Rico, advised that he (REINOL RODRIGUEZ) in addition to being head of CORU in Puerto Rico, is also head of "El Bloque de Organizaciones" in Puerto Rico with "El Bloque" having strong affiliations in Chicago, Illinois, New York City, New York. RODRIGUEZ reportedly said that CORU is currently discussing the possibilities of attacks on Cuban Consuls outside the United States, possibly utilizing silencer equipped handguns rather than bombs.

~~CONFIDENTIAL~~

SECRET

SECRET

RE: CORU ~~CONFIDENTIAL~~

On July 6, 1978, MM T-2, MM T-3 and MM T-8 advised as follows: (U)

On the evening of July 6, 1978, and at 152 N.W. 27th Avenue, Miami, the following CORU members and/or sympathizers are meeting: (U)

From New York/Newark: (U)

CARLOS DOMINICIS, ROGER HERNANDEZ, Attorney; HELADIO VALDEZ, ORESTES PEREZ, TOMAS DALMAU, JUAN ISIDRON, JULIO AMADOR, EDUARDO ESPINOSA, JOSE TENREIRO, PEDRO HERNANDEZ, ISRAEL ROMERO. (U)

From Miami: (U)

MIGUEL ISA, HUMBERTO LOPEZ, SR., JOSE YEBER, Dr. CRISTOBAL GONZALEZ MAYO, Dr. MANUEL CAMPOS, DIEGO MEDINA, ARMANDO FLEITES. (U)

From San Juan, Puerto Rico: (U)

"Colonel" RAMON BARQUIN. (U)

The purpose of the meeting is to strengthen ties between the various Cuban activists in Miami, New York and Puerto Rico into a unified front. This, according to sources, should strengthen collections of funds and activities which may be programmed to further their aims. (U)

MM T-8 advised that the power structure of CORU sympathizers in the North Zone, also known as Bloque Cubano de Organizaciones Revolucionarias - Zona Norte (Cuban Block of Revolutionary Organizations - North Zone) are as follows: (U)

Dr. CASTULO FERAUD, President.
Dr. RAFAEL ALOMA SABAS, Secretary.
HELADIO VALDEZ, Secretary of Organizations.
BIENVENIDO CUETO, Treasurer.
CELEDONIO PUERTO, Press Secretary.
ISRAEL ROMERO, Public Relations Secretary.
Dr. CARLOS DOMINICIS.

~~CONFIDENTIAL~~

SECRET

SECRET

RE: CORU

~~CONFIDENTIAL~~

The sources advised that DOMINICIS and ISA have been collecting funds among the Cuban doctors and related professions in the Miami area. DOMINICIS, reportedly, just returned from Venezuela where he talked with Dr. ORLANDO BOSCH who told him that he had been advised he would be released from jail in December, 1978. (U)

MM T-8 and MM T-2 advised that the organizer of the July 6, 1978 meeting is ISRAEL ROMERO who is staying in Room 1706, Colonial Hotel, 100 block of Biscayne Boulevard, Miami. EDUARDO ESPINOSA is supposed to be sharing the room with ROMERO. The sources do not know as of this date whether the other Newark - New York people are staying in the Colonial Hotel also. (U)

On July 13, 1978, MM T-2 voluntarily furnished the following information: (S) U

Dr. CARLOS DOMINICIS, a member of the Cuban Nationalist Movement, is presently in Miami, Florida. He has recently returned from Caracas, Venezuela, where he talked to Dr. ORLANDO BOSCH. Dr. BOSCH, according to Dr. DOMINICIS, has elevated Dr. DOMINICIS to be the interim head of CORU. Dr. BOSCH is reportedly going to be released from jail by December, 1978. MM T-2 noted that the story concerning Dr. BOSCH's release has been around for some time. Dr. DOMINICIS has advised that Dr. BOSCH has ousted FRANK CASTRO from the CORU leadership. (S) U

MM T-2 advised that FRANK CASTRO is presently out of the United States. However, the source stated that he recently spoke with FRANK CASTRO and CASTRO is extremely upset at DOMINICIS' interlopement and has expressed incensement, particularly because this would cause a split in CORU and because he doubts Dr. DOMINICIS' worthiness as a CORU leader. (S) U

On July 17, 1978, MM T-2 advised that former CORU Chief, FRANK CASTRO had received information from the Dominican Republic Intelligence Services that the Cuban Government is trying to have FRANK CASTRO assassinated in the Miami, Florida area. (S) U

~~CONFIDENTIAL~~

SECRET

SECRET

RE: CORU

~~CONFIDENTIAL~~

MM T-2 advised that a relative of FRANK CASTRO is a former high-ranking officer in the Dominican Republic Navy and that possibly through this relative, CASTRO may have found out about the assassination plans. (S) (U)

On July 6, 1978, MM T-8 advised that Dr. CARLOS DOMINICIS, a New Jersey Dentist, is presently in the Miami, Florida area where he is making an effort to collect money from Cuban Medical Doctors. The money will be used by CORU to finance its activities. (S) (U)

Source further advised that several CORU members met on July 6, 1978, at 152 N.W. 27th Avenue, Miami, Florida. Among those attending the meeting were the following: (S) (U)

Dr. CARLOS DOMINICIS
Dr. ROGER HERNANDEZ
ELADIO VALDES
ORESTES PEREZ
TOMAS DALMAU
JESUS ISIDRON
JULIO AMADOR
EDUARDO ESPINOSA
JOSE TENREIRO
PEDRO HERNANDEZ
ISRAEL ROMERO

(S) (U)

Several other persons are expected to attend further meetings at the same location in the next few days. Among those expected to attend are MIGUEL ISA, HUMBERTO LOPEZ, SR., JOSE YEBER, Dr. CRISTOBAL GONZALEZ MAYO, aka Mayito, Dr. MANUEL CAMPOS. (S) (U)

The source also furnished the following list of CORU directors for the Northern section of the United States:

~~CONFIDENTIAL~~

SECRET

SECRET

RE: CORU

~~CONFIDENTIAL~~

President - Dr. CASTULO FERAUD
Vice President - Dr. RAFAEL ALOMA SABAS
Secretary - ELADIO VALDES
Organizational Secretary - BIENVENIDO CUETO
Treasurer - CELEDONIO PUERTO
Press Secretary - ISRAEL ROMERO
Public Relations Chairman - Dr. CARLOS DOMINICIS

MM T-8, on July 11, 1978, advised that on July 10, 1978, a CORU meeting took place at 152 N.W. 27th Avenue, Miami, Florida, with the following persons in attendance: (U)

At this last meeting the topic discussed was the plans for a meeting of CORU members from all over the U.S. and also representatives of other anti-CASTRO organizations, which will take place sometime during the month of September, 1978, in Miami. (U)

On July 11, 1978, source further advised that Dr. ORLANDO BOSCH is expected to be released from prison in Venezuela sometime in December, 1978. BOSCH is expected to remain in Venezuela after his release from prison. (U)

~~CONFIDENTIAL~~

SECRET

R 0 0 074

UNION NICARAGUENSE OPOSITORA
(U.N.O)

2 Septiembre 86.

DISTRIBUCION EN GENERAL DE MATERIAL EN BODEGA DE:

12 Julio 86.

18,000 Cartuchos 7.62x51.
28,000 Cartuchos 7.62x39.
504 Granadas de 40mm para M-79.
130 Gorras Militares.
130 Uniformes Camuflados USA.
130 Fajas con Hebillas.
130 Pares de Botas de Jungla USA.
260 Pares de Medias Militares.
130 Suspensores de Cinturon.
130 Cinturones 1911.
260 Camisetas.
260 Calzoncillos.
130 Mochilas de Jungla.
130 Ponchos Lynar.
130 Ponchos de Lluvia.
130 Cantimploras con sus fundas.
130 Pañuelos Camuflados.
260 Portamagasines M-16.
130 Pocos de Mano tipo Militar.
130 Pares de Baterias para foco de mano.

Material enviado a Fuerzas del Frente Sur.O/Max Gómez

15 Julio 86

3 Uniformes Camuflados USA.
2 Suspensores de Cinturon.

Material tomado de Bodega, para apoyar a 3 Soldados coolaboradores nuestros. O/Ramón Medina.

18 Agosto 86

2,400 Granadas de Mano M-963.

Material enviado a Bodegas del Aguacate, para uso del Frente Norte FDN.O/Bill Cooper.

29 Agosto 86.

1 Par de Botas de Jungla USA.

Material tomado de Bodega, para apoyar a un mecánico coolaborador nuestro. O/Max Gómez.

1ro Septiembre 86

925 Granadas de Mortero 60mm.

Material tomado de Bodega y enviado a Bodegas del Aguacate para uso del Frente Norte FDN.O/Rafaél Quint

2 Septiembre 86.

1 Par de Botas de Jungla USA.

Material tomado de Bodega por Bill Cooper para su uso

Armando Lopez L.
COMANDANTE L-26.

TRANSLATION FOLLOWS

CRS - 5

R 0 00165
Translation of
R C C 074

NICARAGUAN OPPOSITION UNION (UNO)

September 2, 1986

GENERAL DISTRIBUTION OF MATERIAL IN DEPOT ON:

July 12, 1986

18,000 (7.62 x 51) cartridges
28,000 (7.62 x 39) cartridges
504 40-mm grenades for M-79
130 service caps
130 U.S. camouflage uniforms
130 belts with buckles
130 pairs of U.S. jungle boots
260 pairs of military socks
130 suspenders
130 1911 type belts
260 undershirts
260 shorts
130 jungle packs
130 lynar ponchos
130 rain ponchos
130 canteens with cases
130 camouflage kerchiefs
260 M-16 clips /?/
130 military-type flashlights
130 sets of batteries for flashlights

Material sent to Southern Front forces Or/Max Gomez

July 15, 1986

3 U.S. camouflage uniforms
2 suspenders

Material taken from depot to support 3 soldiers, collaborators of ours
Or/ Ramon Medina

August 18, 1986

2,400 M-963 hand grenades

Material sent to Aguacate depots for use by the FDN Northern Front
Or/ Bill Cooper

R 0 00166

August 29, 1986

1 pair of U.S. jungle boots

Material taken from depot to support a mechanic, collaborator of ours
Or/ Max Gomez

September 1, 1986

925 60-mm mortar shells

Material taken from depot and sent to Aguacate depots for use by the FDN
Northern Front Or/Rafael Quintero

September 2, 1986

1 pair of U.S. jungle boots

Material taken from depot by Bill Cooper for his use.

(s) Armando Lopez I.
Comandante L-26

RELEASED PER P.L-102-526(JFK ACT)
NARA ___ DATE 5/4/05

Reproduced at the National Archive

MESSAGE RELAY

10/1/76

Transmit in ☒ Code
Via Teletype the Attached ☐ Urgent ☐ Immediate ☐ Routine
☐ Priority ☐ Routine

From: Director, FBI

To: SAC Miami
SAC San Juan
Mexico City
Buenos Aires

To: RUEAWW ☐ The President ☐ The Vice President / Attn: ☐ White House Situation Room / Attn:
RUEBDAA ☐ Attorney General ☒ Deputy Attorney General ☒ Attn: Intelligence and Evaluation Unit
RUEBWAA ☐ Assistant Attorney General, Civil Rights Division
RUEBAAA ☒ Attn: Internal Security Section ☒ Attn: General Crimes Section
RUEANDA ☐ Drug Enforcement Administration
RUEBWAA ☒ Immigration and Naturalization Service
RUEBDAA ☐ Department of the Air Force (AFOSI)
RUEAGSI ☐ Department of the Army
RUEANIA ☒ Director, CIA
RUEDGAA ☒ Commandant, U.S. Coast Guard
RUEKJCS ☒ Director, Defense Intelligence Agency
RUEGCTN ☐ Director, Research and Development Division (Attention:)
RUEGCDA ☒ Federal Aviation Administration
RUEANSA ☐ National Security Agency
RUEBARE ☐ Naval Investigative Service
RUEGSSA ☐ Director, Defense Intelligence Agency
RUEAROVDBB Undersecretary
RUEHSD ☒ U.S. Secret Service (DIU)
RUEHC ☒ Secretary of State
RUEHGAA ☐ Department of Transportation Attn: Director, Security
RUEATRS ☒ Department of Justice
☒ Attn: Director
☐ Attn: Director, Criminal Division

Classified by Sobeloff 6/3/03
Declassify on: OADR

Classified by: Sobeloff
Declassify on: OADR

COMMUNICATIONS SECTION

OCT 03 1976
TELETYPE

[redacted]

1 OCT 19 1976

70 NOV 16 1976

SECRET

SECRET

FEDERAL BUREAU OF INVESTIGATION
COMMUNICATIONS SECTION
OCT 07 1976
TELETYPE

~~0 072345Z OCT 76~~
~~RL BARBADOS (2-0)~~
~~TO DIRECTOR IMMEDIATE NR 1GE PM~~
~~FM~~
~~S E C R E T~~

Cubana Airlines

INSUBJ: SUSPECTED BOMBING OF CUBANA AIRLINES DC-8 NEAR BARBADOS, WEST INDIES, OCTOBER 6, 1976, NM - CUBA - WEST INDIES.

BY TELETYPE 10/7/76, LEGAT CARACAS ADVISED AS FOLLOWS:

CUBANA AIRLINES FLIGHT 455, DC-8 AIRCRAFT LEASED BY CUBANA FROM AIR CANADA, CRASHED IN THE CARIBBEAN SEA OFF THE COAST OF BARBADOS AT ABOUT 1:45 PM ON OCTOBER 6, 1976, SHORTLY AFTER TAKEOFF FROM SEAWELL AIRPORT, BARBADOS, EN ROUTE TO HAVANA, CUBA, VIA KINGSTON, JAMAICA. NO SURVIVORS REPORTED AMONG THE 78 PERSONS ABOARD THE PLANE.

ACCORDING TO AMERICAN EMBASSY, BRIDGETOWN, BARBADOS, PILOT REPORTED TO SEAWELL AIRPORT TOWER SHORTLY BEFORE CRASH THAT AN EXPLOSION HAD OCCURRED ABOARD THE PLANE. FLIGHT LOG RECOVERED AFTER CRASH NOTED POWER FAILURE IN NUMBER FOUR ENGINE, BUT NO MENTION OF EXPLOSION. AIRPORT OFFICIAL AT BARBADOS REPORTEDLY INFORMED THAT PILOT TOLD TOWER THERE HAD BEEN EXPLOSION IN ONE OF THE REAR LAVATORIES OF THE PLANE.

STATE DEPT. INFO (PARA 2 - END) & LEGATS FILED PER DOS AUTHORITY 4/29/96.

AMERICAN EMBASSY, PORT OF SPAIN, TRINIDAD, ADVISED ON OCTOBER 7, 1976, AS FOLLOWS:

"TRINIDAD AND TOBAGO POLICE ARE HOLDING TWO VENEZUELAN

SECRET

~~END PAGE ONE~~

~~CARBON COPY DO NOT FILE~~

2

SECRET

~~END CAR C.R. S E C R E T~~

TIONS WHOM THEY BELIEVE MAY BE CONNECTED WITH THE CUBANA AIRLINE CRASH OCTOBER 6 OFF BARBADOS. TWO SUSPECTS ARE:

"A. JOSE VAZQUEZ GARCIA - HOLDER OF VENEZUELAN PASSPORT 720733 (THIS IS THE PERFERATED NUMBER--NUMBER WRITTEN IN THE PASSPORT IS 3140806), ISSUED ON JUNE 6, 1976, IN CARACAS. BORN DECEMBER 9, 1950 IN CARACAS. HOLDS VENEZUELAN ID CEDULA V 3140806.

"B. FREDDY (NOT FEDERICO) LUGO - HOLDER OF VENEZUELAN PASSPORT 006543 (THIS IS THE PERFERATED NUMBER--NUMBER WRITTEN IN THE PASSPORT IS 2123051), ISSUED JULY 6, 1976, IN CARACAS. SINGLE. BORN OCTOBER 17, 1942. GAVE RESIDENCE AS CARACAS AND OCCUPATION AS JOURNALIST. HOLDS ID CEDULA VO 2123051. CARRIES OFFICIAL PRESS CARD NO 152 OF CIRCULO DE REPORTEROS GRAFICOS DE VENEZUELA. HE ALSO HAD IN HIS POSSESSION TOURIST CARD FOR COLOMBIA DATED JULY 15, 1976. THIS GAVE PERMANENT ADDRESS AS IRB URDANETA VERDA 24, CARACAS.

"THESE TWO VENEZUELANS ARRIVED IN TRINIDAD FROM CARACAS ON PANAM 443 EARLY MORNING HOURS WEDNESDAY, OCTOBER 6. CHECKED INTO HOLIDAY INN AT 0200 HOURS. HOTEL REGISTRATION MADE IN NAMES OF

~~END PAGE ONE~~

STATE DEPT. INFO (ALL PARAS) IS UNCLASSIFIED PER DOS AUTHORITY 8/28/96

SECRET

~~PAGE ONE S E C R E T~~

JOSE GARCIA/FREDDY PEREZ. HOME ADDRESS GIVEN AS CRR CRISTO
N NO 61, VALENCIA, VENEZUELA. HAD LUGGAGE WHEN CHECKED INTO HOTEL.

"VENEZUELANS CHECKED OUT OF HOLIDAY INN ABOUT 0600 OCTOBER 6 WITH LUGGAGE AND WERE SEEN AT PIARCO AIRPORT. BOARDED CUBANA FLIGHT AT 1150 OCTOBER 6 TO BARBADOS.

"RETURNED FROM BARBADOS TO TRINIDAD ON SAME DAY ON BWIA FLIGHT AT 2155 AND CHECKED INTO HOLIDAY INN AT 2300 WITHOUT SUITCASES. REGISTRATION IN NAME OF GUSTAVO GARCIA, RESIDENCE BOGOTA, COLOMBIA. THEY CLAIMED THE SUITCASES HAD BEEN STOLEN, BUT THEY HAVE MADE NO REPORT OF STOLEN SUITCASES EITHER TO AIRLINE OR BARBADOS OR TRINIDAD POLICE.

"AMONG DOCUMENTS IN HANDS OF POLICE IS BOARDING PASS OF E. SEALY FOR DIFFERENT BWIA FLIGHT. POLICE CHECKING THIS OUT. THIS THEY BELIEVE COULD BE TRINIDAD ACCOMPLICE.

"OF INTEREST IS FACT BOTH PASSPORTS FAIRLY NEW. THEREFORE DIFFICULT TRACE PAST TRAVEL. HOWEVER, PASSPORT OF FREDDY LIBORIO HAVE STAMP SHOWING ENTRY AT BARBADOS ON JULY 9. (NOTE: THE BOMBS WHICH WENT OFF AT THE BWIA OFFICE AND AT THE GENERAL MANAGER'S CAR AND YACHT IN BRIDGETOWN, BARBADOS, TOOK PLACE ON 10 AND 11 JULY 1976.)

~~END PAGE THREE~~

STATE DEPT. INFO (ALL PARAS.) IS UNCLASSIFIED PER DOS AUTHORITY 6/26/96

SECRET

4

"PAGE IN POSSESSION OF LIGO APPARENTLY FROM ADDRESS BOOK WITH LETTER "E" ON IT CITED FOLLOWING: EMBASSY AMERICAN 2846111-1271 FBI JOSEPH LEO 331511.

"TRINIDAD AND TOBAGO POLICE ARE FINGERPRINTING BOTH SUSPECTS AND COPYING ALL DOCUMENTS IN THEIR POSSESSION.

"TRINIDAD AND TOBAGO POLICE REQUEST URGENTLY ANY INFORMATION OF THESE PERSONS, PARTICULARLY ANY CRIMINAL RECORDS. NO OBJECTION TO LEGATT CONTACTING LOCAL POLICE/SECURITY SERVICES. POLICE REQUEST AT LEAST INTERIM REPLY BEFORE 1700 LOCAL TIME. PLEASE SEND REPLY REACT IMMEDIATE.

"POLICE WOULD LIKE TO KNOW IF ANYONE FROM LEGATT OFFICE PLANS TO COME TO TRINIDAD ON THIS CASE, OR HOW YOUR WOULD LIKE TO RECEIVE COPIES OF FINGERPRINTS, ETC."

[redacted] (b)

ON OCTOBER 7, 1976, A CONFIDENTIAL SOURCE ABROAD ADVISED THAT (b)

END PAGE FOUR

SECRET

~~PAGE FIVE OAR 2-5 S E C R E T~~

FREDDY LUGO IS A VENEZUELEN NEWSMAN WHO IS ALSO EMPLOYED AS AN IN-
VESTIGATOR BY LUIS POSADA, [redacted] (S)
[redacted] CARACAS. HE RESIGNED FROM HIS POSITION [redacted] (S)
IN 1973, [redacted] (S) POSADA IS A CUBAN EXILE WHO IS KNOWN FOR HIS ANTI-CASTRO
ACTIVITIES, AND HE REPORTEDLY ASSISTED ORLANDO BOSCH AVILA IN 1974,
SHORTLY BEFORE BOSCH WAS ARRESTED BY VENEZUELAN AUTHORITIES. (S)

LEGAT BECAME ACQUAINTED WITH POSADA WHILE THE LATTER WAS
[redacted] (S) AND AFTER HIS RESIGNATION, POSADA CONTINUED
TO CONTACT LEGAT ON RARE OCCASIONS, USUALLY IN ORDER TO OBTAIN
PERSONALIZED SERVICE IN CONNECTION WITH VISA REQUESTS. IN VIEW OF
LUGO'S EMPLOYMENT BY POSADA, LEGAT ASSUMES HIS NAME AND TELEPHONE
NUMBER WERE FURNISHED TO LUGO BY POSADA. LEGAT ESTIMATES HE HAS
SEEN POSADA IN PERSON ON PERHAPS THREE OCCASIONS SINCE 1973, THE
LAST TIME BEING ON JUNE 10, 1976, WHEN POSADA VISITED LEGAT OFFICE
TO INQUIRE IF FBI HAD INTEREST IN CARLO BORDONI (BUFILE 29-[illegible]
OARFILE 29-19). INFORMED IN THE AFFIRMATIVE, POSADA REVEALED
BORDONI HAD HIRED TWO OF HIS OPERATIVES AS ARMED BODY GUARDS AT HIS
HOME. THAT INFORMATION WAS SUBSEQUENTLY PASSED BY LEGAT TO [redacted]
[redacted] (S) WHO WERE INVOLVED IN THE ARREST ACTION AGAINST BORDONI. (S)

~~END PAGE FIVE~~

SECRET

SECRET

~~PAGE SIX CAR C O S E C R E T~~

POSADA MORE OFTEN REFERRED TO LEGAT RELATIVES AND ASSOCIATES SEEKING ADVICE REGARDING VISAS, THE LAST BEING ONE OF HIS EMPLOYEES, HERNAN RICARDO LOZANO, WHO SOUGHT A VISA TO TRAVEL TO SAN JUAN, PUERTO RICO, ON OCTOBER 1, 1976. LEGAT WILL PROVIDE ADDITIONAL INFO DEVELOPED REGARDING RICARDO IN A SUBSEQUENT COMMUNICATION. (S)

1C ON OCTOBER 7, 1976, THE CONFIDENTIAL SOURCE FURTHER ADVISED THAT IN VIEW OF THE ARREST OF VAZQUEZ AND LIGO IN TRINIDAD, THE [redacted] B (S)(U) WAS ARRANGING FOR LUIS POSADA AND ORLAND BOSCH AVILA TO B LEAVE [VENEZUELA] (S)(U) AS SOON AS POSSIBLE. THE SOURCE ALL BUT ADMITTED THAT POSADA AND BOSCH HAD ENGINEERED THE BOMBING OF THE AIRLINE, AND HE PROMISED TO FURNISH FURTHER DETAILS ON OCTOBER 8, 1976. (S)

~~CLASSIFIED BY KRUS, ADD, CATEGORIES B AND A, INDEFINITE.~~

ADMIN TO FIELD AND LEGATS ONLY

ADMINISTRATIVE: CONFIDENTIAL SOURCE IS [redacted] A

[redacted] CARACAS, A-B VENEZUELA. (S)(U)

FROM STATEMENTS OF [redacted] IT APPEARS ALMOST CERTAIN THAT THE A [redacted] WAS PRIVY TO THE ACTIVITIES OF POSADA AND B BOSCH AND THAT IT NOW WILL ATTEMPT TO DISASSOCIATE ITSELF FROM THEM FOR FEAR OF RETALIATION BY THE CUBAN GOVERNMENT. (S)(U)

END

ADMIN TO FIELD AND LEGATS ONLY

SECRET

INITIAL 7WA

RELEASED PER P.L.-102-526(JFK ACT)
NARA R.T. DATE 5-17-05

Reproduced at the National Archives

DIRECTORATE OF OPERATIONS

Intelligence Information Cable

PRIORITY

IN 069101

WARNING NOTICE
SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED

STATE/INR JCS/MC (DIA) CIA/NMCC SWS NSA TREAS NSC/S SDO NIO CBS

PAGE 1 OF 5 PAGES

{SY/I/PIB} SS/IN FBI SECUR

Classified by Recorded Reporting Officer. Exempt from General Declassification Schedule of E.O. 11652 Exemption Category 5B (1), (2). Impossible to Determine Date of Automatic Declassification.

FURTHER DISSEMINATION AND USE OF THIS INFORMATION SUBJECT TO CONTROLS STATED AT BEGINNING AND END OF REPORT.

THIS IS AN INFORMATION REPORT, NOT FINALLY EVALUATED INTELLIGENCE

SECRET

CITE TDFIR DB-315/10256-76

ALL FBI INFORMATION CONTAINED HEREIN IS ~~UNCLASSIFIED~~ DATE 7-27-94 BY SP1 mc/ksa (OPIC)

DIST 16 OCTOBER 1976

REPORT CLASS S E C R E T--WARNING NOTICE-SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED--NOT RELEASABLE TO FOREIGN NATIONALS--NOT RELEASABLE TO CONTRACTORS OR CONTRACTOR/CONSULTANTS

POLITICAL MATTERS

COUNTRY: VENEZUELA/CUBA

DOI : LATE SEPTEMBER -12 OCTOBER 1976

SUBJECT: ACTIVITIES OF CUBAN EXILE LEADER ORLANDO BOSCH DURING HIS STAY IN VENEZUELA

PLACE : VENEZUELA, CARACAS (13 OCTOBER 1976) FIELD NO. [redacted]7514

SOURCE: A FORMER VENEZUELAN GOVERNMENT OFFICIAL WHO STILL MAINTAINS CLOSE RELATIONSHIPS WITH GOVERNMENT OFFICIALS. HE IS A USUALLY RELIABLE REPORTER. THIS INFORMATION IS NOT TO BE DISCUSSED WITH ANY FOREIGN OFFICIALS, INCLUDING THOSE OF THE VENEZUELAN GOVERNMENT.

1. (FIELD COMMENT: IN LATE SEPTEMBER 1976 A USUALLY RELIABLE SOURCE REPORTED THAT CUBAN EXILE LEADER ORLANDO BOSCH WAS IN VENEZUELA UNDER THE PROTECTION OF VENEZUELAN PRESIDENT CARLOS ANDRES PEREZ. FURTHERMORE, PEREZ HAD APPOINTED HIS SECURITY AND INTELLIGENCE ADVISER ORLANDO GARCIA TO PROTECT AND ASSIST BOSCH DURING HIS STAY IN VENEZUELA. FOR THIS INFORMATION SEE [redacted]7483, TDFIRDB-315/09430-76, [redacted]7483, TDFIRDB-315/09434-76.

SECRET

REC-86 DE-40 ST-108 109-12-228

CIA chart

OF MID-SEPTEMBER, A SOURCE OF UNDETERMINED RELIABILITY REPORTED THAT BOSCH ARRIVED IN VENEZUELA ON APPROXIMATELY 13 SEPTEMBER.

2. UPON HIS ARRIVAL IN CARACAS, BOSCH WAS MET AT THE AIRPORT BY GARCIA AND LUIS CLEMENTE P O S A D A, A PRIVATE INVESTIGATOR AND ONE-TIME MEMBER OF THE DIRECTORATE FOR THE SERVICES OF INTELLIGENCE AND PREVENTION (DISIP), WHO ESCORTED BOSCH TO HIS CARACAS HOTEL. (FIELD COMMENT: WHILE CURRENTLY NATURALIZED VENEZUELAN CITIZENS, BOTH GARCIA AND POSADA ARE NATIVE-BORN CUBANS.)

3. SOMETIME FOLLOWING BOSCH'S ARRIVAL IN CARACAS, A BS. 5,000 (APPROXIMATELY U.S. $1,118) A PLATE FUND-RAISING DINNER FOR BOSCH WAS HELD AT THE HOME OF HILDO F O L G A R, A PROMINENT SURGEON AND CUBAN EXILE. IN ADDITION TO BOSCH, AMONG THOSE ATTENDING THE DINNER WERE GARCIA; RICARDO G O N Z A L E S NAVARETTE, GARCIA'S DEPUTY WHO IS ALSO A NATIVE-BORN CUBAN; POSADA; AND AN UNIDENTIFIED HIGH-LEVEL OFFICIAL OF THE MINISTRY OF INTERIOR.

4. DURING THE EVENING BOSCH APPROACHED THE MINISTRY OF INTERIOR OFFICIAL THROUGH GARCIA PROPOSING THAT THE VENEZUELAN GOVERNMENT MAKE A SUBSTANTIAL CASH CONTRIBUTION TO HIS ORGANIZATION. IN RETURN, BOSCH AGREED TO GUARANTEE THAT THERE WOULD BE NO CUBAN EXILE DEMONSTRATIONS IN THE UNITED STATES DURING PRESIDENT PEREZ' PLANNED

NOVEMBER APPEARANCE AT THE UNITED NATIONS(UN). (SOURCE COMMENT: IT IS BELIEVED THAT BOSCH'S PROPOSITION WAS AT LEAST TENTATIVELY ACCEPTED BY THE MINISTRY OF INTERIOR OFFICIAL.)

5. ALSO DURING THE EVENING BOSCH MADE THE STATEMENT THAT, "NOW THAT OUR ORGANIZATION HAS COME OUT OF THE LETELIER JOB LOOKING GOOD, WE ARE GOING TO TRY SOMETHING ELSE." BOSCH DID NOT NAME THE ORGANIZATION NOR DID HE EXPAND ON HIS MEANING. (FIELD COMMENT: THE LETELIER MENTIONED ABOVE IS PROBABLY FORMER CHILEAN FOREIGN MINISTER ORLANDO L E T E L I E R, WHO WAS ASSASSINATED IN THE UNITED STATES ON 21 SEPTEMBER.)

6. A FEW DAYS FOLLOWING THE FUND-RAISING DINNER, POSADA WAS OVERHEARD TO SAY THAT, "WE ARE GOING TO HIT A CUBAN AIRPLANE," AND THAT "ORLANDO HAS THE DETAILS." (SOURCE COMMENT: THE IDENTITIES OF THE "WE" AND "ORLANDO" MENTIONED IN THE STATEMENT ARE NOT KNOWN.)

7. FOLLOWING THE 6 OCTOBER CUBANA AIRLINE CRASH OFF THE COAST OF BARBADOS, BOSCH, GARCIA AND POSADA AGREED THAT IT WOULD BE BEST FOR BOSCH TO LEAVE VENEZUELA. THEREFORE, ON 9 OCTOBER POSADA AND GARCIA ESCORTED BOSCH TO THE COLOMBIAN BORDER, WHERE THE LATTER CROSSED OVER INTO COLOMBIAN TERRITORY.

8. ON THE BASIS OF INFORMATION RECEIVED FROM TRINIDADIAN

IN 069101

TDFIRDB-315/10256-76

WARNING NOTICE
SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED

PAGE 4 OF 5 PAGES

SECRET

FURTHER DISSEMINATION AND USE OF THIS INFORMATION SUBJECT TO CONTROLS STATED AT BEGINNING AND END OF REPORT

(classification)

AUTHORITIES IMPLICATING HIM, POSADA WAS ARRESTED BY DISIP AUTHORITIES ON 12 OCTOBER. HIS OFFICE WAS SUBSEQUENTLY RAIDED AND ALL FILES AND EQUIPMENT CONFISCATED.

9. MEANWHILE, PRESIDENT PEREZ HAS ASSURED THE CUBAN GOVERNMENT, THROUGH CUBAN AMBASSADOR NORBERTO H E R N A N D E Z CURBELO, THAT THE VENEZUELAN GOVERNMENT WILL ENERGETICALLY PURSUE THE INVESTIGATION OF THE CUBANA CRASH. IN RETURN, HOWEVER, CUBA WILL BE EXPECTED TO SUPPORT VENEZUELA'S ANTI-TERRORISM POSITION AT THE UN.

10. (EMBASSY COMMENT: THE AMBASSADOR COMMENTS: "THE LEGATT HAS DIFFERENT INFORMATION AS TO WHETHER BOSCH WAS EXFILTRATED OR IS OR IS NOT IN VENEZUELA. GARCIA SPOKE TO LEGATT SUNDAY MORNING, 10 OCTOBER, AND ON THE AFTERNOON OF 12 OCTOBER TOLD HIM "INFORMALLY" THAT THE PRESIDENT WOULD SHORTLY ADVISE ME THAT BOSCH WOULD BE TURNED OVER TO US. THIS WAS REPEATED TO LEGATT BY DISIP DIRECTOR RAUL G I M E N E Z GAINZA AND OTHER DISIP OFFICIALS (INCLUDING GARCIA) IN A MEETING THE MORNING OF 13 OCTOBER. CONCEIVABLY GARCIA CAN BE PLAYING A DARK GAME; BUT THE DISCREPANCIES ARE NOTEWORTHY. I HAVE NOT YET RECEIVED ANY OFFICIAL WORD AS TO THE PRESIDENT'S DECISION.")

11. FIELD COMMENT: EMBASSY, LEGATT AT CARACAS SENT TO

SECRET

IN 069101

TDFIR DB-315/11756-76

WARNING NOTICE
SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED

PAGE 5 OF 5 PAGES

SECRET
(classification)

FURTHER DISSEMINATION AND USE OF THIS INFORMATION SUBJECT TO CONTROLS STATED AT BEGINNING AND END OF REPORT.

PORT OF SPAIN, GEORGETOWN, KINGSTON, MEXICO CITY, MANAGUA, GUATEMALA CITY, PANAMA CITY, SANTO DOMINGO, SANTIAGO, BOGOTA.

REPORT CLASS S E C R E T--WARNING NOTICE-SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED--NOT RELEASABLE TO FOREIGN NATIONALS--NOT RELEASABLE TO CONTRACTOS OR CONTRACTOR/CONSULTANTS.

CLASSIFIED BY RECORDED REPORTING OFFICER. XGDS-2.

ADVANCE COPY TRANSMITTED TO: STATE, DIA, ARMY, NAVY, AIR, JCS, NSA, SMS, CIA/OPSCEN, SS/ID, FBI, TREASURY.

[redacted]

30009

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20504

January 25, 2001

INFORMATION

MEMORANDUM FOR CONDOLEEZZA RICE

FROM: RICHARD A. CLARKE

SUBJECT: Presidential Policy Initiative/Review -- The *Al-Qida* Network

Condi,
Steve asked today that we propose major Presidential policy reviews or initiatives. We *urgently* need such a Principals level review on the *al Qida* network.

Just some Terrorist Group?

As we noted in our briefings for you, *al Qida* is not some narrow, little terrorist issue that needs to be included in broader regional policy. Rather, several of our regional policies need to address centrally the transnational challenge to the US and our interests posed by the *al Qida* network. By proceeding with separate policy reviews on Central Asia, the GCC, North Africa, etc. we would deal inadequately with the need for a comprehensive multi-regional policy on *al Qida*.

al Qida is the active, organized, major force that is using a distorted version of Islam as its vehicle to achieve two goals:

--to drive the US out of the Muslim world, forcing the withdrawal of our military and economic presence in countries from Morocco to Indonesia;

--to replace moderate, modern, Western regime in Muslim countries with theocracies modeled along the lines of the Taliban.

al Qida affects centrally our policies on Pakistan, Afghanistan, Central Asia, North Africa and the GCC. Leaders in Jordan and Saudi Arabia see *al Qida* as a direct threat to them. The strength of the network of organizations limits the scope of support friendly Arab regimes can give to a range of US

[redacted]

Classified by: Richard A. Clarke
Reason: 1.5(d)(x6)
Declassify On: 1/25/25
Derived From: Multiple Sources

NSC DECLASSIFICATION REVIEW [E.O. 12958]
/X/ Exempt in part and redact as shown
by D.Sanborn Date 4/7/2004

policies, including Iraq policy and the Peace Process. We would make a major error if we underestimated the challenge *al Qida* poses, or over estimated the stability of the moderate, friendly regimes *al Qida* threatens.

Pending Time Sensitive Decisions

At the close of the Clinton Administration, two decisions about *al Qida* were deferred to the Bush Administration.

-- First, should we provide the Afghan Northern Alliance enough assistance to maintain it as a viable opposition force to the Taliban/al Qida? If we do not, I believe that the Northern Alliance may be effectively taken out of action this Spring when fighting resumes after the winter thaw. The al Qida 55th Brigade, which has been a key fighting force for the Taliban, would then be freed to send its personnel elsewhere, where they would likely threaten US interests. For any assistance to get there in time to effect the Spring fighting, a decision is needed now.

-- Second, should we increase assistance to Uzbekistan to allow them to deal with the al Qida/ IMU threat? [redacted]

Operational detail, removed at the request of the CIA

Three other issues awaiting addressal now are:

--First, what the new Administration says to the Taliban and Pakistan about the importance we attach to ending the al Qida sanctuary in Afghanistan. We are separately proposing early, strong messages to both.

--Second, do we propose significant program growth in the FY02 budget for anti-al Qida operations by CIA and counter-terrorism training and assistance by State and CIA?

--Third, when and how does the Administration choose to respond to the attack on the USS Cole. That decision is obviously complex. We can make some decisions, such as the those above, now without yet coming to grips with the harder decision about the Cole. On the Cole, we should take advantage of the policy that we "will respond at a time, place, and manner of our own choosing" and not be forced into knee jerk responses.

[redacted]

[redacted] 3

Attached is the year-end 2000 strategy on al Qida developed by the last Administration to give to you. Also attached is the 1998 strategy. Neither was a "covert action only" approach. Both incorporated diplomatic, economic, military, public diplomacy and intelligence tools. Using the 2000 paper as background, we could prepare a decision paper/guide for a PC review.

I recommend that you have a Principals discussion of *al Qida* soon and addresss the following issues:

1. Threat Magnitude: Do the Principals agree that the *al Qida* network poses a first order threat to US interests in a number or regions, or is this analysis a "chicken little" over reaching and can we proceed without major new initiatives and by handling this issue in a more routine manner?

2. Strategy: If it is a first order issue, how should the existing strategy be modified or strengthened?

Two elements of the existing strategy that have not been made to work effectively are a) going after *al Qida's* money and b) public information to counter *al Qida* propaganda.

3. FY02 Budget: Should we continue the funding increases into FY02 for State and CIA programs designed to implement the *al Qida* strategy?

4. Immediate [redacted] Decisions: Should we initiate [redacted] funding to the Northern Alliance and to the Uzbek's?

Please let us know if you would like such a decision/discussion paper or any modifications to the background paper.

Concurrences by: Mary McCarthy, Dan Fried, Bruce Reidel, Don Camp

Attachment
Tab A December 2000 Paper: Strategy for Eliminating the Threat from the Jihadist Networks of al-Qida: Status and Prospects

Tab B September 1998 Paper: Pol-Mil Plan for al-Qida

[redacted]

Elwood, Courtney

From: David.Kris@timewarner.com
Sent: Thursday, December 22, 2005 12:37 PM
To: Elwood, Courtney
Subject: Re: NSA talkers

Thanks, Courtney, these are very helpful and interesting. From a quick read on my BB, it looks like you guys are leading with Article II and using the AUMF as support, rather than leading with the AUMF interpreted broadly in light of constitutional avoidance doctrine, and then falling back to Article II. If I'm reading it right, that's an interesting choice -- maybe it reflects the VP's philosophy that the best defense is a good offense (I don't expect you to comment on that :-)). Thanks again for sharing these and I hope you have a nice holiday. I'll be in Texas (BB and cell: [redacted]) until next Tuesday. ← FOIA EXEMPTION b6 (72)

-----Original Message-----
From: Courtney.Elwood@usdoj.gov
To: Kris, David
Sent: Thu Dec 22 12:05:26 2005
Subject: NSA talkers

FYI.

==========
This message is the property of Time Warner Inc. and is intended only for the use of the addressee(s) and may be legally privileged and/or confidential. If the reader of this message is not the intended recipient, or the employee or agent responsible to deliver it to the intended recipient, he or she is hereby notified that any dissemination, distribution, printing, forwarding, or any method of copying of this information, and/or the taking of any action in reliance on the information herein is strictly prohibited except by the original recipient or those to whom he or she intentionally distributes this message. If you have received this communication in error, please immediately notify the sender, and delete the original message and any copies from your computer or storage system. Thank you
==========

[redacted]

-----Original Message-----
From: David.Kris@timewarner.com <David.Kris@timewarner.com>
To: Elwood, Courtney <Courtney.Elwood@SMOJMD.USDOJ.gov>
Sent: Thu Jan 19 23:31:45 2006
Subject: RE: NSA

Not responsive to request

tmp.htm (6 KB)

Courtney

I'm making my way through the whitepaper now, and of course it's very professional and thorough and well written. I kind of doubt it's going to bring me around on the statutory arguments -- which I have always felt had a slightly after-the-fact quality or feeling to them -- but you never know, and in any event I can respect the analysis even if I don't fully agree. And I will remain open on the constitutional arguments, which is what I have always felt this was really about; I just don't feel I have much to say on the constitutional issues without knowing the facts.

But I do have one fairly minor question about this whitepaper that I may as well send you now. I am a little puzzled as to why you guys didn't rely more heavily on footnote 54 on page 100 of the 1978 House Intelligence Committee Report. You have the New York Telephone case cited and you make the pen-trap argument (on page 22), but I would have thought you'd put footnote 54 in neon lights.

Talk to you later.

-- David

Not responsive to request

[redacted]

lwood, Courtney

From: David.Kris@timewarner.com
Sent: Wednesday, December 21, 2005 6:04 PM
To: Elwood, Courtney
Subject: RE: IN CASE YOU MISSED IT: President Had Legal Authority To OK Ta ps

My major disagreement with this, I think, is that the President's inherent authority to conduct electronic surveillance or physical searches in the *absence* of legislation is not the same as his inherent authority to do so in the *presence* of such legislation.

102

-----Original Message-----
From: Courtney.Elwood@usdoj.gov [mailto:Courtney.Elwood@usdoj.gov]
Sent: Wednesday, December 21, 2005 3:37 PM
To: Kris, David
Subject: Fw: IN CASE YOU MISSED IT: President Had Legal Authority To OK Taps
Importance: Low

I am sure you saw this.

Sent from my BlackBerry Wireless Handheld

Not responsive to request

[redacted]

Help
Return to Headlines

THE WALL STREET JOURNAL.

REVIEW & OUTLOOK (Editorial)

Open the Iraq Files

967 words
3 March 2006
The Wall Street Journal
A10
English
(Copyright (c) 2006, Dow Jones & Company, Inc.)

When the 9/11 Commission bullied Congress into creating the Directorate of National Intelligence, we doubted that another layer of bureaucracy on top of the CIA would fix much of anything. Our skepticism has since been largely reinforced -- most recently by the DNI's reluctance to release what's contained in the millions of "exploitable" documents and other items captured in Iraq and Afghanistan.

These items -- collected and examined in Qatar as part of what's known as the Harmony program -- appear to contain information highly relevant to the ongoing debate over the war on terror. But nearly three years after Baghdad fell, we see no evidence that much of what deserves to be public will be anytime soon.

For example, if it hadn't been for the initiative of one Bill Tierney, we wouldn't know that Saddam Hussein had a habit of tape recording meetings with top aides. The former U.N. weapons inspector and experienced Arabic translator recently went public with 12 hours (out of a reported total of 3,000) of recordings in which we hear Saddam discuss with the likes of Tariq Aziz the process of deceiving U.N. weapons inspectors and his view that Iraq's conflict with the U.S. didn't end with the first Gulf War.

In one particularly chilling passage, the dictator discusses the threat of WMD terrorism to the United States and the difficulty anyone would have tracing it back to a state. With the 2001 anthrax attacks still unsolved, that strikes us as bigger news than the DNI or most editors apparently considered it.

In another disclosure, the Weekly Standard's Stephen Hayes was told by about a dozen officials that Harmony documents describe in detail how Saddam trained thousands of Islamic radicals in the waning years of his regime. So much for the judgments of many in the intelligence community -- including Paul Pillar, the latest ex-spook to go public with his antiwar message -- that the secular Saddam would never consort with such religious types.

To its credit, the DNI did bless the recent release of about two dozen documents from Afghanistan as part of a West Point study painting a portrait of al Qaeda's organizational structure. They show that al Qaeda functioned like a corporation in some ways, with fixed terms for employee benefits such as family leave, and seem to vindicate the once-controversial decision to move quickly to destroy al Qaeda's base of operations in Afghanistan.

But these tantalizing tidbits represent only a fraction of what's in U.S. possession. We hear still other documents expand significantly on our knowledge of Saddam's WMD ambitions (including more on the Niger-uranium connection) and his support for terrorism, right down to lists of potential targets in the U.S. and Europe. Former Assistant Defense Secretary Richard Perle accuses the DNI of "foolish restraint" on releasing information that could broaden understanding and bolster support for a war that is far from won. Representative Pete Hoekstra (R., Mich.) echoes that criticism. And after chatting with the Congressman and with someone we agreed to describe as a "senior intelligence official familiar with the program," we largely agree.

The intelligence community has a point that some caution must be exercised. For example, the senior intelligence official pointed out, some documents describe in detail rapes and other abuses committed by Saddam's regime -- details that could still haunt living victims in such an honor-bound society as Iraq. But while it would seem to make sense to screen the documents for such items -- and perhaps terrorist recipes such as ricin -- we still can't understand how that justifies the current pace and method of making information public.

And our alarm bells really rang when the intelligence official added another category of information that's never slated to see the light of day: "We cannot release wholesale material that we can reasonably foresee will damage the national interest." Well, what exactly does that mean and who makes the call? The answer, apparently, is unaccountable analysts following State Department guidelines.

But consider just one hypothetical: Is it in the "national interest" to reveal documents if they show that Jacques Chirac played a more substantial role in encouraging Saddam's intransigence than is already known? No doubt some Foggy Bottom types would say no. But we'd strongly disagree. The "national interest" exception is so broad and vague that it would end up being used to

justify keeping secret the merely embarrassing.

What's more, according to Mr. Hoekstra, the DNI release plans don't call for making any documents publicly available per se, but only through scholars in the manner of the West Point study. As he puts it, the decision to move everything through analysts and carefully chosen outsiders is an "analog" method in a "digital" age, when we could be calling on the interpretive wisdom of so many by putting much of it on the Internet.

Yesterday Mr. Hoekstra introduced a bill to require the intelligence community to be more forthcoming with the Iraq and Afghanistan documents. "I'm beginning to believe the postwar intelligence may be as bad as the prewar intelligence," he says. Another person who sees vast room for improvement is Iraqi scholar Kanan Makiya, who founded the Iraq Memory Foundation. While he shares the DNI's concerns about potential damage to some people mentioned therein, he also says the U.S. government has gone too far and needs to find better ways to grant access to this information.

America went to war in Iraq and Afghanistan because we believed that the truth about the regimes in those countries justified it. Why should so much of that truth now be deemed so sensitive?

Document J000000020060303e2330001k

Return to Headlines

factiva © 2006 Factiva, Dow Jones & Reuters

Mr. SHAYS. At this time, the chair would recognize Mr. Van Hollen.

Mr. VAN HOLLEN. Thank you, Mr. Chairman. I want to thank you and Mr. Kucinich for holding these hearings and thank the witnesses for being here.

The latest episodes we have seen of the administration scrambling to reclassify information that had been declassified is just the latest sign of an obsession with secrecy over the public interest. I think it is amazing now that an individual working for the government could be criminally liable for providing to a Member of Congress in an unclassified setting a document that had been published by the U.S. Government. That turn of events, it seems to me, shows how we have our policies just turned on their head.

I would just like to very briefly read from the 9/11 Commission, which was a bipartisan commission that identified this over-classification problem as a national security problem, where they stated that the security concerns need to be weighed against the cost. "Current security requirements nurture over-classification and excessive compartmentalization of information among agencies. Each agency's incentive structure opposes sharing, with risks but few rewards for sharing information. No one has to pay the long-term costs of over-classifying information, though these costs, even in literal financial terms, are substantial." There are no punishments for not sharing information, and they go on to talk about this issue.

It seems to me that from a pure national security perspective, in this day and age where we learned from over-compartmentalization before September 11th the dangers to our national security of people not talking to each other, we should learn the lessons of more sharing of information. Instead, what we have seen is an effort to use the classification system not to hide information from our enemies, but in many cases, to hide embarrassing analyses and facts from the Congress and the American people.

So I hope, Mr. Chairman, that we will continue to explore this area. The other thing that, of course, I think, rankles many people is not just the classification process, but the random ad hoc declassification process, where all of a sudden you read that the administration has released classified information selectively for their own political benefit. I mean, we read now in the Valerie Plame case, oh, yes, well, they were able to leak classified information to the press. Why? Because the Vice President has the ability to declassify whenever he decides to declassify something. That breeds cynicism in the system and public distrust. If we think that the administration or any executive branch agency is playing politics with the release of classified information, is playing politics with the classification of information, it will undermine the public's trust in our entire system and breed increasing cynicism, and I think that is what we are seeing, Mr. Chairman.

So hopefully, we can begin to shine a little sunshine on this and reverse that cynicism. Thank you.

Mr. SHAYS. I thank the gentleman.

At this time, the chair would recognize the gentlelady from New York, Mrs. Maloney.

Mrs. MALONEY. Again, I want to thank the Subcommittee on National Security for their continued work on really sensitive issues

of our country. I want to cite the chairman's efforts on the creation of the 9/11 Commission report and then working with me and many others to author the recommendations into law and to finally pass it.

We all understand that classification is necessary. Maintaining access to sensitive information helps ensure the safety of all Americans. No one can argue that. However, over the last few years, a number of us have become very concerned with the dramatic surge in what is being classified and the advent of new pseudo-classifications of information.

At the last hearing the subcommittee held on the subject, I held up a poster of a redacted copy of a staff report from the 9/11 Commission. Black ink was practically poured over the whole document. What was amazing about the redactions on this poster were that they clearly covered up public testimony that was available on the Internet. Holding them side to side, we found one redacted line that read, literally—you can't make this stuff up—this was the line: "This, this, this, and this." That was redacted. It was more bad English than sensitive information, and that is our concern here.

There is a huge upswing in classified information, a result of more information that needs to be classified or is it just really more convenient to keep it classified? Is information kept classified because it is embarrassing? That is another concern. Or inconvenient?

We know that under an Executive order signed by President Clinton, we were able to declassify 864 million documents, but another Executive order by the Bush administration has halted these efforts by allowing officials to classify information even when there is significant doubt that this information needs to be classified.

I know that I have had to fight for the release of information held by government. I had a bill in on the Nazi War Crimes Disclosure Act. It has been years since World War II. It became law in 1998 and we really disclosed more information than we have had since the Nuremberg trials, and this was important for us to understand many things, not only our history but now to address informers and security matters in today's troubled times.

I am very concerned about the uniformity, the point that my colleague made that some ridiculous items are classified and then some information that may help a political cause, such as the Valerie Plame case, is released.

I also am concerned about that there is no review. Say you get a document back, like the 9/11 Commission report that was all redacted. How do we appeal to see if this is really, truly something that should be redacted or not? There is no appeal process. I think that the right of citizens to have access to their government files when this is appropriate helps build strength and support for our democracy.

So I want to thank Chairman Shays for holding this hearing and really for his continued work on it. I think it is important. I think it is an important part of our government and I think it does need to be reviewed. I find it infuriating—can I add this? I have constituents who come to me and they have tried to get documents from the EPA or whatever. The document comes back completely

redacted. I mean, what kind of response is that? Who do they appeal when it concerns their family farm or their family business? I think this is a serious matter and I appreciate the chairman looking at it.

Mr. SHAYS. I thank the gentlelady from New York.

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

Statement of Congresswoman Carolyn B. Maloney
Government Reform Subcommittee on National Security,
Emerging Threats and International Relations
Drowning in a Sea of Faux Secrets:
Policies on Handling of Classified and Sensitive Information
2154 Rayburn House Office Building
March 14, 2006
2:00 pm

I would like to thank Chairman Shays
for holding this important hearing
and his continued work in this area.

We all understand the need for the classification.

Maintaining access to sensitive information
helps ensure the safety of all Americans.

No one can argue with that.

However, over the last few years,
a number of us have been concerned
with the dramatic surge in what is being classified
and the advent of new pseudo-classifications
of information.

At the last hearing on this subject,

I held up a poster of a redacted copy
of a staff report of the 9/11 Commission.

Black ink was practically poured all over this report.

What was amazing about the redactions
on this poster were that they clearly covered-up
public testimony,
available on the internet.

Holding them side-to-side,
we found redacted line read:

"This, this, this and this"

It is more bad English than sensitive information.

That is what our concern is here.

Is the huge up-tick in classified information a result
of more information that needs to be classified
or is it just more convenient to keep it classified?

Is information kept classified just because it is

embarrassing?

We know that under an Executive Order
signed by President Clinton,
we were able to declassify 864 million documents,
but another Executive Order
by the current administration
has halted these efforts by allowing officials
to classify information even when there is significant
doubt that this information needs to be classified.

I know that I have had to fight for the release of
information held by the CIA
regarding our government's relationships
with Nazi war criminals after World War II –
relationships that were illegal.

I sponsored a bill that became law in 1998,
the Nazi War Crimes Disclosure Act,
but still to this day we are battling with the CIA f
or the full disclosure of these documents.

I would be hard pressed to find a current-day
need to continue to keeps these relationships

and interactions a secret.

But that does not seem to matter.

Certainly the right of the American people to know
is long overdue.

Information that we can use
to make sure that this piece of history is not lost,
instead it can be something that we can learn from
and make sure we never do again.

Anyway, I look forward to the testimony
of our witnesses
and I thank the Chairman for holding this hearing.

Mr. SHAYS. Let me just take care of a few business items before we swear you in, and thank you all for your patience.

I ask unanimous consent that all members of the subcommittee be permitted to place an opening statement in the record and the record remain open for 3 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, and without objection, so ordered.

I ask even further unanimous consent that the following be made part of the record: A GAO report titled "Managing Sensitive Information: Departments of Energy and Defense Policies and Oversight Could Be Improved;" George Washington University National Security Archive report, "Pseudo Secrets: Freedom of Information Audit of Sensitive But Unclassified (SBU) Policies in the U.S. Government;" a letter from Senator Jim Bunning Concerning the improvement of storage of classified information by defense contractors; and finally, a letter from Mr. Lamar Waldron from Marietta, Georgia, concerning the reclassification of government records. Without objection, the reports and correspondence will be made part of the record.

[NOTE.—The GAO report entitled, "Managing Sensitive Information, Departments of Energy and Defense Policies and Oversight Could be Improved," may be found in subcommittee files.]

[The information referred to follows:]

PSEUDO-SECRETS:

A Freedom of Information Audit of the U.S. Government's Policies on Sensitive Unclassified Information

March 2006

The National Security Archive
www.nsarchive.org

The George Washington University
Gelman Library, Suite 701
2130 H Street, NW
Washington, D.C. 20037
Phone: 202/994-7000
Fax: 202/994-7005
nsarchiv@gwu.edu

CONTENTS

EXECUTIVE SUMMARY i

INTRODUCTION 1

METHODOLOGY 3
Impact of Card Memorandum 3
Policies on Protection of Sensitive Unclassified Information 4
What is Sensitive Unclassified Information? 4
Notes on Findings 5

FINDINGS 6

CARD MEMORANDUM AND PROTECTION OF UNCLASSIFIED HOMELAND SECURITY INFORMATION 6
Review of Records for WMD or Other Sensitive Information 6
Web Site Information Removal 6
Increased Emphasis on Using Applicable FOIA Exemptions 7
Implementing New Security and Safeguarding Measures 7
Dissemination of Card Memorandum 7
No Records or No Response 7

AGENCY CONTROL OF SENSITIVE UNCLASSIFIED INFORMATION (SUI) 9
Authority for Policy 9
Definition and Guidance 12
Designation Authority 14
Decontrol Authority 16
Government Employees' Access to Protected Information 17
Physical Safeguards for Sensitive Information 19
Limitations on Use of Information Controls 20
Unclassified Information Policies and the Freedom of Information Act 21

AGENCY PROCESSING OF FOIA REQUESTS 23
Processing Time 23
Disparity in Response 23

RECOMMENDATIONS 25
Monitoring of Protected Documents 25
A Black Hole 26
The Hidden Costs 26
A Unified System 26

FURTHER READING 30

APPENDIX I: Card Memorandum FOIA Requests, Summary of Agency Processing

APPENDIX II: Impact of Card Memorandum, By Agency

APPENDIX III: Sensitive Unclassified Information FOIA Requests, Summary of Agency Processing

APPENDIX IV: Sensitive Unclassified Information, Policies by Agency

APPENDIX V: Sensitive Unclassified Information, Distinct Policies

APPENDIX VI: Glossary of Acronyms

EXECUTIVE SUMMARY

Although the numerous investigations into the September 11 attacks on the United States each concluded that excessive secrecy interfered with the detection and prevention of the attacks, new secrecy measures have nonetheless proliferated. This is the first comprehensive Report to summarize the policies for protection of sensitive unclassified information from a wide range of federal agencies and departments and identify the significant security, budgetary, and government accountability risks attendant to unregulated and unmonitored secrecy programs.

The picture that emerges from the diverse policies examined shows little likelihood that Congress or the public will be able to assess whether these policies are being used effectively to safeguard the security of the American public, or abused for administrative convenience or for improper secrecy. Unlike classified records or ordinary agency records subject to FOIA, there is **no monitoring of or reporting on the use or impact of protective sensitive unclassified information markings. Nor is there a procedure for the public to challenge protective markings.** Given the wide variation of practices and procedures as well as some of their features, it is probable that these policies interfere with interagency information sharing, increase the cost of information security, and limit public access to vital information.

The September 11 attacks on the United States and a March 2002 directive from White House Chief of Staff Andrew H. Card to federal agencies, requesting a review of all records and policies concerning the protection of "sensitive but unclassified" information spurred Congress and agencies to increase controls on information. What followed was the significant removal of information from public Web sites, increased emphasis on FOIA exemptions for withholding, and the proliferation of new categories of information protection markings.

Using targeted FOIA requests and research, the Archive gathered data on the information protection policies of 37 **major agencies and components**. Of the agencies and components analyzed, **only 8 of 37 (or 22%) have policies that are authorized by *statute or regulation*** while the majority (24 out of 37, or 65%) follow information protection policies that were generated internally, for example by directive or other informal guidance. Eleven agencies reported no policy regarding sensitive unclassified information or provided no documents responsive to the Archive's request.

Among the agencies and components that together handle the vast majority of FOIA requests in the federal government, **28 distinct policies for protection of sensitive unclassified information** exist: some policies conflate information safeguarding markings with FOIA exemptions and some include definitions for protected information ranging from very broad or vague to extremely focused or limited.

- **8 out of the 28 policies (or 29%) permit *any employee* in the agency to designate sensitive unclassified information for protection**, including the Department of Homeland Security (DHS is now the largest agency in the federal government other than Defense, with more than 180,000 employees); 10 of the policies (or 35%) allow only senior or supervisory officials to mark information for protection; 7 policies (or 25%) allow departments or offices to name a particular individual to oversee information protection under the policy; and 3 policies (or 11%) do not clearly specify who may implement the policy.

- In contrast, **12 of the policies (or 43%) are unclear or do not specify how, and by whom, protective markings can be removed**. Only one policy includes a provision for automatic decontrolling after the passage of a period of time or particular event. This is in marked contrast to the classification* system, which provides for declassification after specified periods of time or the occurrence of specific events.

- **Only 7 out of 28 policies (or 25%) include qualifiers or cautionary restrictions that prohibit the use of the policy markings for improper purposes**, including to conceal embarrassing or illegal agency actions, inefficiency, or

* The term "classified" or "classification" refers to information designated as protected under Executive Order 12958, as amended by E.O. 13292.

© 2006, The National Security Archive

administrative action. Again, this is distinguishable from the classification system, which explicitly prohibits classification for improper purposes.

- **There is no consistency among agencies as to how they treat protected sensitive unclassified information in the context of FOIA.** In a number of the agency policies, FOIA is specifically incorporated—either as a definition of information that may be protected or as a means to establish mandatory withholding of particular information subject to a sensitive unclassified information policy. Some agencies mandate ordinary review of documents before release, without regard to any protective marking. Others place supplemental hurdles that must be surmounted before sensitive information may be released to the public, for example the requirement of specific, case-by-case review by high-level officials for each document requested.

This Study finds that the procedures and regulations for safeguarding sensitive but unclassified information that were in use before September 11—particularly those protecting nuclear and other major, potentially-susceptible infrastructure information—differ markedly from the post-September 11 regulations. **The newest information protection designations are vague, open-ended, or broadly applicable,** thus raising concerns about the impact of such designations on access to information, free speech, and citizen participation in governance. As these findings suggest, more information control does not necessarily mean better information control. The implications certainly suggest that the time is ripe for a government-wide reform—with public input—of information safeguarding.

WHAT THE EXPERTS ARE SAYING

"[N]ever before have we had such a clear and demonstrable need for a seamless process for sharing and protecting information, regardless of classification."
-- J. William Leonard, ISOO Director (2003)[i]

"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."
-- Report, U.S. House of Representatives, Committee on Gov't Operations (1973)[ii]

"[T]hese designations sometimes are mistaken for a fourth classification level, causing unclassified information with these markings to be treated like classified information."
-- Moynihan Commission Report (1997)[iii]

"[T]hose making SSI designation . . . should have special training, much as FOIA officers do, because they are being asked to make difficult balancing decisions among competing values."
-- Coalition of Journalists for Open Government (2004)[iv]

"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."
-- Representative Christopher Shays (2005)[v]

"Terms such as 'SHSI' and 'SBU' describe broad types of potentially sensitive information that might not even fall within any of the FOIA exemptions."
-- Department of Justice, Freedom of Information Act Guide (2004)[vi]

"The fact that for official use only (FOUO) and other sensitive unclassified information (e.g. CONOPS, OPLANS, SOP) continues to be found on public web sites indicates that too often data posted are insufficiently reviewed for sensitivity and/or inadequately protected."
-- Sec. of Defense Donald Rumsfeld (2003)[vii]

"[V]ery little of the attention to detail that attends the security classification program is to be found in other information control marking activities."
-- Harold C. Relyea, Congressional Research Service (2005)[viii]

© 2006, The National Security Archive

INTRODUCTION

Four months after the September 11 attacks, the *New York Times* published a front page story that reported "the government is still making available to the public hundreds of formerly secret documents that tell how to turn dangerous germs into deadly weapons."[1] That story started a chain of events including, in March 2002, explicit direction from President Bush's Chief of Staff Andrew H. Card for all federal agencies and departments to review their methods for safeguarding records regarding weapons of mass destruction (WMD), including chemical, biological, radiological, and nuclear weapons ("Card Memorandum"). Attached to the Card Memorandum was a memorandum from the Acting Director of the Information Security Oversight Office (ISOO) and the Co-Directors of the Justice Department's Office of Information and Privacy (OIP) ("ISOO-DOJ Guidance") that concerned handling classified, declassified, and sensitive but unclassified information.

Since that time there have been reports about the proliferation of new categories of "safeguarded" sensitive unclassified information, congressional and public criticism about unregulated "pseudo-classification," and calls for reform.[2] Aside from a few studies looking at the origins of protection of sensitive, unclassified information, however, there is very little information in the public domain that could be used to assess such safeguarding. This Study examines the implementation of the Card Memorandum, the attributes of the new safeguard markings, and the impact that this extra protection of sensitive unclassified information may have on information disclosure.

DOCUMENT CONTROL LABELS USED BY EXECUTIVE DEPARTMENTS AND AGENCIES

Control label:	[Number of agencies using it]
ACDA use only	1
Addressee only	1
Administrative-Internal use only	1
Administratively confidential	1
Administratively restricted	4
ATOMAL	2
ATOMAL/COSMIC	2
Company confidential	1
Confidential	1
Confidential-Administrative	1
Confidential FR	1
Confidential-Personnel	1
Continued control	1
Critical nuclear weapon design information	1
CRYPTO	1
Distribution to U.S. Government agencies only	1
Distribution restricted—See DoD map or Chart Catalog for Guidance or Release Outside the U.S. Government	1
Exdis	2
Eyes only	2
For (name) only	1
For official use only	11
For staff use only	1
Formerly restricted data	4
10S channel-eyes only	1
Information for official use only	1
Internal NASA use only	1
Internal office	1
Limdis	2
Limit distribution	1
Limited access	1
Limited access to	1
Limited distribution	1
Limited—For official use only	1
Limited information	1
Limited official use	9
NASA sensitive data	1
NATO	1
No distribution outside department	1
Nodis	2
Noforn	4
Nonpublic	1
Not public information	1
Official use only	8
Personal	1
Private	1
Privileged business information	1
Proprietary	1
Restricted	2
Restricted data	6
SIOP	1
SIOP-ESI	1
SIOP/Special handling required not releasable to foreign nationals	1
SPECAT	1
Sensitive	1
Sensitive-in confidence	1
Special handling required not releasable to foreign nationals	1
U.S. Government use only	1
Weapon data	1

List of 63 labels identified by the Foreign Operations and Government Information Subcommittee in 1972.

The government's safeguarding or restricting access to documents and other information that *does not fall* within the purview of the national security classification system has been an issue for decades. In its first omnibus hearings on the implementation of the Freedom of Information Act (FOIA), in 1972, the Foreign Operations and Government Information Subcommittee of the House Government Operations Committee raised the issue of the "secrecy terms" that are used to identify and restrict access to government information outside of the classification system. The subcommittee identified 63 separate terms at that time which, according to Chairman William Moorhead, "range[d] from the asinine to the absurd."[3]

> *I do not see how nine categories of information can be expanded to 63 secrecy stamps. It might require further legislation to convince the secrecy-minded bureaucrats that Congress meant what it said 5 years ago when it passed the first Freedom of Information Act.*
>
> *–Chairman William Moorhead, House Subcommittee on Foreign Operations and Gov't Operations (1973)*[4]

The predominant congressional concern at that time was the overuse of control markings and distribution restrictions, applied to both classified and unclassified information, in the context of FOIA exemption 1, which permits information to be withheld because it is properly classified pursuant to Executive Order. In addition, the subcommittee evaluated

© 2006, The National Security Archive

the implications of the new Executive Order and the attendant security of classified information: "It is a concern because the more stamps you put on documents the less security you are going to have at the very sensitive levels where maximum security should be always safeguarded."[4]

Following these early congressional discussions, little action was taken beyond the threatening message that Chairman Moorhead sent to federal agencies about their use of control markings. Nonetheless, it appears that the use of such markings decreased, and public discussion of the matter quieted down in the subsequent years. In 1977, President Jimmy Carter issued a Directive mandating federal protection of telecommunications materials "that could be useful to an adversary."[5] Subsequently, one of President Ronald Reagan's National Security Decision Directives referred to "sensitive, but unclassified, government or government-derived information, the loss of which could adversely affect the national security interest" and, without further defining such information, ordered that it should be "protected in proportion to the threat of exploitation and the associated potential damage to the national security."[6]

The Computer Security Act of 1987 was passed in response to the proliferation of electronic communications and information systems and uncertainty about the nature of their security vulnerabilities. The Act defined "sensitive" information as "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under . . . the Privacy Act, but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."[7] The implementation of the Computer Security Act, directed in part by guidance from the National Institute of Standards and Technology, emphasized a "risk-based approach" to safeguarding information, in which agencies in their discretion were to determine the required level of protection for designated "sensitive" information in their computer systems, based on the nature of the information.

In 1997, Senator Daniel Patrick Moynihan's Commission on Protecting and Reducing Government Secrecy recognized the mounting difficulties with the use by more than 40 departments and agencies of various protective markings for unclassified information: "there is little oversight of which information is designated as sensitive, and virtually any agency employee can decide which information is to be so regulated." As to the general lack of understanding and consistency in the management of such protected information, the Commission found: "these designations sometimes are mistaken for a fourth classification level, causing unclassified information with these markings to be treated like classified information."[8]

Only an alert and knowledgeable citizenry can compel the proper meshing of the huge industrial and military machinery of defense with our peaceful methods and goals, so that security and liberty may prosper together.
– President Dwight D. Eisenhower[1]

Since the September 11 attacks and the inception of the War on Terrorism, new protective markings for unclassified information have been created, while numerous others have been updated, broadened, or used with increasing frequency. The Homeland Security Act of 2002 mandated information sharing among federal, state, and local authorities, and in conjunction directed the President to "identify and safeguard homeland security information that is sensitive but unclassified."[9] In 2003, President Bush delegated responsibility for protecting Sensitive Homeland Security Information (SHSI) to the Secretary of Homeland Security, but no regulations or other formalized SHSI protections have been implemented.

In December 2005, President Bush issued a memorandum for department heads regarding "Guidelines and Requirements in Support of the Information Sharing Environment." In this memo, the White House directed the agencies to develop standard procedures for handling Sensitive But Unclassified (SBU) information, including SHSI. These procedures, the memo asserted, "must promote appropriate and consistent safeguarding of the information and must be appropriately shared with, and accommodate and reflect the imperative for timely and accurate dissemination of terrorism information to, State, local, and tribal governments, law enforcement agencies, and private sector entities." The memo prescribes several action items, beginning with mandatory agency inventories of SBU procedures, followed by the Secretary of Homeland Security along with the Attorney General, the Secretaries of State, Defense, and Energy, and the DNI developing a recommendation for standardization of all the SBU policies, and finally implementing the standardized procedures through the Office of Management and Budget (OMB). To date, no proposals have been disseminated.

© 2006, The National Security Archive

METHODOLOGY

This Study seeks to evaluate the impact of the Card Memorandum directing the safeguarding of unclassified information and the breadth of policies related to the protection or control of unclassified information across the federal agencies. A number of recent reports have compiled lists of the array of different categories for non-classification protection, but none have requested and compared information from a broad swath of federal agencies on the protection of information that cannot properly be classified under existing procedures guided by the President's EO 12958. The Archive used Freedom of Information Act requests to compile data from federal agencies.

IMPACT OF CARD MEMORANDUM

On March 19, 2002, President Bush's Chief of Staff Andrew H. Card sent a memorandum ("Card Memorandum") to the heads of all executive departments and agencies of the Federal Government. The Card Memorandum called on departments and agencies to immediately reexamine current measures for identifying and safeguarding records regarding weapons of mass destruction (WMD), including chemical, biological, radiological, and nuclear weapons.

The Acting Director of the Information Security Oversight Office (ISOO) and the Co-Directors of the Justice Department's Office of Information and Privacy (OIP) prepared guidance ("ISOO-DOJ Guidance") that was attached to the Card Memorandum to assist the information reviewing process. The ISOO-DOJ Guidance examines three levels of sensitivity for government information and the corresponding steps necessary to safeguard that information. These are: 1) Classified Information; 2) Previously Unclassified or Declassified Information; and 3) Sensitive but Unclassified Information. The guidance also reminds departments and agencies to process FOIA requests for records containing WMD or national security information in accordance with Attorney General John Ashcroft's FOIA Memorandum ("Ashcroft Memorandum") of October 12, 2001, by giving full and careful consideration to all applicable FOIA exemptions.

The Card Memorandum directed each department and agency to report its findings directly to the Office of the White House Chief of Staff or the Office of Homeland Security no later than 90 days from the date of the Memorandum. Agencies and departments were also instructed to contact the Department of Energy's Office of Security for assistance in determining the classification of nuclear and radiological weapons information under the Atomic Energy Act, and to contact the Justice Department's Office of Information and Privacy for assistance in applying exemptions of the Freedom of Information Act (FOIA) to sensitive but unclassified (SBU) information.

The National Security Archive ("Archive") made FOIA requests to each of thirty-five (35) federal agencies, departments and offices. The 35 agencies included the 25 agencies surveyed by the Government Accountability Office (GAO) in its 2001, 2002, and 2003 reports regarding administration of FOIA. These agencies account for an estimated 97% of all FOIA requests government-wide. The Archive also submitted FOIA requests to ten (10) additional agencies and components to which the Archive frequently submits FOIA requests. Each FOIA request asked for:

> **All records, including but not limited to guidance or directives, memoranda, training materials, or legal analyses, concerning the March 19, 2002 memorandum issued by White House Chief of Staff Andrew Card to the heads of all federal departments and agencies regarding records containing information about Weapons of Mass Destruction (WMD). Attached with this memo was a supporting memorandum by the U.S. Department of Justice and Information Security Oversight Office.**

With one exception, all requests were faxed to the central FOIA processing office of each department or agency on January 8, 2003.[10] The 20-business day statutory time limit for a substantive FOIA response expired on February 5 or 6, 2003. On February 7, 2003, after 21 or 22 business days had expired, appeals were filed with 30 agencies that had not substantively responded to the requests. The Chart presented in Appendix I summarizes agency processing times and information releases.

© 2006, The National Security Archive

POLICIES ON PROTECTION OF SENSITIVE UNCLASSIFIED INFORMATION

The Archive submitted FOIA requests to each of 43 different federal agencies, departments, and offices. This survey included the 25 agencies examined by the Government Accountability Office (GAO) in its annual reports; the agencies considered by the GAO represent an estimated 97% of all FOIA requests. We selected ten additional agencies and components to which the National Security Archive submits a substantial number of FOIA requests each year, as well as eight agencies that we believed, because of the nature of their functions, might play an important role in the protection of sensitive unclassified information. Each request sought:

> **All documents including, but not limited to, directives, training materials, guides, memoranda, rules and regulations promulgated on and after January 1, 2000, that address the handling of,**
> **"sensitive but unclassified," (SBU)**
> **"controlled unclassified information," (CUI)**
> **"sensitive unclassified information," (SUI)**
> **"sensitive security information," (SSI)**
> **"sensitive homeland security information," (SHSI)**
> **"sensitive information," (SI)**
> **"for official use only," (FOUO)**
> **and other types and forms of information that, by law, regulation or practice, require some form of protection but are outside the formal system for classifying national security information or do not meet one or more of the standards for classification set forth in Executive Order 12958 as amended by Executive Order 13292.**

The requests were faxed to the central FOIA processing office of each agency or department on February 25, 2005. In some cases separate requests were submitted to component agencies that may have occasion to independently safeguard unclassified information. The 20-business day statutory time limit for a substantive FOIA response expired on March 25, 2005. The chart presented in Appendix III summarizes agency processing times and information releases.

Agency responses were examined for:

- Authority (statutory or internal) for the policy;
- Definition and guidance;
- Power to designate protected information;
- Power to remove designation;
- Government employees' access to information;
- Physical protections for information;
- Limitations on use of designation;
- Relation to or effect on Freedom of Information Act (FOIA) policies.

Each of the above categories corresponds with the explanatory sections below (*see* **Findings**). The constraints of this Report format do not allow the details of each agency policy to be communicated; instead, we have drawn generalized findings based on an overall review and used specific aspects of agency responses as examples or case studies within our broader discussion. The complete documentation of each agency's response is available on file with the National Security Archive, http://www.nsarchive.org.

What Is Sensitive Unclassified Information?

This study is focused solely on security sensitive information that does not meet the standard for classification or, for some other reason, is not classified in accordance with Executive Order 12958 (as amended by E.O. 13292). When referring generally to the category of policies examined in this Study, rather than a specific agency policy (the names of which are denoted in **bold text**), we use the term "sensitive unclassified information" policies. Because of the number of policies and the extent to which they overlap–some use the same terminology but differ in substance–this is used as a generic phrase, as it incorporates the two common elements (the claimed sensitivity of the information and its unclassified

© 2006, The National Security Archive

nature). We include as "security"-related concerns those potential harms related to national security or law enforcement, as well as protection of other information the release of which may impair the functioning of the government.

What Is Not Sensitive Unclassified Information?

The web of government information control policies and practices is vast and complex. As this Study makes clear, many documents may potentially fall into multiple categories or be marked with more than one type of restriction. For purposes of clarity and focus, this Study examines specifically those policies aimed at controlling unclassified information for purposes of security. This category of information overlaps substantially with what are often referred to as "dissemination control markings"[11] or routing guidelines. Such markings may be applied to either classified or unclassified information, and serve the purpose of directing *where* a given document may go and *who* may receive it, rather than characterizing the substantive content of the document.

Examples of these "caveats" or "special handling designations" used by the Department of Defense and exclusively applicable to classified information include: ATOMAL (containing atomic materials); NATO (NATO classified information); and SIOP-ESI (Single Integrated Operations Plan-Extremely Sensitive Information) and other SPECAT (Special Category) designators.[12] The Department of State and several other agencies recognize markings specifically prescribing distribution restrictions for the document, including: EXDIS ("exclusive distribution to officers with essential need to know"); LIMDIS ("distribution limited to officers, offices, and agencies with the need to know, as determined by the chief of mission or designee"); NODIS ("no distribution to other than addressee without approval of addresser or addressee. NODIS is used only on messages of the highest sensitivity between the President, the Secretary of State, and Chiefs of Mission.");[13] and NOFORN ("intelligence which . . . may not be provided in any form to foreign governments, international organizations, coalition partners, foreign nations, or immigrant aliens without originator approval.")[14]

NOTES ON FINDINGS

The Study's findings are qualified on a number of grounds. First, there are limitations to the method of requesting documents under the FOIA. The Archive cannot be certain that every relevant office was searched, that every responsive document was found, or that all the data on these issues was released. The wide range of responses received suggests that there almost certainly are additional responsive documents that were not provided to the Archive.

Second, as to the sensitive unclassified information policies presented in this Study, in the majority of cases, we were unable to determine to what extent these policies have affected agency practice. Due to the amorphous, decentralized, and generally unmonitored nature of policies controlling unclassified information, it is impossible to discern how many employees in a given agency are using the policy and how much information has been designated for protection or withholding under the policy. Some inferences can be drawn in cases where the means of dissemination of a given policy can be discerned, but this was not possible with the material provided by most agencies.

Third, as of today, 258 business days since submission of the FOIA request for documents on sensitive unclassified information policies, only 32 agencies out of 42 surveyed (or approximately 76%) have responded, but only 20 or 48% have provided responsive documents. In some cases, such policies are created by statute or have been pronounced publicly as agency policy. Therefore, the agency FOIA responses were supplemented with research based on publicly-available materials. Thirty-three out of 35 agencies surveyed (approximately 91%) have responded to our Card Memorandum request, but over 750 business days have passed since those requests were submitted.

Finally, there are many different tallies of the total number of sensitive unclassified information policies. Several attempts have been made to measure the volume of distinct designations used to protect unclassified information, but each organization has employed its own approach and, in particular, its own interpretation of how the boundaries of the category should be defined. In 1972, a study commissioned by the House Government Operations Committee revealed 63 separate "control labels" used by various federal agencies; however, a number of the labels included in that count are applied only as an additional safeguard to classified information–for example, Restricted Data, Siop-Esi ("Single integrated operational plan–extremely sensitive information"), and Noforn ("No foreign distribution"). Further, at least eight of the

© 2006, The National Security Archive

agencies included in that survey are no longer in existence, and others are small agencies that were not included in this Study.

A more recent quantification of sensitive unclassified information policies was completed by OpenTheGovernment.org as part of their Secrecy Report Card 2005.[15] OpenTheGovernment.org referred to 50 "restrictions on unclassified information"; included in this count, however, are the nine defined exemptions under the Freedom of Information Act, as well as several other restrictions that were not reported by the agencies surveyed for this Study or that do not clearly qualify as either distribution or control markings–for example, protective measures in place under the Export Administration Regulations and restrictions applied to Grand Jury Information under the Federal Rules of Criminal Procedure. Once again, for this Study we considered principally the information and policies provided by the agencies in response to FOIA requests. The deviations as to the total number of policies exhibits two conclusions about the state of sensitive unclassified information regulation–namely, that these diverse policies are not clearly set out by the agencies or publicly available, and that there is even misunderstanding and disagreement within agencies about the nature and application of the policies.

© 2006, The National Security Archive

FINDINGS

CARD MEMORANDUM AND PROTECTION OF UNCLASSIFIED HOMELAND SECURITY INFORMATION

Of the 35 FOIA requests, the Archive received 24 responses with documents. Nine departments responded that their searches yielded "no records." Finally, two departments (USAID and CIA) have not provided any formal response to the Archive's initial request after more than three years nor formally responded to administrative appeals based on their non-responsiveness. Surprisingly, seven agencies apparently did not provide a report back to Mr. Card despite his explicit direction to prepare such a report. The agency response times ranged from 9 to 702 business days. A summary of the agency processing times and document releases is attached in Appendix I.

Each agency that provided records indicated taking some action in response to the Card Memorandum and/or the ISOO-DOJ guidance. A summary of the agencies responses to the Card Memorandum is attached in Appendix II and the agencies complete responses are available on our Web site at http://www.nsarchive.org. Overall, the Card Memorandum appears to have resulted in increased withholding of information, both in the form of information removal from Web sites and increased emphasis on using FOIA exemptions. Some of the new security measures put into place at agencies, including Web site policies, appear to have been long overdue and are likely to increase the security of sensitive information.

REVIEW OF RECORDS FOR WMD OR OTHER SENSITIVE INFORMATION

At a minimum, responsive departments and agencies provided records indicating that they reviewed their records and identified whether they held WMD information. Some departments conducted much more expansive searches to identify a far broader range of potentially sensitive information, including "Sensitive Homeland Security Information" (SHSI), classified information, "Safeguard Information," "potentially sensitive information," and "other information that could be misused to harm the security of [the] nation or threaten public safety."

WEB SITE INFORMATION REMOVAL

At least ten agencies indicated that they removed information from their Web sites or blocked access to their Web sites. Several departments and agencies reported identifying WMD information, national security, and public safety information on their public Web sites. The common reaction by these departments and agencies upon identifying this information was to immediately remove the information or begin the bureaucratic process of removing it. This number almost certainly underestimates the number of agencies that removed data from Web sites post-September 11, as many agencies, such as the Nuclear Regulatory Commission, began closing access to online information prior to receiving the Card Memorandum.

Individual approaches to identifying information on Web sites and making the decision to remove the information varied. A few responses indicated that special task forces or teams were created to inventory Web sites, identify sensitive information on the sites, and to assess whether the information should be removed. Some agencies had teams immediately remove all sensitive information from public Web sites and then either used those same teams or other individuals, including FOIA officers or other authorized personnel, to determine what information could be reposted. Additionally, a number of agencies created specific protocols or policies for posting future potentially sensitive content on public Web sites.

Some agencies used the review as an opportunity to increase cyber-security by installing firewalls, conducting vulnerability scans on Web sites, and enhancing access restrictions.

© 2006, The National Security Archive

Increased Emphasis on Using Applicable FOIA Exemptions

At least 16 of the 24 agencies that responded provided records that demonstrated an increased emphasis on using FOIA exemptions to withhold information. Several agencies that would be expected to hold or handle WMD or other sensitive information emphasized to FOIA officers that they should use careful consideration in determining the applicability of all FOIA exemptions when processing a request for sensitive information, often citing verbatim the language and instruction of the ISOO-DOJ guidance. For example, the Office of Security in the Energy Department generated: a list of "Subject Area Indicators and Key Word List for Restricted Data and Formerly Restricted Data" and an "Interim Guide for Identifying Official Use Only Information." These lists include scientific terms, sites, or organizations associated with Restricted Data and Formerly Restricted Data, frequently encountered names of people involved in Nuclear Weapons Programs, and "possible markings." These lists presumably will be used by FOIA officers to help determine the applicability of FOIA exemptions to records containing one or more of the words on the lists. The "Interim Guide" emphasizes usage of all FOIA exemptions and offers examples of situations in which a particular FOIA exemption could be applied.

In addition, some agencies either employed additional review of FOIA requests or developed new procedures. For example, a joint DOD response indicates a decision that any Chemical, Radiological, Biological, and Nuclear (CBRN) is found subject to declassification, then it must be approved by Washington Headquarters Services, Directorate of Freedom of Information and Security Review (WHS/DFOISR). DFOISR planned to issue a change to DoD Directive 5230.29 to require CBRN to be referred to DFOISR before public release of such information.

Several agencies implemented ongoing training programs or training sessions for FOIA officers to ensure future compliance with the ISOO-OIP Guidance.

Only two agencies provided statements to balance out any increased emphasis on withholding. In a memorandum disseminating the Card Memorandum and ISOO-OIP Guidance, the EPA informed its offices that no EPA policies were changed as a result of the memoranda and indicated that EPA offices should recognize both the risks and the benefits of disclosure. Similarly, DOD provided records indicating that safety should be considered alongside the benefits associated with the free exchange of information.

Implementing New Security and Safeguarding Measures

Several agency responses indicated that the agencies implemented new security and safeguarding measures. For example, the Department of Agriculture commenced parallel in-house and external reviews of its most sensitive research laboratories, with a major focus of the reviews being "human reliability" and "information security." In addition, the Department "ramped up" its department-wide personnel security and information security programs by "increasing the budget for personnel security investigation and adjudications several-fold" and "drafting an updated departmental regulation on protecting national security information."

Dissemination of Card Memorandum

Agencies that would not be expected to handle WMD information or other sensitive information, in some cases, simply forwarded the Card Memorandum and the ISOO-DOJ guidance to its FOIA offices in a "for your information" manner.

No Records or No Response

Nine agencies responded that they held no documents responsive to the Archive's FOIA request. Those agencies include: (1) Social Security Administration; (2) Office of Management and Budget; (3) Department of Housing and Urban Development; (4) Department of Health and Human Services (HHS); (5) Federal Bureau of Investigation (FBI); (6) Department of Education; (7) Defense Intelligence Agency (DIA); (8) Office of Personnel Management (OPM); and (9) Central Command (CENTCOM). Since the Card Memorandum *required* each agency to submit a report to either the Office of the White House Chief of Staff or to the Office of Homeland Security, these agencies either failed to release their reports to the Archive or failed to submit the report requested by Mr. Card. Two agencies, CIA and AID, have not provided any substantive response, despite administrative appeals by the Archive.

© 2006, The National Security Archive

For those agencies that do not deal with military or intelligence issues, it is not surprising that the Card Memorandum did not result in much activity, including possibly the failure to submit a formal response to the White House Chief of Staff or the Office of Homeland Security. Other "no records" responses raised questions, however. For example, although HHS reported holding no documents responsive to the Archive's request, the HHS Web site shows that the department, particularly through the Center for Disease Control (CDC), disseminates information regarding biological, chemical, and radiological weapons.

AGENCY CONTROL OF SENSITIVE UNCLASSIFIED INFORMATION

AUTHORITY FOR POLICY

The agencies and departments examined in this study present a broad range of varied approaches to protecting information that is not subject to security classification. The authority for these diverse policies ranges from an agency's inherent information management authority to specific statutory direction. It is striking to note the multiplicity of policies and terms that agencies have created internally to apply to unclassified information, as compared to the relative simplicity and perceptible origins of statutorily-authorized policies. The "patchwork quilt" of guidelines related to sensitive unclassified information is made up primarily of squares sewn with agency—rather than congressional—threads.

I firmly believe that never before have we had such a clear and demonstrable need for a seamless process for sharing and protecting information, regardless of classification. Yet in many ways, we are not only continuing the current 'patchwork quilt' but we are quite possibly adding new seams every day.
– J. William Leonard, ISOO Director[44]

Agency-Originated Policies

Of the 37 agencies surveyed (both by way of responses to our requests as well as by outside research, see chart at Appendix III), 24 follow one or more different internally-generated policies (in some cases, an internal agency policy statement will draw on the definition and criteria in a statute or another agency's policy) to protect information that is considered "sensitive" for security reasons. In general, because of their less formal nature, these policies are less restrictive in terms of which employees or officials may mark sensitive information and are more expansive in terms of what information may potentially be covered. Definitions tend to be less precise or concrete in their application than statutorily-authorized policies.

24 out of 37 of agencies and departments analyzed (65%) protect certain types of unclassified information originating within the agency according to *internal* policies, procedures, or practices.

Some of the materials provided regarding these agency-generated policies consist of formal orders or directives establishing agency policy and procedures; in other cases, particularly those agencies that have little involvement in security matters, the policies are contained within employee handbooks or manuals, or even training materials such as pamphlets and Power Point presentations assumedly targeted to provide essential but simplified background to new employees or security trainees. Unfortunately, it is impossible to reach any conclusions as to the extent of use or dissemination of the policy based on the form or content of these documents.

It is clear from the multiplicity of internal policies that there has been no coordination among agencies as to the content of the policies. This is also particularly evident in the fact that many of the agencies use the same terms or markings for their policies, but control, monitor, and release designated documents according to very different guidelines.

© 2006, The National Security Archive

AGENCY-ORIGINATED POLICIES	
Agency	Policy
Agency for International Development (AID)	Sensitive But Unclassified (SBU)
Centers for Disease Control (CDC) *	Sensitive But Unclassified (SBU)
Citizenship and Immigration Services (CIS) *	Sensitive But Unclassified (SBU) [DHS]
Customs and Border Protection (CBP) *	Sensitive But Unclassified (SBU) [DHS]
Department of the Air Force ("Air Force") *	For Official Use Only (FOUO) [DOD]
	Computer Security Act Sensitive Info [DOD]
Department of Agriculture ("USDA")	Sensitive Security information (SSI)
Department of the Army ("Army") *	For Official Use Only (FOUO)
Department of Defense (DOD) *	For Official Use Only (FOUO)
Department of Energy (DOE)	Official Use Only (OUO)
Department of Homeland Security (DHS)	Sensitive But Unclassified (SBU)
Department of Justice (DOJ)	Limited Official Use (LOU)
Department of State (DOS)	Sensitive But Unclassified (SBU)
Department of the Treasury ("Treasury")	Sensitive But Unclassified (SBU)
Drug Enforcement Agency (DEA)	DEA Sensitive
Environmental Protection Agency (EPA)	Confidential Agency Information (CAI)
	Confidential Business Information (CBI)
	Enforcement-Confidential Information (ECI)
Federal Aviation Administration (FAA)	For Official Use Only (FOUO)
General Services Administration (GSA)	Sensitive But Unclassified Building Info
Immigration and Customs Enforcement (ICE) *	Sensitive But Unclassified (SBU) [DHS]
National Aeronautics and Space Admin. (NASA)	Administratively Controlled Info (ACI)
National Geospatial-Intelligence Agency (NGA)	For Official Use Only (FOUO) [DOD]
National Reconnaissance Office (NRO)	For Official Use Only (FOUO)
National Science Foundation (NSF)	Sensitive Information
Nuclear Regulatory Commission (NRC)	Official Use Only (OUO)
	Proprietary Information (PROPIN)
Transportation Security Administration (TSA)	Sensitive But Unclassified (SBU) [DHS]

* The information was not provided by this agency, but rather is based on independent research or materials submitted by other agencies.

Statutory and/or Regulatory Policies

Of the agencies analyzed, eight follow one or more statutory guidelines applicable to unclassified information. Two of these agencies–the Department of Energy and the Nuclear Regulatory Commission–have long-standing policies, based on the Atomic Energy Act of 1954. The remaining statutory policies were created or restructured from previous enactments by the Homeland Security Act of 2002. They include:

8 out of 37 agencies (22%) analyzed have policies that are authorized *by statute* and implemented *by regulation*.

Authorization for 2 policies is derived from the Atomic Energy Act of 1954; 5 rely on the Homeland Security Act of 2002, and 3 are based on other statutory pronouncements or regulatory authority.

- Sensitive Security Information (SSI)

  Sensitive Security Information (SSI) related to civil aviation has been statutorily safeguarded for more than three decades under the Air Transportation Security Act of 1974. It was initially intended to prevent airplane hijackings. These provisions have been expanded under the Homeland Security Act. New authority to withhold information has been extended to the Under Secretary of Transportation for Security and authority has been extended to the TSA and the DHS. The **SSI** restrictions

© 2006, The National Security Archive

are now applicable to all transportation information and to maritime-related security information under the jurisdiction of the Coast Guard.

- Protected Critical Infrastructure Information (PCII)

  The Department of Homeland Security (DHS) issued regulations in 2004 based on provisions of the Homeland Security Act, creating its Protected Critical Infrastructure Program. The program applies to **"critical infrastructure information" (CII)**—information "not customarily in the public domain and related to the security of critical infrastructure or protected systems," which, if sabotaged, attacked, or otherwise impeded, would result in the incapacitation of interstate commerce, national security, or public health or safety—that is voluntarily submitted to DHS by private sector entities. A new office established within DHS will handle applications connected to the submission of **CII**, and will grant **PCII** status if certain conditions are met; once designated as **PCII**, this information will be withheld on FOIA exemption 3 grounds.[16]

- Sensitive Homeland Security Information (SHSI)

  The 2002 Act defines **"homeland security information" (HSI)** as "Any information possessed by a Federal, State, or local agency that (A) relates to the threat of terrorist activity; (B) relates to the ability to prevent, interdict, or disrupt terrorist activity; (C) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (D) would improve the response to a terrorist attack."[17]

  The President is granted authority to safeguard homeland security information—that which is classified as well as that which he deems to be "sensitive but unclassified." The statute outlines the ways in which this type of information should be shared among federal, state, and local officials and personnel, including in particular, "[w]ith respect to information that is sensitive but unclassified, entering into nondisclosure agreements with appropriate State and local personnel."[18]

  President Bush delegated to the Secretary of Homeland Security the task of promulgating procedural regulations to comply with the statutory provisions. DHS has yet to issue formal proposed regulations implementing the SHSI provisions of the Homeland Security Act.

STATUTORY POLICIES		
Agency	Policy	Statutory/Regulatory Authority
AIR	Sensitive Information	Computer Security Act of 1987, P.L. 100-235
DHS	Sensitive Security Information (SSI)	49 U.S.C.A. § 40119 49 C.F.R. § 1520.5
	Protected Critical Infrastructure Information (PCII)	Homeland Security Act of 2002, 6 U.S.C.A. § 131 6 C.F.R. § 29
DOD*	Unclassified Controlled Nuclear Information (UCNI)	10 U.S.C.A. § 128 32 C.F.R. § 223
	Sensitive Information	Computer Security Act of 1987, P.L. 100-235
DOE	Unclassified Controlled Nuclear Information (UCNI)	Atomic Energy Act of 1954, 42 USCA § 2011 10 C.F.R. §1017.7
FAA/ DOT	Sensitive Security Information (SSI)	Air Transportation Security Act of 1974 Homeland Security Act of 2002, 6 U.S.C.A. § 101 49 C.F.R. Part 15.5
NRC	Safeguards Information (SGI)	Atomic Energy Act of 1954, 42 USCA § 2167 10 C.F.R. § 73.21
TSA	Sensitive Security Information (SSI)	49 U.S.C.A. § 40119 49 C.F.R. § 1520.5
	Protected Critical Infrastructure Information (PCII)	Homeland Security Act of 2002, 6 U.S.C.A. § 131 6 C.F.R. § 29

* The information was not provided by this agency, but rather is based on independent research or materials submitted by other agencies.

© 2006, The National Security Archive

No Policies

Most of the agencies that interact on an individual level with the citizens they serve do not maintain SBU or similar information-control policies. In other cases, those agencies that deal extensively with the federal budget and other matters that are generally part of the public domain would not have a need for such a policy.

11 of the agencies that responded provided *no documents* showing a policy for protecting security-related sensitive information. They include:

- Social Security Administration (SSA)
- Small Business Administration (SBA)
- Office of Management and Budget (OMB)
- Federal Emergency Management Agency (FEMA) – *Fwd. to DHS*
- Department of Housing and Urban Development (HUD)
- Office of Personnel Management (OPM)
- National Institutes of Health (NIH)
- Department of Commerce ("Commerce")
- National Archives and Records Administration (NARA)
- Department of Veterans' Affairs (VA)
- Federal Bureau of Investigation (FBI)

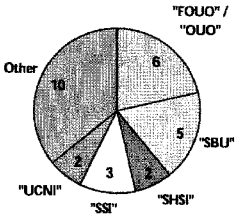
DEFINITION AND GUIDANCE

This Study analyzed the specificity and extent of guidance given to individuals who are to designate or mark protected information under the policy. The research revealed 28 *distinct* policies related to sensitive unclassified information,[19] and the various policies were grouped according to what type of definition or guidance was provided in the policy statement

This Study examined 28 *distinct* policies prescribing treatment of sensitive unclassified information.
Of these 28 policies:

- 6 refer to protected information as "For Official Use Only" (FOUO/OUO);
- 5 as "Sensitive But Unclassified" (SBU);
- 2 as "Sensitive Homeland Security Information" (SHSI);
- 3 as "Sensitive Security Information" (SSI); and
- 2 as "Unclassified Nuclear Information" (UCNI).

Sensitive Unclassified Information
Labels, 28 Distinct Agency Policies



or other procedural document. The definitional features considered were whether the policy relies on a broad/specific definition; delineated categories/criteria of information to be protected (broad or specific); examples of agency-specific materials to clarify either a definition or set of categories; and any other statutory guidance to which the policy refers, for example, one or more of the nine exemptions under FOIA, 5 U.S.C. §552(b). See charts, Appendices IV and V.

The degree of guidance offered is an essential consideration in our analysis of these policies because it shows to what extent government officials (and, in some cases, low-level employees) are constricted in their decision to mark information for protection. Facing challenges to its SSI policy in 2004, the TSA Internal Security Policy Board concluded: ". . . [E]xacting specificity with respect to what information is covered and what is not covered. . . . could be documented in a classification guide type format because imprecision in this area causes a significant impediment to determining SSI. Experience has shown that employees unsure as to what constitutes SSI may err on the side of caution and improperly and unnecessarily restrict information, or may err inappropriately and potentially disastrously on the side of public disclosure."[20]

"Sensitive but unclassified information is a very imprecise term that has more often than not been misunderstood. It might refer to information that should be protected from public disclosure, or should be safeguarded, or both."
- I. William Leonard, ISOO Director[21]

© 2006, The National Security Archive

More constrained, specific policy guidance—as opposed to broad, general criteria or categories—allows for only a narrow range of interpretation and prevents misunderstanding or abuse of the policy.

In comparison to the strict, detailed principles of the national security classification regime, the formal categories and criteria in protective markings for unclassified materials are often sparse, inconsistent, and ambiguous. Because, as ISOO Director J. William Leonard has highlighted, "[t]here is no underestimating the bureaucratic impulse to 'play it safe' and withhold information,"[21] the poor guidance in many cases may presage poor decision-making, or at least increase the likelihood that secrecy by default will become the rule rather than the exception.

FOIA-Based Definitions

In a number of agencies, FOIA exemptions two through nine are transposed into sensitive unclassified information policies by way of definition. The potential for conflating the statutorily defined FOIA exemptions with broader notions about potentially sensitive information is significant. For instance, the State Department manual, 12 FAM 540, defines SBU as "information which warrants a degree of protection and administrative control that meets the criteria for exemption from public disclosure set forth under . . . the Freedom of Information Act and the Privacy Act." The provision goes further to illustrate what information is covered, explaining: "**SBU** information includes, but is not limited to . . . [m]edical, personnel, financial, investigatory, visa, law enforcement, or other information which, if released could result in harm or unfair treatment to any individual or group, or could have a negative impact upon foreign policy or relations."

Other FOIA-based definitions—the Department of Defense **FOUO** information, for example—expressly limit protected information to that which is subject to withholding under the FOIA exemptions. The problem with this approach is that the goal of FOIA is disclosure, while the goal of SBU-type policies is information safeguarding or non-disclosure. It is important that sensitive unclassified information designations not be seen as determinant of FOIA releasability, particularly because FOIA release decisions for the same documents may change over time. Especially where these policies can be invoked by *any employee*, it is acutely important that their scope and purpose be limited to avoid potential misuse and excessive secrecy. The one benefit of FOIA-based definitions, however, is that there are statutory definitions and a body of administrative and public law interpreting those definitions. Nonetheless, it remains imperative that FOUO not be considered a FOIA exemption.

Definitions Versus Categories

In most cases, agency policies include a definition, which is often broad or circular in terms of describing the information to be protected. For example, the Department of Justice authorizes selected personnel to designate agency information as **"Limited Official Use" (LOU)**; **LOU** is defined as "[u]nclassified information of a sensitive, proprietary or personally private nature which must be protected against release to unauthorized individuals." (DOJ 2620.7). Like a number of other agencies, DOJ's policy lists the types of information that fit under this definition, some very narrow and statutorily defined—for example, Grand Jury information and Privacy Act-protected information—and some vague and open-ended—"Reports that disclose security vulnerabilities" and "Information that could result in physical risk to individuals."

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. 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."
– JASON Program Office, MITRE Corp.[22]

Several other policies describe sensitive information broadly in terms of national security or general governmental interests. DHS permits *any employee* (the agency is now the largest in the Federal Government, with more than 180,000 employees) to mark a document "FOR OFFICIAL USE ONLY" if they consider that its contents "could adversely impact . . . the conduct of Federal programs, or other programs or operations essential to the national interest." This directive is further clarified with 9 sub-categories, including, among others: "Information that could be sold for profit";

© 2006, The National Security Archive

"Information that could constitute an indicator of U.S. government intentions, capabilities, operations, or activities or otherwise threaten operations security"; and "Developing or current technology, the release of which could hinder the objectives of DHS, compromise a technological advantage or countermeasures, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system." (DHS Management Directive 11042.1)

Some of the policies surveyed for this project, to their credit, offer extremely narrow and well-delineated categories, such that it would be very difficult for employees applying the policy to mistakenly conclude that a document does or does not need protection. The Nuclear Regulatory Commission, in an internal memo to senior officials, directs that Safeguards Information must be withheld from public release; the guidance includes such materials related to nuclear facilities as: "Site-specific drawings, diagrams, sketches, or maps that substantially represent the final design features of the physical protection system"; "Details of the onsite and offsite communications systems"; "Lock combinations and mechanical key design"; "Size, armament, and disposition of onsite reserve forces"; and "Schedules and itineraries for specific shipments."

It is relevant to note that NRC's SGI policy has been in effect since 1981 (although the agency proposed new regulations in February 2005 that would expand the existing definition). This change would add a new category of Safeguards Information-Modified Handling (SGI-M) to cover many security and emergency planning procedures and particular types of safety assessments regarding nuclear facilities. This example exhibits the problematic though critical difference between information control procedures before and after September 11: namely, the United States has recognized the extent of its ignorance about the precise threat posed by terrorists and through what means a potential future strike might occur. Given this uncertainty, the Government has thrown an increasingly wide net of protection over information in the hope that the right secrets will be kept to avert another attack.

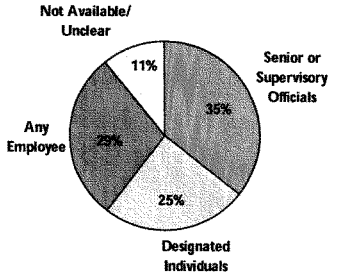
"[T]hose making SSI designation . . . should have special training, much as FOIA officers do, because they are being asked to make difficult balancing decisions among competing values. All of us value security, but any security gained from the regulations is of considerably less comfort if it comes with a loss of faith and confidence in our local, state and national governments to safeguard our other values."
- Coalition of Journalists for Open Government[xiv]

DESIGNATION AUTHORITY

Each agency policy was examined for how it delegates the authority to determine what is (and what is not) protected material. In a handful of cases, the policies were distressingly ambiguous or did not explicitly delegate this role to any particular individuals. It may be that further procedural or practical steps taken by the agencies in this regard are not reflected in the documentation provided. When a policy was ambiguous in a way that suggested intentional breadth and was apparently intended to target a broad, agency-wide audience, this Study concludes that any agency personnel has the authority to act according to its dictates.

Clearly, individuals who are authorized to designate (rather than just to view or possess) materials as protected have great power in terms of the impact of the policy, both for dissemination of information within the agency or the government (information sharing) and access of the public to government information. In particular, with the newest policies–those instituted or revamped since September 11–more agencies are ambiguous in their selection of responsible employees. Other agencies explicitly have assigned the designation role, but to a group of employees that is arguably so large as to make training or oversight impractical unless directed at the entire agency staff.

Authority to Designate Protected Information



Recently, during consideration of the Department of Homeland Security Appropriations Act, 2006, the congressional Conference Committee specifically addressed

© 2006, The National Security Archive

the use of the **Sensitive Security Information (SSI)** designation, particularly within components of DHS including the Transportation Security Administration (TSA). In its report, the Committee stated:

> The conferees are concerned that because of insufficient management controls, information that should be in the public domain may be unnecessarily withheld from public scrutiny. The conferees require the Secretary to ensure that each appropriate office has an official with the clear authority to designate documents as **SSI** and to provide clear guidance as to what is **SSI** material and what is not.[22]

The solution that the congressional committee proposes–requiring each office, department, or division to select a single individual to whom they delegate the responsibility of marking, reviewing, and disseminate those documents that are "sensitive" or otherwise protected–is one that seven (7) agencies already follow.

Several other agencies have taken an approach that is effectively a two-step process for designation. A senior-level official or other designated authority will first have the task of implementing the stated policy and by indicating particular *categories* or *types* of information that should be protected within the agency or department. Based on this list of specific criteria that constrain decision-making, other employees will then be able to mark and protect particular information they produce according to the guidelines. The **Department of Homeland Security's FOUO** policy takes this approach. The DHS policy has been widely criticized for its breadth, but in actuality may be more nuanced in its controlled application: "Any DHS employee, detailee, or contractor can designate information falling within one or more of the categories cited. . . . Officials occupying supervisory or managerial positions are authorized to designate other information, not listed above and originating under their jurisdiction, as FOUO." (DHS MD 11042.1). The clarity of the stated categories is debatable, as noted above, but they undoubtedly narrow a much larger scope of information that could fall within the definition of FOUO and avert the potentiality of haphazard, unguided application that might otherwise exist.

Similarly, the Department of Energy (DOE) has written its policy in such a way that the terms can evolve based on high-level guidance as the agency's needs change over time. The **DOE OUO** policy includes as a responsibility of both Secretarial Officers and the Director of the Office of Security to issue guidance "to assist individuals in determining whether a document contains **OUO information**." Employees may mark a document from their office as **OUO** if they determine that "the information has the potential to damage governmental, commercial, or private interests if disseminated to persons who do not need the information to perform their jobs or other DOE-authorized activities"; *and* if the information contained therein either is specifically identified as **OUO** information under the official guidance *or* if they believe the information otherwise qualifies for protection under FOIA exemptions 2 through 9.

AUTHORITY TO *DESIGNATE* PROTECTED INFORMATION	
Senior or supervisory officials **10 of 28 (35%)**	ACI/NASA ("originating NASA management official") DEA Sensitive ("senior official") FOUO/FAA ("FAA managers") OUO/NRC ("Branch chiefs and above" and contractor-appointed) SBU/State ("US citizen direct-hire supervisory employees") SSI/DOT SGI/NRC ("Branch chiefs and above") SSI/USDA ("Heads of Departmental Organizations") UCNI/DOD ("Heads of DoD components") Unclassified Technical Info/DOD
Designated individuals **7 of 28 (25%)**	LOU/DOJ ("designate[d] subordinate officials") PCCI/DHS SASI/HHS SBU/CDC ("Document control officers") SHSI/FAA ("SHSI Program Officer") SHSI/NRC (staff assigned as "points of contact" for SHSI) UCNI/DOE ("Reviewing Official")

© 2006, The National Security Archive

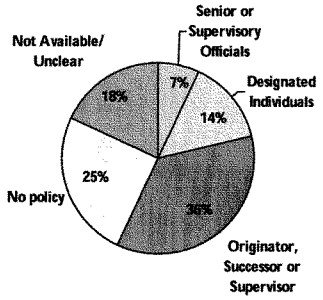
Any employee 8 of 28 (29%)	CAI/EPA ("originator or information manager") CBI/EPA ("originator or information manager") ECI/EPA ("originator or information manager") FOUO/DHS ("An y DHS employee, detailee, or contractor") FOUO/DOD FOUO/NRO ("Originator of info") OUO/DOE ("Any Federal or contractor employee" originating/controlling document) SBU/GSA
Not available / unclear 3 of 28 (11%)	Computer Security Act Sensitive/DOD PROPIN/NRC WMD/State

DECONTROL AUTHORITY

This Study inquired as to whether each policy sets forth a procedure for removing a protective marking or otherwise sharing or disseminating the information after it has previously been controlled under one of the subject policies. In addition, whether or not such a process was outlined, this Study looks at whether the policy identifies an individual or individuals authorized to effectively erase a protective stamp from a sensitive unclassified document and thereby release it from safeguarding measures.

The comparison between the identification of a designating authority and of decontrol authority speaks loudly as to the breadth and indeterminate nature of these policies. In fact, the contrast proves stark. While only three out of 28 policies (11%) *do not* clearly identify specific authority to designate information for protection, 12 of the same 28 policies (43%) either were examined in their entirety and clearly provided no guidance on decontrol or were incomplete or ambiguous as to establishing a decontrol procedure or authority. Further, although several agencies name individuals responsible for decontrol, none has mandatory review or tracking policies for decisions to protect unclassified information, and only one has a time limit (USDA, 10 years) and few have other restrictions on the use of these designations. In a majority of agencies, the only opportunity for review of a document designated for protection is when the information is requested under the FOIA. At this point, there are different procedures for how an agency will handle such a request, which will be discussed below.

Authority to Decontrol Protected Information



Some of the policies designate a removal authority–in many cases limited to the individual who placed the original designation (or his or her successor or superior). Without any mandated review, however, any examination or removal of markings (whether by the document's originator or other specified authority) will inevitably be completed in a haphazard manner. NASA's **Administratively Controlled Information (ACI)** policy, for example, states that the "[o]fficial who originally designated material as ACI (or successor or superior) are responsible for prompt removal of restricted markings when the necessity no longer exists." Without knowing the extent of the paper that one individual official may imprint with the "ACI" stamp on a daily basis but considering the nature of the federal bureaucracy, one questions how an already-burdened NASA management

© 2006, The National Security Archive

official will be capable of paging through his or her filing cabinets to make sure the status of each document has not changed.

The least common approach is to follow the pattern of the classification system, mandating a maximum duration for protective marking. At USDA, "[i]nformation shall not remain protected as **SSI** when it ceases to meet the criteria established in sections 6.b of this regulation. Information ordinarily should remain protected as **SSI** for no longer than 10 years, unless a designating official makes a new determination the protection is warranted for a longer period." (USDA, DR 3440-2).

AUTHORITY TO *DECONTROL* PROTECTED INFORMATION	
Senior or supervisory officials 2 of 28 (7%)	SSI/USDA, *maximum 10 years* Unclassified Technical Info/DOD
Designated individuals 4 of 28 (14%)	PCCI/DHS SASI/HHS SBU/CDC ("Document control officers") SHSPI/FAA ("SHSI Program Officer")
Originator or successor / supervisor 10 of 28 (36%)	ACI/NASA ("originating NASA management official") FOUO/DHS ("Any DHS employee, detailee, or contractor") FOUO/DOD FOUO/FAA ("FAA managers") FOUO/NRO ("Originator of info") – with senior authorization OUO/DOE ("Any Federal or contractor employee" originating/controlling document) OUO/NRC ("Branch chiefs and above" and contractor-appointed) PROPIN/NRC SGI/NRC ("Branch chiefs and above") UCNI/DOE ("Reviewing Official")
No policy provided 7 of 28 (25%)	CAI/EPA ("originator or information manager") CBI/EPA ("originator or information manager") ECI/EPA ("originator or information manager") SBU/State ("US citizen direct-hire supervisory employees") SBU/GSA SHSI/NRC (staff assigned as "points of contact" for SHSI) UCNI/DOD ("Heads of DoD components")
Not available / unclear 5 of 28 (18%)	Computer Security Act Sensitive/DOD DEA Sensitive ("senior official") LOU/DOJ ("designate[d] subordinate officials") SSI/DOT WMD/State

GOVERNMENT EMPLOYEES' ACCESS TO PROTECTED INFORMATION

All of the agency policies included some limit on who may have access to protected unclassified information, both within the agency itself and among agencies, government contractors, and other federal (and in some cases state and local) government offices. In all cases, the provision involved some variation of a "need-to-know" requirement. The intention of applying this general principle is to minimize distribution and duplication of protected materials, by allowing them to circulate only when necessary for government business.

© 2006, The National Security Archive

The most common specific definition of "need-to-know" refers to those individuals who need the specific information to perform their official duties or other agency-authorized activities. In most cases, these individuals can be government employees or contractors who require access to particular sensitive information in order to do their job. Some agencies also express this restriction as a limitation on access for job-related endeavors or "government business." One example, part of the State Department policy, permits that: "Employees may circulate **SBU** material to others, including Foreign Service nationals, to carry out an official U.S. Government function if not otherwise prohibited by law, regulation, or interagency agreement." (Department of State, 12 FAM 540).

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.
-- Rep. Christopher Shays[xv]

Some variation can be seen in the specification of who may decide that another individual possesses the requisite need-to-know. In a number of cases, the policies grant this responsibility to "the person in possession of the document," (for example, in **Energy's OUO policy**) which could assumedly refer to any employee who either originated the document or has previously been recognized as having a need-to-know its contents. The authority to disseminate protected information presumably also bestows a more general duty to protect the information in accordance with the applicable policy. NRO, for example, states in its policy that "individuals possessing **FOUO information** must ensure the information is only disclosed or revealed to people who need the information to conduct business on behalf of the NRO." Similarly, **USDA sensitive security information (SSI)** may be distributed based on a "determination made by an authorized holder of SSI that a prospective recipient requires access to that SSI in order to perform or assist in a lawful and authorized governmental function." (USDA Departmental Regulation 3440-2).

Several agencies also place additional, although relatively minor, conditions on access to protected unclassified information. The most common condition is a specific mandate of a security background check, although it is important to note that none of the policies in question require authorized possessors of the information to have a security clearance, which is generally required to handle classified information. Agencies that require some form of background check include: AID and State (need-to-know access is "permitted only after individuals are granted a favorable background investigation"); Nuclear Regulatory Commission (access requires "determination of trustworthiness" (e.g. background check). The Department of Defense (DOD) in its policy on **Unclassified Controlled Nuclear Information (UCNI)** also enunciates specific limitations based on citizenship or position: only U.S. citizens who are government or contractor employees or members of the armed forces are granted general authorization for others, while exceptions for non-citizens to access the information are provided in certain specific situations.

In a few cases, agencies have required contract agreements or other signed notices to protect the integrity of documents designated as sensitive. Current GSA policy regarding **Sensitive but Unclassified Building Information** states that the holder of such information "must assure that recipient is an authorized user and completes Document Security Notice." In 2004, however, the Department of Homeland Security came under fire when it instituted a requirement that all of its 180,000 employees and contractors sign three-page forms, as a condition of their employment, that prohibit them from publicly disclosing **SBU information**. The policy, announced in May, threatened administrative or disciplinary action and potentially criminal or civil penalties for employees who violated the agreement. In addition, the agreement stated that signers agreed to consent to compliance searches by government inspectors "at any time or place."[23] In January 2005, after months of criticism from civil liberties groups, unions representing federal workers, and congressional members and staff (some of whom had been asked to sign the agreements in order to gain access to certain department information, but refused to so), DHS repealed the policy.[24]

"[T]hese designations sometimes are mistaken for a fourth classification level, causing unclassified information with these markings to be treated like classified information."
-- Moynihan Commission Report[xvi]

Since September 11 in particular, information dissemination has been as much a critical part of our national security as has protecting secrets from potential enemies. The Homeland Security Act of 2002 imposes upon the President not just the

© 2006, The National Security Archive

obligation to protect potentially sensitive information about infrastructure and security, but more importantly to facilitate the sharing among federal, state, and local officials such information that is relevant and important to security efforts.[25] This recommendation was enunciated clearly by the National Commission on Terrorist Attacks Upon the United States ("9/11 Commission"), which emphasized the role of communication and disclosure over that of protection and secrecy in the post-September 11 political climate: "Information procedures should provide incentives for sharing, to restore a better balance between security and shared knowledge. . . . The president should lead the government-wide effort to bring the major national security institutions into the information revolution. He should coordinate the resolution of the legal, policy, and technical issues across agencies to create a 'trusted information network.'"[26]

PHYSICAL SAFEGUARDS FOR SENSITIVE INFORMATION

Although each policy analyzed has specific and distinct instructions (or lack thereof) for the treatment and safeguarding of subject information, most of the policies are similar in many ways and contain protective restrictions or requirements for each of several categories of different activities and uses of information. In evaluating the levels of protection and control measures prescribed, this study looked at how the policy dictated that information—both physical materials and electronic information—should be marked, stored (both during work hours and non-work hours), transmitted, and destroyed.

The chart below summarizes representative examples of different levels of protection that agencies may apply to protected unclassified information. Each agency may not have identical procedures, but this list is useful in understanding the general approach of most agencies. Note that the vast majority of policies examined (25 out of 28, or 89%) contain what will be labeled as "moderate" protective measures, with only slight variation among the categorized approaches. While this approach does serve to illuminate prescribed procedures—which are, in most cases, clearer and more expansive than the rest of the agency policies—it is important to keep in mind that this compendium does not reflect the *actual practice* within the agencies.[27]

SAFEGUARD PROCEDURES			
	Low/Non-specific	Moderate	High
Storage			
Work hours	- "Adequately safeguarded," "reasonable care to limit unauthorized dissemination" (LOU/DOJ) - Balancing: value of info and probability of adverse impact from disclosure (Sensitive/DOD)	- Keep in access-controlled space - No entry by unauthorized persons	- Locked security storage container (steel filing cabinet, safe deposit box) when unattended
Non-work hours		- Secure container (locked desk, file cabinet, office)	- Locked security storage container (e.g. steel filing cabinet, safe deposit box)
Electronic		- Password-protect file - No storage on public networks, if possible	
Transmission			
Physical	- Ordinary mail	- Opaque envelope; - USPS or commercial	- Opaque cover, marked; - Government/contract messenger
Electronic	- Use discretion on phone; - Follow standard computer security policies	- Include marking; - Secure phone/fax when available - Encrypted email when available	- Secure or encrypted communications systems at all times

© 2006, The National Security Archive

Destruction			
Physical	- Tearing - Other (to prevent access)	- Tearing, - Shredding, - Burning	- Shredding, - Burning, - Pulping, - Chemical decomposition
Electronic		- Destroy/erase electronic media and back-up copies	
Marking			
	- No specific marking requirement; - Should carry distribution restriction		

LIMITATIONS ON USE OF INFORMATION CONTROLS

The following qualifiers are examples of the types of cautionary or prescribed restrictions included in several of the policies:

> Only 7 out of the 28 policies (25%) include an explicit stipulation against the misuse for improper purposes of the information control measures contained therein.

- "Information must not be designated as **Sensitive Security Information (SSI)** to conceal violations of law; inefficiency; administrative error; prevent embarrassment to a person, organization, department or agency; or restrain competition." (Department of Agriculture)
- "No other material shall be considered **FOUO** and **FOUO** is not authorized as an anemic form of classification to protect national security interests." (Department of Defense)
- "By designation, **FOUO** is used solely for official purposes, which generally precludes work at a residence or other non-official location." (National Reconnaissance Office)
- "Information must not be designated as **Limited Official Use** to conceal inefficiency, misdeeds or mismanagement." (Department of Justice)
- "Information shall not be designated as **FOUO** in order to conceal government negligence, ineptitude, or other disreputable circumstances embarrassing to a government agency." (Department of Homeland Security)

It is important to note that of these stated restrictions, all except one are part of policies that were in place prior to September 11. Only the Department of Homeland Security, which as an entity came into being in January 2003, has a newly-crafted qualifier. This restriction is particularly important in the case of DHS, however, as the FOUO marking can be applied by *any employee* of DHS, and so is potentially open-ended and subject to abuse more so than other, more specific policies.

Certainly this type of precise limitation is highly important as a means to alert employees and officials subject to the policy how it should, and should not, be used. Various aspects of these policies governing the protection of sensitive unclassified information certainly present a risk of abuse or misapplication. Although our research does not show to what extent qualifiers or explicit restrictions on these policies actually influence decision-making, nor does it describe what if any punishment might follow from employees' failure to heed such warnings, it is instructive to review the small number of provisions that at least on the surface seek to control the rampant protection of unclassified documents.

© 2006, The National Security Archive

UNCLASSIFIED INFORMATION POLICIES AND THE FREEDOM OF INFORMATION ACT

The Freedom of Information Act (FOIA) is inevitably intertwined with agency policies related to the protection, control, or non-disclosure of government information. Thus, policy changes within the Executive Branch (and in some cases initiated or supported by Congress) regarding the control of sensitive information can affect public access to information under the FOIA.

A majority of the agencies surveyed include in their policies some reference to FOIA. In certain cases, the FOIA is incorporated as a *definition of* protected information. At the other extreme, certain agency policies declare conclusively that a particular category of protected information fits within one or more of exemptions under the FOIA, and therefore suggests, encourages, or mandates withholding under that exemption unless review determines disclosure to be appropriate under FOIA policy. Some agencies stipulate an ordinary review of protected information under the FOIA before release, and in such cases, the sensitive designation ought not change the status of a document in the FOIA context. Others, however, place supplemental limitations on disclosure of protected information under FOIA, ranging from a requirement of specific authorization from high-level officials for each document to a policy of standard withholding of particular types of information under a specified exemption(s).

As a final note, agencies should be aware that although various government agencies today might use newly created terms to refer to categories of homeland security-related information--such as "Sensitive Homeland Security Information" (commonly referred to as "SHSI"), "Sensitive But Unclassified Information" (sometimes referred to as "SBU information"), or "Critical Infrastructure Information" (commonly referred to as "CII")--these categorical labels do not indicate classification pursuant to Executive Order 12,958. Terms such as "SHSI" and "SBU" describe broad types of potentially sensitive information that might not even fall within any of the FOIA exemptions.

– DOJ Freedom of Information Act Guide[xviii]

FOIA Treatment	Policy/Agency
Ordinary review	FOUO/DHS FOUO/NRO LOU/DOJ OUO/NRC
No FOIA Release	SSI/TSA (3) SSI/DOT (3) PCII/FAA (3) PCII/DHS (3) SHSI/FAA (3) UCNI/DOD (3)
FOIA Exemptions, Applicable	CBI/EPA (4) ECI/EPA (7) FOUO/DOD (2-9) FOUO/FAA (2-9) OUO/DOE (2-9) PROPIN/NRC (4) SBU/State (2-9)
FOIA Exemptions, Suggested	CAI/EPA (2,5) SSI/USDA (2-4, 7) WMD/State (2, 4)
Ashcroft Memo	SHSI/NRC WMD/State WMD/Treas.
Specific Authorization	PCII/FAA SBU/CDC SBU/GSA SSI/TSA SSI/USDA
No policy/ not available	DEA Sensitive Sensitive/DOD SGI/NRC Technical/DOD UCNI/DOE

The instances where a policy absolutely forbids release of certain unclassified information involve statutes that clearly proscribe disclosure under Exemption 3. For example, DHS regulation prohibits any release of **Protected Critical Infrastructure Information (PCII)**, a new designation created by the Homeland Security Act, Sec. 212: "**Protected CII** shall be treated as exempt from disclosure under the Freedom of Information Act and, if provided by the Protected CII Program Manager or the Protected CII Program Manager's designees to a State or local government agency, entity, or authority, or an employee or contractor thereof, shall not be made available pursuant to any State or local law requiring disclosure of records or information."[28]

It is important to note several other approaches that agencies have taken in light of the conflict between their policies and the statutory language of FOIA. Some agencies require specific authorization on a case-by-case basis before controlled materials can be released under FOIA. This practice moves review of SBU-designated information one step beyond that ordinarily conducted under FOIA, such that FOIA managers who receive requests for this type of information must consult agency officials outside of their ordinary processing protocol. It is unclear whether these agencies have further specified detailed procedures for how such a review is to take place.

© 2006, The National Security Archive

In some cases, as well, agencies have written their policies explicitly to comply with Attorney General Ashcroft's October 12, 2001 memorandum, or at least to abide by the general spirit of its mandate. In it, the Attorney General stated: "I encourage your agency to carefully consider the protection of all such values and interests when making disclosure determinations under the FOIA. Any discretionary decision by your agency to disclose information protected under the FOIA should be made only after full and deliberate consideration of the institutional, commercial, and personal privacy interests that could be implicated by disclosure of the information."[29] Several agencies, including the Departments of State and Treasury, have adopted the Card Memo's formulation of weapons of mass destruction (WMD) and other sensitive homeland security information as part of their information management program. Other policies reference the memo and/or demand more attentive review of specified information under certain exemptions with a view towards withholding, if at all possible.

In other cases, agency officials have provided employees with "suggested" FOIA exemptions, those under which the particular information in question *may* qualify for withholding. Potentially, this policy approach could make freedom of information personnel more likely to try to "find" an exemption for information that may not be precisely addressed. For example, USDA encourages its personnel to process requests "with consideration of all applicable FOIA exemptions" and lists four "FOIA Exemptions Potentially Applicable to SSI:

(1) For SSI pertaining to USDA operations or assets, FOIA Exemption 2 should be considered;
(2) For current SSI consisting of private sector or industry information submitted voluntarily to USDA that is customarily protected by the submitted, FOIA Exemption 4 should be considered;
(3) For any SSI the disclosure of which is banned by federal statute, FOIA Exemption 3 should be considered; and
(4) For any SSI that consists of information compiled for law enforcement purposes, FOIA Exemption 7 should be considered."

There are several different but equally significant problems with the treatment of designated sensitive unclassified information under the FOIA. The Executive Branch is already governed by an overarching policy regarding the protection of information that is unclassified but may nonetheless be inappropriate for public release, codified in FOIA Exemptions 2 through 9. In 1966, Congress expressly permitted agencies to shield from public view certain types of information, the nondisclosure of which respects a significant and identifiable government interest. Without necessitating amendment, Congress also left the door open for itself to expand the scope of FOIA, namely by passing a statute that would exempt particular information under Exemption 3, 5 U.S.C. § 552(b)(3), which safeguards information that is exempt under other laws.

The statutory FOIA language, however, nowhere sanctions internal agency decisions that would potentially override the FOIA in specific situations. Although none of the agency policies do this overtly, the prevalence of merged definitions, where information ordinarily protected under the FOIA is given the additional shield of a formal coversheet and an **SBU** or **FOUO** stamp, somehow suggests an additional level of security between it and the public. Logic dictates that information flagged and reviewed in FOIA offices before it is circulated to members of the public is already getting special treatment, and that an additional marking is superfluous; the same rationale would suggest that information designated as sensitive unclassified information must be different (i.e. *more* sensitive) than materials ordinarily controlled under FOIA. If nothing else, the psychological impact of supplementary control designations applied to unclassified information has the potential to reduce the amount of information that will now be released under FOIA.

© 2006, The National Security Archive

AGENCY PROCESSING OF FOIA REQUESTS

PROCESSING TIME

For both the Card Memorandum and sensitive unclassified information FOIA requests, we assumed that the information necessary to respond would be easily identifiable by agency FOIA offices. None of the materials we received were classified or otherwise significantly protected, and many can be found on agency Internet sites. As such, the search from the perspective of FOIA officers should have been relatively simple in comparison to the numerous topic-specific or sensitive issue-related FOIA requests received in most offices. The policies at issue are themselves part of agency information management regimes, and so it would be logical for these policies and guidelines to be located within the FOIA office at each agency.

In fact, the processing of the FOIA requests varied enormously. The range of response times for the Card Memorandum request was 9-702 business days, and two requests are still pending over 750 business days later. The range for the sensitive unclassified information requests was 6-186 business days, and nine requests are still pending. In both cases there are still agencies that have not responded at all. These delays illustrate the limitations of using FOIA for informed public policy debate. While the passage of significant time, the persistence of researchers, and the responsiveness of certain FOIA officers has resulted in the release of useful records, this experience demonstrates that there are still significant backlogs in the current federal FOIA system.

It was clear from reviewing the materials provided by most agencies which office within the agency or organization is specifically responsible for the creation and/or oversight of the policy. In four cases, the responsible body was one tasked with information management or information security specifically (e.g., the Office of Information Resources Management at AID, the Personnel and Document Security Division at USDA, and Information and Physical Security at Treasury). In seven other cases, the task fell within a more general security office (such as NASA's Office of Security and Program Protection and NRC's Office of Nuclear Security and Incident Response). The rest of the policies came from another source, including general operations or a very high-level individual such as the secretary or administrator (the latter occurs in three agencies). The problems that some agencies had with processing the requests suggests that these security offices may not be adequately integrated with the records management and FOIA branches of the agencies.

DISPARITY IN RESPONSES

In addition, the type of information released varied significantly, with some agencies releasing extensive communications demonstrating their policy development and implementation activities and other agencies releasing only limited formal documentation of policies (which, in many cases, were publicly available). Thus, the subjectivity of release decisions can have a significant impact on the value of FOIA for informing the public about the activities and operations of government.

For example, a common problem was lack of understanding or misinterpretation of the FOIA requests. At some agencies (including State, DHS, and Energy), **FOUO** or **SBU information** can be designated by *any employee*, which assumedly includes those employees who process FOIA requests. However, we encountered several inquiries about the nature of the request itself. Furthermore, several agency representatives expressed a concern that our request was too broad, which questions the suitability of the searches conducted; for example, a search for "sensitive unclassified information" in a poorly organized records system might return those documents which are marked for protection per the agency policy in addition to documents establishing or discussing the policy. The Department of the Army denied any further processing of our request, declaring it too broad; however, a search of the Army's Web site produces Army Regulation 25-55, "The Department of the Army Freedom of Information Act Program," a chapter of which is entitled **"For Official Use Only."** These sorts of problems and inconsistencies cannot be addressed without adequate communication channels between FOIA requesters and FOIA offices, and educated FOIA officers with adequate records management training and adequate tools and resources.

In addition, several of the agencies that responded favorably released documents generally unrelated to the request or unhelpful in revealing the relevant policies of their agency, suggesting either a faulty search or the absence of relevant

© 2006, The National Security Archive

documents. Two of these agencies–the Department of Veterans' Affairs and the Department of Housing and Urban Development–provided us with guidelines related to information security in the employment context, including criteria for background checks or security clearances and sensitivity designations for various positions at the agency that require access to sensitive or classified information.

In one case, the Department of State failed to provide us with the section of their Foreign Affairs Manual, 12 FAM 540, entitled **"Sensitive But Unclassified Information (SBU)"** but instead sent a different section of the same manual, 5 FAM 470, "Access to and Use of Information," which details general policies about employees' access to records, sharing of State Department records with other government agencies, and general release of agency records under the FOIA. The section that defines **SBU information** specifically and outlines procedures for its treatment is available on the State Department's Web site, and was provided to us by USAID, which also follows this policy.

© 2006, The National Security Archive

RECOMMENDATIONS: STRATEGIES AND BEST PRACTICES TO SECURE AND SHARE SENSITIVE INFORMATION

Our research and appraisal of current agency practice shows a system that is seriously flawed. The diversity of policies, ambiguous or incomplete guidelines, lack of monitoring, and decentralized administration of information controls on unclassified information is troubling from the perspectives of safety, security, and democracy.

MONITORING OF PROTECTED DOCUMENTS

Arguably the most significant problem with agencies' protection of unclassified information is the lack of data concerning how many protected documents exist and the unavailability of any means to find out. The absence of reporting systems makes any assessment of the extent to which a policy is being used difficult, if not impossible. In written questions from the House Subcommittee on National Security, Emerging Threats, and International Relations, in conjunction with its recent hearing on pseudo-classification, Rear Admiral Christopher McMahon of the Department of Transportation, Office of Intelligence, Security, and Emergency Response, was asked how many FOUO, SSI, or similar designation decisions were made by DOT and its components. Admiral McMahon responded, "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 record of how many times."[30]

[V]ery 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.
– Harold C. Relyea, Congressional Research Service[xxii]

In comparison, it is useful to look to the formal classification system, which is governed by Executive Order 12958, as amended, and is managed and monitored by the Information Security Oversight Office (ISOO) of the National Archives and Records Administration (NARA). ISOO publishes an annual report to the President in which they quantify the number of classification and declassification decisions, the number of individuals with authority to classify material, and the type of information that is being classified.[31] Such reports enable the Executive Branch and Congress to monitor the costs and benefits of the classification system and to identify trends that may suggest the need to reform the system.

Because safeguarding sensitive unclassified information impacts safety, security, budget and information disclosure–all important national concerns–some form of overarching monitoring of *all* information control would be valuable. Agencies should be required to maintain a record of who can use sensitive unclassified information designations and how many documents they designate for protection. Furthermore, the agencies should be required to maintain a record of how often FOIA officials release or withhold documents that have been marked as sensitive. Such data would make it possible for Congress and the public to be able to assess agency secrecy.

The Government Accountability Office (GAO) recently conducted a study of TSA's new Sensitive Security Information (SSI) policy at the request of members of Congress. GAO's report concluded that the omission of oversight mechanisms of any sort was a serious problem: "internal control policies and procedures for monitoring the compliance with regulations governing the SSI designation process, including internal controls for ongoing monitoring, communicated to all staff, would help ensure accountability and consistency in the implementation of TSA's SSI regulations."[32]

© 2006, The National Security Archive

THE BLACK HOLE OF INFORMATION SAFEGUARDING

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.
- Heritage Foundation Special Report (2004)[xix]

For classified information, the security classification system provides precise limits on the extent and duration of classification as well as a system for declassification, including public requests for declassification. For non-security sensitive information, the FOIA provides a relatively clear and user-friendly process for the public to seek access to information held by the government. Sensitive unclassified information, however, falls into a black hole. As this Study shows, it is likely that information previously available under FOIA or on unrestricted Web sites may no longer be available to the public. Yet, there is virtually no opportunity for the public or other government personnel to challenge a decision to mark a document for protection as **SBU**, **FOUO**, or **SSI**. Accordingly, in order to protect the important role that public access has played in government accountability, it is important that a system for challenging the use of sensitive unclassified information markings be established at each agency or, alternatively, that FOIA procedures be adjusted to counteract the chilling effect that these markings may have on disclosure under FOIA. Moreover, classified information is subject to limits on the duration of protection, but few such limits exist for SUI. Thus, once marked may mean forever marked.

THE HIDDEN COSTS

ISOO reports annually on the estimated costs of classification and declassification activities throughout the government. During FY 2003, agencies spent a total of $6.5 billion on information security generally, including classification and declassification management and security for information systems; an additional $536 million was spent on physical security for buildings and storage of classified information.[33] By referring to the chart on page 19, which depicts the range of safeguarding methods that are applied to unclassified information by some agencies, it is apparent that many of the measures mirror those applied to classified information. It is possible, therefore that some portion of the spending ISOO reported was in fact used for unclassified information protection. Convenience, resource constraints, or established practices may lead to the commingling of classified and sensitive unclassified materials in order to ensure both are properly safeguarded. If this occurs, it could potentially undermine the security of the classification system. Accordingly, agencies should be required to take steps to assess the cost of their sensitive unclassified information systems and ensure that safeguards do not undermine the security of classified information.

Moreover, the cost of an impaired information sharing system cannot by quantified. There are two aspects to this problem. The first, which has been well-documented, is the problem of inter-agency information sharing. The second is the problem of public-private sector information sharing; if private industry is unable to learn information and is required to adopt restrictions on information from the government, it may be well inhibit the willingness of private industry to engage in activities that could benefit the public good.

A UNIFIED SYSTEM

This Study suggests that a great deal of non-sensitive information is being withheld today that should be or previously would have been released under the FOIA. It is also likely, however, that the current system of diverse and unregulated safeguard mechanisms is not actually succeeding in shielding much of the information that could be useful to terrorists or others desiring to undermine the security of the United States. Even Secretary of Defense Rumsfeld has recognized that **FOUO** is not working properly at the Department of Defense,[34] and similar policies are probably not achieving their goals elsewhere across the federal government.

© 2006, The National Security Archive

An Al Qaeda training manual recovered in Afghanistan states: "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80% of information about the enemy." At more than 700 gigabytes, the DOD web-based data makes a vast, readily available source of information on DOD plans, programs, and activities. One must conclude our enemies access DOD web sites on a regular basis. . . . The fact that for official use only (FOUO) and other sensitive unclassified information (e.g. CONOPS, OPLANS, SOP) continues to be found on public web sites indicates that too often data posted are insufficiently reviewed for sensitivity and/or inadequately protected. Over 1500 discrepancies were found during the past year. This continuing trend must be reversed.
– Sec. of Defense Donald Rumsfeld[x]

Although classification is centrally managed, agencies implement their own classification programs according to central guidance and criteria, in a way that makes sense within the function and mission of their particular organization. ISOO Director J. William Leonard has recommended that a unified framework be instituted to both simplify and supervise control of unclassified information as well. In his proposed structure, Leonard offers several suggestions that seem appropriate, particularly in light of our findings. He advocates for: "Strict limitations as to who can designate information as falling under the system of controls"; "Built-in criteria that must be satisfied in order to place controls on dissemination"; "Uniform 'due-diligence' standards with respect to how to handle and protect controlled information"; and "A process . . . whereby both authorized holders and outsiders can appeal the application of dissemination controls."[35]

This Study suggests that issues of information security, information sharing, and public access to information should not be addressed in a piecemeal manner. There are best practices in agencies that should be shared, as well as lessons to be learned about the costs and benefits of secrecy and disclosure. Unnecessary secrecy has been on the rise since September 11, with the result of threatening our safety and national security while impeding the process of democracy and the effective functioning of the government. In presenting markers of possible successes and failures of sensitive unclassified information programs among the federal agencies, this Study seeks to offer a rationale and a sense of urgency for initiating reforms, in these and other information-control programs government-wide.

ENDNOTES

[1] William J. Broad, "A Nation Challenged; The Biological Threat; U.S. Is Still Selling Reports on Making Biological Weapons," The New York Times, at A1 (Jan. 13, 2002).
[2] *See, e.g. Emerging Threats: Overclassification and Pseudo-Classification*, Hearing Before the Subcomm. On National Security, Emerging Threats, and International Relations, 109th Cong. (2005).
[3] *Government Information Policies and Practices--Security Classification Problems Involving Subsection (b)(1) of the Freedom of Information Act (Part 7)*, Hearing before the Foreign Operations and Government Information Subcommittee of the U.S. House Committee on Government Operations, 92nd Cong. (1972) (Opening statement of Chairman Moorhead), at 2283.
[4] *Id* (questioning by William G. Phillips, Staff Director), at p. 2498.
[5] President Jimmy Carter, "Telecommunications Protection Policy," PD/NSC-24 (Nov. 16, 1977)
[6] For more background, see Genevieve Knezo, *"Sensitive But Unclassified" and Other Federal Security Controls on Scientific and Technical Information: History and Current Controversy*, Congressional Research Service, RL 31845 (July 2, 2003).
[7] The Computer Security Act of 1987, 40 U.S.C. 1441 (1987).
[8] *Report of the Commission on Protecting and Reducing Government Secrecy*, Senate Document 105-2, 103rd Congress, U.S. Government Printing Office (1997) [hereinafter "Moynihan Commission Report"], http://www.access.gpo.gov/congress/commissions/secrecy/.
[9] Homeland Security Act of 2002, 6 U.S.C. § 482(a).
[10] The Archive faxed a FOIA request to the Office of Management and Budget (OMB) on January 9, 2003.
[11] Defense Information Systems Agency, "DMS GENSER Message Security Classifications, Categories, and Marking Phrase Requirements," Version 1.2, Attachment 5 (Mar. 19, 1999).
[12] *Id.* at 6-7.
[13] *Id.* at 9.
[14] *Id.* at 12.
[15] http://www.openthegovernment.org/otg/SRC2005.pdf.
[16] Department of Justice, *FOIA Post: Critical Infrastructure Information Regulations Issued by DHS* (2004), http://www.usdoj.gov/oip/foiapost/2004foiapost6.htm.

© 2006, The National Security Archive

[17] Homeland Security Act of 2002, 6 U.S.C.A. § 482(f)(1).
[18] Homeland Security Act of 2002, 6 U.S.C.A. § 482(c).
[19] Because several of the responsive agencies have multiple policies to protect different categories of sensitive information, and because a number of agencies have no reported policy, the number of different SBU-like policies to be analyzed is different from the number of agencies considered. In addition, some agencies share policies–for example, a DHS-wide directive on SBU information applies at least in name to each component of the department, and AID follows the SBU policy set forth by the Department of State in its *Foreign Affairs Manual*. Please note, however, that this study has not combined policies with the same title or similar definition, where those policies are distinct in that they have been internally or otherwise derived from different sources or are substantially different in any other way.
[20] U.S. Government Accountability Office, "Transportation Security Administration: Clear Policies and Oversight Needed for Designation of Sensitive Security Information," GAO-05-677 Report to Congressional Requesters (June 2005), at 3.
[21] Remarks of J. William Leonard, Director, Information Security Oversight Office (ISOO), at the National Classification Management Society's Annual Training Seminar, Salt Lake City, UT (June 12, 2003).
[22] *Conference Report on H.R. 2360, Department of Homeland Security Appropriations Act*, H.R. Conf. Rep. No., at 109-241 (2006).
[23] Spencer S. Hsu, *Homeland Security Employees Required to Sign Secrecy Pledge; Gag Order Raises Concern on Hill*, Washington Post (Nov. 16, 2004).
[24] John Files, *Security Dept. Eases Its Nondisclosure Rule*, New York Times (Jan. 18, 2005).
[25] Homeland Security Act Sec. 892(c)(2). The President delegated authority to regulate in accordance with the Act in Executive Order 13311, in July 2003.
[26] U.S. National Commission on Terrorist Attacks Upon the United States, The 9/11 Commission Report (Washington: GPO, 2004), at 417-18.
[27] Moynihan Commission Report, *supra* note 8.
[28] Disclosure of Protected Critical Infrastructure Information, 6 C.F.R. §29.8; *see also* Homeland Security Act of 2002 § 214, 6 U.S.C.A. § 133(a)(1).
[29] Memorandum for Heads of All Federal Departments and Agencies: "The Freedom of Information Act," from Attorney General John Ashcroft (October 12, 2001), http://www.usdoj.gov/04foia/011012.htm.
[30] McMahon letter to Representative Christopher Shays, Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, U.S. House of Representatives (May 9, 2005).
[31] *See, e.g.*, Information Security Oversight Office (ISOO), "Report to the President 2004" (March 31, 2005), http://www.archives.gov/isoo/reports/2004-annual-report.html.
[32] GAO, *supra* note 20, at 7.
[33] ISOO, *2003 Report on Cost Estimates for Security Classification Activities* (July 2004), http://www.archives.gov/isoo/reports/2003-cost-report.html.
[34] Sec. of Defense Donald Rumsfeld, Cable: "Web site OPSEC discrepancies," January 14, 2003, http://www.fas.org/sgp/news/2003/01/dodweb.html.
[35] Leonard remarks, *supra* note 21.

QUOTATIONS

i Remarks of J. William Leonard, Director, Information Security Oversight Office (ISOO), at the National Classification Management Society's Annual Training Seminar, Salt Lake City, UT (June 12, 2003).
ii *Executive Classification of Information, Security Classification Problems Involving Exemption (b)(1) of the Freedom of Information Act*, U.S. House of Representatives, Committee on Government Operations, H.R. Rep. 93-221 (1973).
iii Report of the Commission on Protecting and Reducing Government Secrecy ("Moynihan Commission Report"), Senate Document 105-2, 103rd Congress, U.S. Government Printing Office (1997), http://www.access.gpo.gov/congress/commissions/secrecy/
iv Coalition of Journalists for Open Government, Comments on Proposed Regulations: In the Matter of Protection of Sensitive Security Information (filed July 16, 2004), http://www.cjog.net/protest_sensitive_security_inform.html.
v *Emerging Threats: Overclassification and Pseudo-Classification*, Hearing Before the Subcomm. On National Security, Emerging Threats, and International Relations, 109th Cong. (2005) (Statement of Representative Christopher Shays, Chairman), http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_house_hearings&docid=f:20922.wais.
vi U.S. Department of Justice, *Freedom of Information Act Guide* (May 2004), http://www.usdoj.gov/oip/foi-act.htm.
vii Sec. of Defense Donald Rumsfeld, Cable: "Web site OPSEC discrepancies," January 14, 2003, http://www.fas.org/sgp/news/2003/01/dodweb.html.
viii Emerging Threats: Overclassification and Pseudo-Classification, Hearing Before the Subcomm. On National Security, Emerging Threats, and International Relations, 109th Cong. (2005) (Statement of Harold C. Relyea, Congressional Research Service).

© 2006, The National Security Archive

[ix] *Government Information Policies and Practices—Security Classification Problems Involving Subsection (b)(1) of the Freedom of Information Act (Part 7)*, Hearing before the Foreign Operations and Government Information Subcommittee of the U.S. House Committee on Government Operations, 92nd Cong. (1972) (Opening statement of Chairman Moorhead), at 2283.
[x] President Dwight D. Eisenhower, Farewell Radio and Television Address to the American People (January 17, 1961).
[xi] Remarks of J. William Leonard (2003).
[xii] *Id.*
[xiii] MITRE Corporation, JASON Program Office, *Horizontal Integration: Broader Access Models for Realizing Information Dominance* (Dec. 2004), p. 5, *available at* http://www.fas.org/irp/agency/dod/jason/classpol.pdf.
[xiv] Coalition of Journalists for Open Government, Comments on Proposed Regulations: In the Matter of Protection of Sensitive Security Information (filed July 16, 2004), http://www.cjog.net/protest_sensitive_security_inform.html.
[xv] Statement of Representative Christopher Shays (2005)
[xvi] Moynihan Commission Report (1997).
[xvii] DOJ, *FOIA Guide* (2004).
[xviii] Statement of Harold C. Relyea (2005).
[xix] James Jay Carafano and David Heyman, "DHS 2.0: Rethinking the Department of Homeland Security," *Heritage Special Report* (Dec. 13, 2004), p. 27, http://www.heritage.org/Research/HomelandDefense/sr02.cfm.
[xx] Rumsfeld Cable (2003).

© 2006, The National Security Archive

FURTHER READING

Aftergood, Steven & Henry Kelly, "Making Sense of Information Restrictions After September 11," 55 *Federation of American Scientists Public Interest Report* 2 (March/April 2002).

Bagley, James J., "Understanding Controls on Unclassified Government Information or 'Who's on First?'" National Classification Management Society, NCMS Viewpoints (1993), http://www.fas.org/sgp/eprint/bagley.html.

Buchalter, Alice R. et al., "Laws and Regulations Governing the Protection of Sensitive But Unclassified Information," Federal Research Division, Library of Congress (Sept. 2004).

Emerging Threats: Overclassification and Pseudo-Classification, Hearing Before the Subcomm. On National Security, Emerging Threats, and International Relations, 109th Cong. (2005), http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_house_hearings&docid=f:20922.wais.

Executive Classification of Information—Security Classification Problems Involving Exemption (b)(1) of the Freedom of Information Act, H.R. Rep. No. 93-221 (1973).

Government Information Policies and Practices—Security Classification Problems Involving Subsection (b)(1) of the Freedom of Information Act (Part 7), Hearing before the Subcomm. Foreign Operations and Government Information of the H. Comm. on Government Operations, 92nd Cong. (1972).

Knezo, Genevieve J., "'Sensitive But Unclassified' and Other Federal Security Controls on Scientific and Technical Information: History and Current Controversy," CRS Report RL31845 (July 2, 2003).

OMB Watch, *Background on Sensitive But Unclassified Information* (2005), http://www.ombwatch.org/article/archive/238?TopicID=2.

OpenTheGovernment.org, "Secrecy Report Card 2005" (Sept. 4, 2005), http://www.openthegovernment.org/otg/SRC2005.pdf.

Report of the Commission on Protecting and Reducing Government Secrecy, Senate Document 105-2, 103rd Congress, U.S. Government Printing Office (1997), http://www.access.gpo.gov/congress/commissions/secrecy/.

Reporters Committee for Freedom of the Press, "Homefront Confidential" (June 8, 2005).

Sollenberger, Mitchel A., *Sensitive Security Information and Transportation Security: Issues and Congressional Options,* Congressional Research Service RL32425 (June 9, 2004).

Sollenberger, Mitchel A., *Sensitive Security Information (SSI) and Transportation Security: Background and Controversies,* Congressional Research Service RS21727 (Feb. 5, 2005).

U.S. Department of Justice, "Critical Infrastructure Information Regulations Issued by DHS," *FOIA Post* (Feb. 27, 2004), http://www.usdoj.gov/oip/foiapost/2004foiapost6.htm.

U.S. Government Accountability Office, "Transportation Security Administration: Clear Policies and Oversight Needed for Designation of Sensitive Security Information," GAO-05-677 Report to Congressional Requesters (June 2005).

U.S. House of Representatives, Committee on Government Reform, Minority Staff, "Secrecy in the Bush Administration," Report prepared for Rep. Henry A. Waxman (Sept. 14, 2004), http://democrats.reform.house.gov/features/secrecy_report/pdf/pdf_secrecy_report.pdf.

© 2006, The National Security Archive

APPENDIX I
CARD MEMORANDUM FOIA REQUESTS, BY PROCESSING TIMES
SUMMARY OF AGENCY PROCESSING

Number of Business Days	Agency	Number of Documents / Pages Provided
9	Federal Bureau of Investigation	No Documents
11	Health and Human Services	No Documents
12	National Science Foundation	1 Document (1 p.)
16	Dept of Housing and Urban Development	No documents
24	Department of Education	No Documents
24	Environmental Protection Agency	3 Documents (18 pp.), 107 Documents withheld Appeal Pending
26	Department of Navy	1 Document (7 pp.)
27	General Services Administration	2 Documents (3 pp.)
30	Small Business Administration	2 Documents (2 pp.)
31	Federal Emergency Management Agency	1 Document (1 p.)
32	Department of Interior	13 Documents (81 pp.), 7 Documents withheld
34	Department of Commerce	13 Documents (25 pp.), 16 Documents withheld
35	Department of Treasury	15 Documents (27 pp.)
36	Office of Management & Business	No Documents
41	Department of Labor	3 Documents (3 pp.)
41	Department of Veterans Affairs	2 Documents (2 pp.)
42	Department of Justice	5 Documents (14 pp.), 40 Documents withheld
46	Department of Agriculture	2 Documents (10 pp.)
61	Drug Enforcement Agency	1 Documents (3 pp.)
69	Nuclear Regulatory Commission	16 Documents (32 pp.)
94	Office of Personnel Management	No Documents
103	Department of Defense	86 Documents (125 pp.)
103	National Archives and Records Admin.	3 Documents (6 pp.)
104	Department of Army	3 Documents (7 pp.)
110	Department of Air Force	9 Documents (63 pp.)
118	Department of Energy	63 Documents (152 pp.)
137	Social Security Administration	1 Document (10 pp.)
151	Defense Intelligence Agency	No Documents
151	Department of Transportation	78 Documents (150 pp.)
160	Securities and Exchange Commission	No Documents
197	U.S. Central Command (CENTCOM)	No Documents
217	Department of State	4 Documents (11 pp.)
* 702	National Aeronautics and Space Admin.	1 Document (2 pp.)
750+	U.S. Agency for International Development	Request Pending
750+	Central Intelligence Agency	Request Pending

* On October 25, 2002 NASA provided responsive documents, including its reply to the White House regarding the Card Memo, in response to a previous request from the National Security Archive for documents on Attorney General John Ashcroft's October 12, 2001 memo on FOIA policy.

© 2006, The National Security Archive

APPENDIX II
IMPACT OF CARD MEMORANDUM, BY AGENCY

AGENCY[i]	REPORT TO CARD	REVIEW FOR WMD RECORDS	REVIEW FOR OTHER SENSITIVE RECORDS	WEB SITE INFORMATION REMOVAL; NEW WEB POLICIES	INCREASED EMPHASIS ON FOIA EXEMPTIONS FOR WITHOLDING	NEW SECURITY AND SAFE-GUARDING MEASURES
AID	No Response	No Response	No Response	No Response	No Response	No Response
AIR	YES, *see* DOD regarding joint response	YES	YES	Web information removal; review of records	Additional review for CBRN[ii]	New Security Training
ARMY	YES, *see* DOD regarding joint response	YES	YES	Web information removal; review of records	Additional review for CBRN	Dissemination of Card Policy
CENTCOM[iii]	No Documents	No Documents	No Documents	No Documents	No Documents	No Documents
CIA	No Response	No Response	No Response	No Response	No Response	No Response
DEA[iv]	No Documents[v]	No Documents	No Documents	No Documents	No Documents	No Documents
DIA[vi]	No Documents	No Documents	No Documents	No Documents	No Documents	No Documents

© 2006, The National Security Archive

APPENDIX II
IMPACT OF CARD MEMORANDUM, BY AGENCY

AGENCY[1]	REPORT TO CARD	REVIEW FOR WMD RECORDS	REVIEW FOR OTHER SENSITIVE RECORDS	WEB SITE INFORMATION REMOVAL; NEW WEB POLICIES	INCREASED EMPHASIS ON FOIA EXEMPTIONS FOR WITHOLDING	NEW SECURITY AND SAFE-GUARDING MEASURES
USDA	YES	YES		Inventoried Web sites; new review procedures	Guidance to use FOIA Exemptions 2, 3 and 7 for sensitive security information	New personnel security and information security measures; new departmental regulations; sought classification authority
DOC	YES	YES	YES			Dissemination of Card guidance
DOD	YES, Joint Military Response	YES	YES	Web information removal; review of records	Additional review for CBRN	New classification guide; new procedures for sharing unclassified sensitive information
DOE	YES	YES	YES	Web information removal; New Security Measures	Additional Review Of Requested Records; New Guides For FOIA Exemptions	New Information Security Guides; Dissemination of Card guidance
DOI	YES	YES	YES	Web information removal	Special Handling of FOIA Requests; dissemination of Card guidance to FOIA officers	Dissemination of Card guidance
DOJ					FOIA Exemption Guidance Disseminated; training on FOIA exemptions 1, 2,3, 4.	Guidance and policies concerning Classified, Declassified and SBU information disseminated.
DOL	YES	YES	YES	Web review (possible info removal); updated Web policies	Guidance on withholding under FOIA	Dissemination of Card guidance
DOS					FOIA Exemption 2 and 4 Guidance Disseminated; training on guidance	Guidance and policies concerning safeguarding information disseminated
DOT	YES	YES	YES	Web information removal; new Web procedures	New Procedures for FOIA Review	New security policies
EDU	No Documents	No Documents	No Documents	No Documents	No Documents	No Documents

© 2006, The National Security Archive

APPENDIX II
IMPACT OF CARD MEMORANDUM, BY AGENCY

AGENCY[i]	REPORT TO CARD	REVIEW FOR WMD RECORDS	REVIEW FOR OTHER SENSITIVE RECORDS	WEB SITE INFORMATION REMOVAL; NEW WEB POLICIES	INCREASED EMPHASIS ON FOIA EXEMPTIONS FOR WITHOLDING	NEW SECURITY AND SAFE-GUARDING MEASURES
EPA	YES	YES	YES	Web information removal; new procedures	Emphasis on FOIA Exemptions 2 and 4	Dissemination of Card guidance
FBI[vii]	No Documents	No Documents	No Documents	No Documents	No Documents	No Documents
FEMA	YES	YES	YES			
GSA	Yes	YES	YES		Review of FOIA Policies	Non Disclosure Agreements; new safeguarding procedures
HHS	No Documents	No Documents	No Documents	No Documents	Card Memo Disseminated to FOIA Offices[viii]	No Documents
HUD	No Documents	No Documents	No Documents	No Documents	No Documents	No Documents
NARA	No Documents[ix]	No Documents	No Documents	No Documents	No Documents	No Documents
NASA[x]	No Response	YES	YES	Web sites Blocked; New Web procedures	Card Memo disseminated to FOIA Offices	Dissemination of Card guidance; New Security Program
NRC	YES	YES	YES		Guidance For Withholding Information Under FOIA	
NSF	YES	YES	YES			
OMB	No Documents	No Documents	No Documents	No Documents	No Documents	No Documents
OPM	No Documents	No Documents	No Documents	No Documents	No Documents	No Documents
SBA	YES	YES	YES			Dissemination of Security Information
SEC	No Documents	No Documents	No Documents	No Documents	No Documents	No Documents
SSA	No Documents	No Documents	No Documents	No Documents	No Documents	No Documents
TRE	YES	YES	YES			Dissemination of Card guidance
USN (NAVY)	YES, see DOD regarding joint response	YES	YES		Disseminated to FOIA Offices; Refers to Ashcroft Memorandum for FOIA Exemptions	

© 2006, The National Security Archive

APPENDIX II
IMPACT OF CARD MEMORANDUM, BY AGENCY

AGENCY[i]	REPORT TO CARD	REVIEW FOR WMD RECORDS	REVIEW FOR OTHER SENSITIVE RECORDS	WEB SITE INFORMATION REMOVAL; NEW WEB POLICIES	INCREASED EMPHASIS ON FOIA EXEMPTIONS FOR WITHOLDING	NEW SECURITY AND SAFE-GUARDING MEASURES
VET	YES	YES	YES			Dissemination of Card guidance

[i] Agencies that did not respond are listed in bold.
[ii] CBRN means Chemical Biological Radiological and Nuclear information.
[iii] CENTCOM is a component of DOD.
[iv] DEA is a component of DOJ.
[v] DEA provided copies of the Card Memorandum and ISOO-OIP Guidance.
[vi] DIA is a component of DOD.
[vii] FBI is a component of DOJ.
[viii] Although HHS reported no documents, a later correspondence indicated that the Card Memorandum was disseminated to FOIA offices.
[ix] NARA withheld records concerning the ISOO-OIP Guidance and offered to send the Card Memorandum and the ISOO-OIP Guidance.
[x] NASA did not respond to the Card FOIA request, but this information was obtained from a NASA response to an earlier FOIA request filed by the Archive for information concerning the implementation of the Ashcroft Memorandum. (See http://www.gwu.edu/%7Ensarchiv/NSAEBB/NSAEBB84/index.html)

© 2006, The National Security Archive

APPENDIX III
SENSITIVE UNLASSIFIED INFORMATION FOIA REQUESTS, BY PROCESSING TIME

Number of Business Days	Agency	Number of documents / Pages provided
6	National Science Foundation	1 Document (2 pp)
14	Social Security Administration	No Documents
14	Treasury Department	8 Documents (51 pp)
16	Small Business Administration	No Documents
19	Department of State	3 Documents (12 pp)
20	Department of Agriculture	3 Documents (18 pp)
21	Federal Aviation Administration	2 Documents (19 pp)
25	Securities and Exchange Commission	No Documents Appeal Pending – new search in progress
26	Office of Management and Budget	No Documents
27 IG 29 Citizen Services	General Services Administration	1 Document (3 pp) – IG 2 Documents (13 pp) – Citizen Services
40	Environmental Protection Agency	1 Document (66 pp)
41	Department of Justice, OIP	No Documents – forwarded to DHS
42	Veterans' Administration	3 Documents (54 pp)
43	Federal Emergency Management Agency	No Documents – forwarded to DHS
43	Transportation Safety Administration	3 Documents (45 pp)
45	National Aeronautics and Space Agency	4 Documents (210 pp)
49	Housing and Urban Development	1 Document (22 pp)
55	Office of Personnel Management	No Documents
71	National Reconnaissance Office	5 Documents (43 pp)
105	Department of the Air Force	No Documents, list of publicly available docs
112	Nuclear Regulatory Commission	20 Documents (223 pp), list of publicly available documents
113	National Institutes of Health	No Documents, refer to HHS request
144	Department of Commerce	No Documents
146	US Agency for International Development	36 Documents (185 pp)
152	Department of Homeland Security	6 Documents (81 pp)
169	Drug Enforcement Agency	1 Document (29 pp)
68 Mgmt. Division 171 Criminal Division	Department of Justice	2 Documents (281 pp) 3 Documents (26 pp)
176	Department of Transportation	59 Documents (382 pp), 99 withheld
250	National Geospatial-Intelligence Agency	3 Documents (81 pp)
* 11	National Archives and Records Administration	No Documents
* 23	Department of the Army	Request denied, too broad Follow-up pending, Army General Counsel
* 26	Department of Energy	12 Documents (177 pp)
42 * 186 – new request	Federal Bureau of Investigation	2 Documents (6243 pp) - request too broad Request denied – no documents Appeal pending
* 140	Centers for Disease Control	Request pending (not yet acknowledged)
* 160	Customs and Border Protection	Request pending (not yet acknowledged)
* 260+	Central Intelligence Agency	Request pending (acknowledged 3/29/05)
* 260+	Citizenship and Immigration Service	Request pending (acknowledged 2/28/05)
* 260+	Defense Intelligence Agency	Request pending (acknowledged 3/17/05)
* 260+	Department of Defense	Request pending (acknowledged 3/9/05)
* 260+	Department of Interior	Request pending (acknowledged 2/28/05)
* 260+	Department of Health and Human Services	Request pending (acknowledged 2/28/05)
* 260+	Immigration and Customs Enforcement	Request pending (acknowledged 6/8/05)

* All figures shown with * are dates and figures that differ from the standard methodology.

© 2006, The National Security Archive

APPENDIX III
SENSITIVE UNLASSIFIED INFORMATION FOIA REQUESTS, BY PROCESSING TIME

DOE reported no record of receiving original request in 2/05, and therefore did not begin processing until a later date; this request was resent on 6/6/05. The initial request sent in 2/05 were sent to confirmed agency fax numbers and received a positive receipt of transaction, however for unknown reasons were never entered into the agency's tracking systems.

NARA -- agency final response letter was dated 3/14/05, but was never received by the Archive; after an inquiry, the response was resent on 9/19/05.

CBP request was resent on 7/18/2005 (originally sent to wrong office but was not forwarded; after inquiry, the Archive resent the request to Office of Regulations and Rulings).

CDC request was sent as an addition to the Audit, on 8/15/2005, based on information learned during our research for this report; the chart reflects the current time of processing since that request was sent.

FBI initial response advised that the request was too broad and suggested the Archive review the FBI Manual of Operations and Procedures and the Manual of Investigative Operations and Guidelines. On 6/9/05, the Archive filed a new, more specific request based on these manuals. The second request was subsequently denied as too broad; follow-up inquiries are pending.

© 2006, The National Security Archive

APPENDIX IV
SENSITIVE UNCLASSIFIED INFORMATION, POLICIES BY AGENCY

AGENCY	POLICY	AUTHORITY	GUIDANCE	DESIGNATION	REMOVAL	ACCESS	PROTECTION	FOIA
AID	Sensitive But Unclassified (SBU)	Internal 12 Foreign Affairs Manual (FAM) 540 [updated 4/25/02]	Broad categories, examples	Supervisory employee	No policy	Need-to-know AND background check	Moderate	Info exempt under FOIA = SBU Review case-by-case
AIR **	For Official Use Only (FOUO)	Internal DOD Dir. 5400.7-R 9/1/1998	FOIA Exemptions	Any employee	Originator OR designated official	Need-to-know AND government business	Moderate	Review
AIR **	Sensitive Information (Computer Security Act, 1987)	Statutory PL 100-235 [DOD 8500.1]	Broad definition	N/A	N/A	Need-to-know	N/A	Review
ARMY*	For Official Use Only (FOUO)	Internal Army Reg. 25-55 11/1/1997 Army Reg. 380-19 3/27/1998	FOIA Exemptions	Any employee	Originator OR other authority (FOIA reviewer)	Need-to-know AND government business	High – transmission	Review
CBP* †	Sensitive But Unclassified [For Official Use Only] Information	Internal DHS Directive 11042.1 [1/6/05]	Broad definition Categories/ examples	Any employee	Originator OR senior official	Need-to-know	Moderate	Review
CDC* †	Sensitive But Unclassified (SBU)	Internal CDC-02 Manual 7/22/2005	Categories Examples	Designated officials	Same	Need-to-know	Moderate	Review, authorization Suggested exemptions
CIA †								
CIS* †	Sensitive But Unclassified [For Official Use Only] Information	Internal DHS Directive 11042.1 [1/6/05]	Broad definition Categories/ examples	Any employee	Originator OR senior official	Need-to-know	Moderate	Review
DEA	DEA Sensitive	Internal Reference Booklet 8/2002	Broad definition categories	Senior officials	N/A	Need-to-know	High	LOU may be exempt from release under FOIA
DHS	Protected Critical Infrastructure Information (PCII)	Statutory 6 U.S.C. 131(3), Homeland Security Act 6 CFR 29	Broad categories Administrative requirements	PCII Program Office	No policy	Specified activities; Training; explicit authorization; AND non-disclosure agreement	Moderate	Specific authorization OR Exemption 3

© 2006, The National Security Archive

APPENDIX IV
SENSITIVE UNCLASSIFIED INFORMATION, POLICIES BY AGENCY

AGENCY	POLICY	AUTHORITY	GUIDANCE	DESIGNATION	REMOVAL	ACCESS	PROTECTION	FOIA
DHS	Sensitive But Unclassified [For Official Use Only] Information	Internal DHS Directive 11042.1 [5/04, updated 1/6/05]	Broad categories with examples	Any employee	Originator OR senior official	Need-to-know	Moderate	Review
DIA †								
DOA	Sensitive security information (SSI)	Internal, DR 3440-2 1/30/2003	Broad definition Categories Restriction on abuse	Senior officials [Head of Dept Org.]	Same	Need-to-know	Moderate	OGC authorization for release Ashcroft / Ex. 2, 4, 3, 7
DOC	No documents							
DOD* †	DoD Unclassified Controlled Nuclear Information (DOD UCNI)	Statutory 10 USC 128 DOD Dir. 5210.83 [11/15/1991]	Specific categories, guidance	Senior officials	N/A	Need-to-know AND U.S. citizen or government employee	Moderate	No disclosure under Exemption 3
DOD* †	For Official Use Only (FOUO)	Internal DOD Dir. 5400.7-R 9/1/1998	FOIA Exemptions	Any employee	Originator OR designated official	Need-to-know AND government business	Moderate	Review
DOD* †	Sensitive Information (Computer Security Act of 1987)	Statutory PL 100-235 [DOD 8500.1]	Broad definition	N/A	N/A	Need-to-know	N/A	Review
DOE	Unclassified Controlled Nuclear Information (UCNI)	Statutory 42 USC 2168, 10 CFR 1017.11 DOE Order 471.1A [update 6/30/00]	Categories, specific	Designated – Reviewing Officials	Same	Need-to-know	Moderate	Review
DOE	Official Use Only (OUO)	Internal DOE O 471.3 [4/903]	Broad definition Official guidance OR FOIA exemptions	Any employee	Guidance: any employee FOIA: originator	Need-to-know	Moderate	Review
DOI †								
DOJ	Limited Official Use (LOU)	Internal DOJ 2620.7 [9/1/1982, update 5/5/2005]	Broad definition, categories Limitation on abuse	Senior officials / designees	N/A	Need-to-know	Low	Review

© 2006, The National Security Archive

APPENDIX IV
SENSITIVE UNCLASSIFIED INFORMATION, POLICIES BY AGENCY

AGENCY	POLICY	AUTHORITY	GUIDANCE	DESIGNATION	REMOVAL	ACCESS	PROTECTION	FOIA
DOJ/ OIP	Request forwarded to DHS							
DOS	WMD / Other Sensitive Homeland Security Info	Internal, 4/4/02 Based on Card Memo	Definition, categories	Originator	No policy	Need-to-know	Moderate	Review Ashcroft Memo: exemptions 2, 4
DOS **	Sensitive But Unclassified (SBU)	Internal 12 Foreign Affairs Manual (FAM) 540 [updated 4/25/02]	Broad categories, examples	Originator	FOIA reviewer	Need-to-know AND Background check	Moderate	Info exempt under FOIA = SBU Review
DOT	Sensitive Security Information (SSI)	Statutory 49 CFR Part 15	Specified categories	Designated senior officials	Secretary, in writing	Need-to-know	Moderate	Exemption 3 GC authorization
EPA	Confidential Agency Information (CAI)	Internal *Information Sensitivity Compendium*, 7/02	Broad definition Categories/ examples	Originator or info. manager	No policy	Need-to-know	Moderate/ high	Review (maybe exemption 2, 5)
EPA	Confidential Business Information (CBI)	Internal *Information Sensitivity Compendium*, 7/02	Definition, Categories (FOIA)	Originator or info. manager	No policy	Need-to-know	Moderate/ high	Exemption 4
EPA	Enforcement-Confidential Information (ECI)	Internal *Information Sensitivity Compendium*, 7/02	Definition, Categories (FOIA)	Originator or info. manager	No policy	Need-to-know	Moderate	Exemption 7
FAA	For Official Use Only (FOUO)	Internal	Definition / FOIA	Senior officials	Originator	Need-to-know	Moderate	Review
FAA	Sensitive Security Information (SSI)	Statutory 49 CFR Part 15	Categories	Secretary [categories] Senior Officials	No policy	Need-to-know	Moderate	No release, Ex. 3
FBI †								
FEMA								
GSA	Sensitive But Unclassified (SBU) Building Information	Internal Public Building Service (PBS) Policy, 3/8/02	Categories, examples	N/A	N/A	Need-to-know	Moderate	Authorization Ashcroft memo
HHS †								

© 2006, The National Security Archive

APPENDIX IV
SENSITIVE UNCLASSIFIED INFORMATION, POLICIES BY AGENCY

AGENCY	POLICY	AUTHORITY	GUIDANCE	DESIGNATION	REMOVAL	ACCESS	PROTECTION	FOIA
HUD	No applicable documents							
ICE* †	Sensitive But Unclassified [For Official Use Only] Information	Internal DHS Directive 11042.1 [1/6/05]	Broad definition Categories/ examples	Any employee	Originator OR senior official	Need-to-know	Moderate	Review
NARA	No documents							
NASA	Administratively Controlled Information (ACI)	Internal [11/3/04]	Categories	Senior officials	Originator	Need-to-know	N/A	No disclosure unless clearly in accordance with law – FOIA Review
NAVY †								
NGA	For Official Use Only (FOUO)	Internal [6/2004], references DOD Directive 5200.1	FOIA Exemptions	Any employee	N/A	Need-to-know AND government business	Moderate	Review
NIH	No documents							
NRC	Safeguards Information (SGI)	Statutory Atomic Energy Act 10 CFR 73	Categories with examples	Senior officials or Designated officials	Originator	Need-to-know AND Background check	High	Review
NRC	Official Use Only (OUO)	Internal [12/20/99]	Categories / FOIA	Senior officials (branch chiefs) OR Contractor designee	Originator or originator's supervisor	Need-to-know	Moderate	Review
NRC	Proprietary Information (PROPIN)	Internal [12/20/99]	Categories / FOIA Ex. 4	Senior officials (branch chiefs) OR Contractor designee	Originator	Need-to-know	Moderate	Review / no release under exemption 4
NRC	Sensitive Homeland Security Information (SHSI)	Internal [4/4/02] Complies with DHS proposed regulations	Categories Examples	Designated staff	N/A	Need-to-know	N/A	Review per Ashcroft memo, exemptions 2, 4
NRO	For Official Use Only (FOUO)	Internal [updated 4/14/03]	Categories / FOIA	Any employee	N/A	Need-to-know	Moderate	Review

© 2006, The National Security Archive

APPENDIX IV
SENSITIVE UNCLASSIFIED INFORMATION, POLICIES BY AGENCY

AGENCY	POLICY	AUTHORITY	GUIDANCE	DESIGNATION	REMOVAL	ACCESS	PROTECTION	FOIA
NSF	Sensitive Information	Internal Memo 5/11/2000	N/A	Any employee	FOIA officer	Need-to-know	N/A	Review
OMB	No documents							
OPM	No documents							
SBA	No documents							
SEC	No documents							
SSA	No documents							
TRE	Sensitive But Unclassified Information (SBU)	Internal Directive [Card Memo, 4/4/02]	Card Memo	N/A	N/A	Need-to-know	Moderate	Review per Ashcroft Memo, Ex. 2, 4
TSA	Sensitive security info (SSI)	Statutory 49 CFR 1520.5	Categories 1520.7(a)-(r)	Any employee (info in given categories) OR Administrator (other info)	No policy	Need-to-know AND Non-disclosure agreement	Moderate	Review [FOIA officer and SSI Program Office]
TSA	Sensitive But Unclassified [For Official Use Only] Information	Internal DHS Directive 11042.1 [1/6/05]	Broad definition Categories/ examples	Any employee	Originator OR senior official	Need-to-know	Moderate	Review
TSA	Critical Infrastructure Information (CII)	Statutory 6 U.S.C. 131(3), Homeland Security Act						
VET	No applicable documents							

CHART KEY

Policy: Name/acronym for agency's policy regarding unclassified information that is otherwise protected
Authority: Statutory/regulatory or internal authority establishing or updating the policy
Guidance: Definition and/or other guidance to be followed by individuals in designating information under the policy
Designation: Individual(s) responsible for designating protected information within the agency
Removal: Individual(s) responsible for removing the designation of protected information

- Same: the same individual(s) who are allowed to designate protection are able to remove such protection
- Originator: only the specific individual (and in most cases the individual's supervisor(s) or successor) who made the original designation may remove it

Access: Qualification(s) for individuals who are authorized to access information protected under the policy

© 2006, The National Security Archive

APPENDIX IV
SENSITIVE UNCLASSIFIED INFORMATION, POLICIES BY AGENCY

Protection: Degree of protection generally applied to documents/electronic media containing information designated under the policy
FOIA: Specific guidelines for treatment of FOIA requests for information protected under the policy

N/A: Not available
No policy: Based on the information collected, the agency's policy includes no specific guidance on this matter

† The Archive's FOIA request is still pending with this Agency (see processing chart, Appendix III)
* The information given was not provided by the Agency, but rather is based on our own research or materials submitted by other agencies.
** This Agency provided some information, but none regarding this specific aspect of their policy; the noted information is based on research or inference from other given information.

© 2006, The National Security Archive

APPENDIX V
SENSITIVE UNCLASSIFIED INFORMATION, DISTINCT POLICIES

POLICY	AGENCY	DATE	AUTHORITY	GUIDANCE	DESIGNATION	REMOVAL	ACCESS	PROTECTION	FOIA
ACI / Administratively Controlled Information	NASA	11/3/2004	Internal NPR 1600.1	Categories (9)	Originating management official	Originator	Need-to-know	N/A	No disclosure except legal obligation (FOIA)
CAI / Confidential Agency Information	EPA	7/2002	Internal *Info. Sensitivity Compendium*	Broad definition, Categories with examples	Originator OR Information manager	No policy	Need-to-know	Moderate / High	Review / exemption 2 or 5
CBI / Confidential Business Information	EPA	7/2002	Internal *Info. Sensitivity Compendium*	Broad definition, Categories with Examples	Originator OR Information manager	No policy	Need-to-know	Moderate / High	Exemption 4
Computer Security Act Sensitive Information	DOD*	1/9/1988	Statutory PL 100-235 [DOD 8500.1]	Broad definition Categories	N/A	N/A	Need-to-know	Low	Review
DEA Sensitive	DEA DOD*	8/2002	Internal Reference Booklet	Broad definition categories, law enforcement-related	Senior officials	N/A	Need-to-know	High	LOU may be exempt from release under FOIA
ECI / Enforcement-Confidential Information	EPA	7/2002	Internal *Info. Sensitivity Compendium*	Broad definition, Categories with examples	Originator OR Information manager	No policy	Need-to-know	Moderate	Exemption 7
FOUO / For Official Use Only [DHS]	TSA DHS CBP* CIS* ICE*	5/2004 Update 1/6/2005	Internal DHS Directive 11042.1	Broad definition Categories with examples	Any employee	Originator OR Senior official	Need-to-know	Moderate	Review
FOUO / For Official Use Only [DOD]	DOD* AIR ARM* USN* NGA	9/1/1998	Internal DOD 5400.7-R	Categories (FOIA exemptions)	Any employee	Originator / designated officials	Need-to-know/ gov't business	Moderate	Review
FOUO / For Official Use Only [FAA]	FAA	6/13/2000	Internal FAA O 1270.1	Broad definition (based on FOIA)	Senior officials	Originator	Need-to-know	Moderate	Review

© 2006, The National Security Archive

APPENDIX V
SENSITIVE UNCLASSIFIED INFORMATION, DISTINCT POLICIES

POLICY	AGENCY	DATE	AUTHORITY	GUIDANCE	DESIGNATION	REMOVAL	ACCESS	PROTECTION	FOIA
FOUO / For Official Use Only [NRO]	NRO	10/5/1999 Update 1/31/2003	Internal NROD 50-12	Categories (FOIA exemptions)	Any employee	Originator (with senior authorization)	Need-to-know	Moderate	Review
LOU / Limited Official Use Information	DOJ	9/1/1982 Update 5/5/2005	Internal DOJ O 2620.7	Definition Categories Examples	Senior official OR other designated	N/A	Balancing test	Low	Review
OUO / Official Use Only [DOE]	DOE	4/9/2003	Internal DOE O 471.3	Broad definition with specific guidance OR FOIA exemption	Any employee	Originator OR supervisor, FOIA official	Need-to-know	Moderate	Review
OUO / Official Use Only [NRC]	NRC	6/2/1998 Update 12/20/1999	Internal MD 12.6	Categories (FOIA exemptions)	Senior officials, selected	Originator OR supervisor	Need-to-know	Moderate	Review
PCCI / Protected Critical Infrastructure Info	DHS	2002	Statutory 6 USC 131 6 CFR 29	Specific definition Categories	Designated official	Same	Need-to-know	Moderate	Authorization / Exemption 3
PROPIN / Proprietary Info	NRC	12/20/1999	Internal MD 12.6	Categories (FOIA Exemption 4)	N/A	Originator	N/A	Moderate	Exemption 4
SASI / Select Agent Sensitive Information	HHS* CDC*	2002	Statutory 42 USC 247d	Categories	Designated official	Same	Need-to-know	Moderate	Review / Authorization Exemptions 2, 3
SBU / Sensitive But Unclassified [CDC]	CDC*	7/22/2005	Internal CDC-02 Manual	Categories Examples	Designated official	Same	Need-to-Know	Moderate	Review / Authorization Suggested exs.
SBU / Sensitive But Unclassified [State]	DOS AID DOD*	4/25/2002	Internal 12 FAM 540	Categories FOIA	Supervisory Employees	No policy	Need-to-know Background ck	Moderate	Review
SBU / Sensitive But Unclassified Building Info [GSA]	GSA	3/8/2002	Internal PBS Order 3490.1	Specific categories with examples	Any employee	No policy	Need-to-know	Moderate	Only released with specific authorization
SGI / Safeguards Information	NRC	10/14/1980 Update 11/2/2001	Statutory Atomic Energy Act/10 CFR 73, MD 12.6	Categories Examples	Designated senior officials	Originator	Need-to-know Background ck	High	Review

© 2006, The National Security Archive

APPENDIX V
SENSITIVE UNCLASSIFIED INFORMATION, DISTINCT POLICIES

POLICY	AGENCY	DATE	AUTHORITY	GUIDANCE	DESIGNATION	REMOVAL	ACCESS	PROTECTION	FOIA
SHSI / Sensitive Homeland Security Information	FAA	2002	Statutory Homeland Sec. Act of 2002	Definition	Designated senior official	Same	Need-to-know State and local officials	Moderate	No release Exemption 3
SHSI / Sensitive Homeland Security Information	NRC	5/28/2002	Internal COMSECY-02-0015	Broad categories, with examples	Designated official	No policy	Need-to-know	Moderate	Review Ashcroft Memo
SSI / Sensitive Security Information [DOT]	DOT/FTA FAA	11/25/2002	Statutory 49 CFR Pt. 15.5	Definition Categories Examples	Senior officials / designated personnel	N/A	Need-to-know	Moderate	No release under Ex. 3 / Administrator's authorization for release
SSI / Sensitive Security Information [USDA]	USDA	1/30/2003	Internal DR 3440-2	Broad definition Categories Restriction	Senior officials	Same / Max 10 yrs	Need-to-know	Moderate	Authorization / suggested exemptions (Ashcroft)
UCNI / Unclassified Controlled Nuclear Information [DOD]	DOD*	10/1990 Updated 9/1998	Statutory 10 USC 128 DoD 5400.7-R	Specific definition/ categories	Senior officials / designees	No policy	Need-to-know US citizen Gov. emp.	Moderate	No release under Exemption 3
UCNI / Unclassified Controlled Nuclear Information [DOE]	DOE	Update 6/30/2000 [internal]	Statutory 42 USC 2168 10 CFR 1017.11 [DOE O471.1A]	Categories, specific	Designated officials	Originator OR FOIA officer	Need-to-know	Moderate	Review
Unclassified Technical Information	DOD*	11/6/1984	Statutory 22 USC 2751 DOD 5230.25	Categories Statutory	Heads of Components	Same	Contractors, need-to-know	N/A	Review Authorization
WMD, other Sensitive Homeland Security Info	TRE DOS	4/4/2002	Internal / Card Memo	Broad definition, categories	N/A	No policy	Need-to-know	Moderate	Ashcroft Memo Exemptions 2, 4

CHART KEY

Policy: Name/acronym for agency's policy regarding unclassified information that is otherwise protected

Agency: Agency or agencies that use the policy listed (where policy features are based on the same documents or authorities, and not merely where the same term is employed to define protected information)

Date: Date of origination date of policy and/or date of update to current policy (where available)

Authority: Statutory/regulatory or internal authority establishing or updating the policy

© 2006, The National Security Archive

APPENDIX V
SENSITIVE UNCLASSIFIED INFORMATION, DISTINCT POLICIES

Guidance: Definition and/or other guidance to be followed by individuals in designating information under the policy
Designation: Individual(s) responsible for designating protected information within the agency
Removal: Individual(s) responsible for removing the designation of protected information

- Same: the same individual(s) who are allowed to designate protection are able to remove such protection
- Originator: only the specific individual (and in most cases the individual's supervisor(s) or successor) who made the original designation may remove it

Access: Qualification(s) for individuals who are authorized to access information protected under the policy
Protection: Degree of protection generally applied to documents/electronic media containing information designated under the policy
FOIA: Specific guidelines for treatment of FOIA requests for information protected under the policy

N/A: Not available
No policy: Based on the information collected, the agency's policy includes no specific guidance on this matter

* The information given was not provided by the Agency, but rather is based on our own research or materials submitted by other agencies.

© 2006, The National Security Archive

APPENDIX VI
GLOSSARY OF ACRONYMS

ACI–administratively controlled information
AID–Agency for International Development
AIR–Department of the Air Force
ARMY–Department of the Army
ATOMAL–special handling designation for classified information containing atomic materials
CAI–confidential agency information (Environmental Protection Agency)
CBI–confidential business information (Environmental Protection Agency)
CBRN–chemical, radiological, biological, and nuclear (weapons)
CENTCOM–United States Central Command (Army)
CIA–Central Intelligence Agency
CONOPS–U.S. Army Intelligence Command Continental [United States] Operations; continuity of operations
CRS–Congressional Research Service
CUI–controlled unclassified information
DEA–Drug Enforcement Agency
DIA–Defense Intelligence Agency
DOC–Department of Commerce
DOD–Department of Defense
DOE–Department of Energy
DOI–Department of the Interior
DOJ–Department of Justice
DOL–Department of Labor
DOS–Department of State
DOT–Department of Transportation
ECI–enforcement-confidential information (Environmental Protection Agency)
EDU–Department of Education
EO–executive order
EPA–Environmental Protection Agency
EXDIS– Department of State special handling designation, "exclusive distribution to officers with essential need to know"
FAM–Foreign Affairs Manual (Department of State)
FAS–Federation of American Scientists
FBI–Federal Bureau of Investigation
FEMA–Federal Emergency Management Agency
FOIA–Freedom of Information Act
FOUO–for official use only
FRD–formerly restricted data
GAO–Government Accountability Office
GPO–Government Printing Office
GSA–General Services Administration
HHS–Department of Health and Human Services
HIS–homeland security information
HUD–Department of Housing and Urban Development
ISOO–Information Security Oversight Office
LIMDIS–Department of State special handling designation, "Distribution limited to officers, offices, and agencies with the need to know, as determined by the chief of mission or designee"
LOU–limited official use
NARA–National Archives and Record Administration
NASA–National Aeronautics and Space Administration
NATO–North Atlantic Treaty Organization; also special handling designation for NATO classified information
NGA–National Geospatial-Intelligence Agency
NODIS–Department of State special handling designation, "No distribution to other than addressee without approval of addresser or addressee"; used only on messages of the highest sensitivity between the President, the Secretary of State, and Chiefs of Mission.

© 2006, The National Security Archive

APPENDIX VI
GLOSSARY OF ACRONYMS

NOFORN–Department of State special handling designation "intelligence which . . . may not be provided in any form to foreign governments, international organizations, coalition partners, foreign nations, or immigrant aliens without originator approval"
NRC–Nuclear Regulatory Commission
NSC–National Security Council
NSF–National Science Foundation
OIP–Office of Information and Privacy, U.S. Department of Justice
OMB–Office of Management and Budget
OPLANS–operation plans
OPM–Office of Personnel Management
OPSEC–operations security
OUO–official use only
PCII–protected critical infrastructure information
PD–Presidential Directive
PROPIN–proprietary information
RD–restricted data
SBA–Small Business Administration
SBU–sensitive but unclassified
SEC–Securities and Exchange Commission
SGI-M–safeguards information-modified handling
SGI–safeguards information
SHSI–sensitive homeland security information
SIOP-ESI–Single Integrated Operations Plan-Extremely Sensitive Information, Department of Defense special handling designation for classified information
SI–sensitive information
SOF–special operations force(s); strategic offensive forces; status of forces
SPECAT–special category designations for classified information, used by Department of Defense
SSA–Social Security Administration
SSI–sensitive security information
SUI–sensitive unclassified information
UCNI–unclassified controlled nuclear information
USDA–U.S. Department of Agriculture
WHS/DFOISR–Department of Defense, Washington Headquarters Services, Directorate of Freedom of Information and Security Review
WMD–weapons of mass destruction

© 2006, The National Security Archive

JIM BUNNING
KENTUCKY

COMMITTEES:
FINANCE
ENERGY AND NATURAL RESOURCES
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET

United States Senate

WASHINGTON, DC 20510

WASHINGTON OFFICE:
316 HART SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-4343

MAIN KENTUCKY OFFICE:
1717 DIXIE HIGHWAY, SUITE 220
FORT WRIGHT, KY 41011
(859) 341-2902

March 14, 2006

The Honorable Christopher Shays
Chairman
Subcommittee on National Security, Emerging
Threats and International Relations
B-372 RHOB
Washington, D.C. 20515

Dear Chairman Shays:

I understand your Subcommittee on National Security, Emerging Threats and International Relations will hold an oversight hearing on March 14, 2006 regarding the handling of sensitive government information. While I believe that federal agencies and the executive branch must have the authority to protect certain information involving our national security to the fullest extent, I share your concern for ensuring only information truly impacting national security should be classified and kept from the public.

Government needs to protect classified information in a cost-effective manner. If we are not protecting "Secret" information with the most advanced tools, we are wasting taxpayer monies and compromising national security. The fact that much of this classified material could be declassified can make the waste even greater.

In 1999, I joined six other Senators in a bi-partisan letter urging the Department of Defense to spend funds appropriated for the improvement of storage of classified information by defense contractors (copy attached). We appropriated monies so defense contractors could replace old "bar-lock" file cabinets with new GSA compliant containers and electronic locks that deter today's lock-picking methods. However, the DOD refused to spend the money to upgrade contractor storage. In the letter and the attached White Paper, we argued that the refusal to upgrade had real cost impacts on the government because it required contractors to employ "supplemental" security to make up for shortcomings in the antiquated locks and containers. By not spending that money, the government has wasted hundreds of millions of dollars over the last seven years on avoidable measures if DOD contractors would have upgraded their storage.

Further, these lock bar cabinets must contain an enormous number of documents – both classified and unclassified – that need the review your subcommittee is proposing. Forcing contractors to upgrade antiquated containers also forces declassification decisions, thus reducing the bulk of information kept in classified storage. The result is improved security for real classified documents with cost savings to the taxpayer.

Best personal regards,

Jim Bunning

JIM BUNNING
Unites States Senator

HAZARD OFFICE:
MAIN STREET
SUITE 2
HAZARD, KY 41701
(606) 435-2360

HOPKINSVILLE OFFICE:
1108 SOUTH MAIN STREET
SUITE 12
HOPKINSVILLE, KY 42240
(270) 885-1212

LEXINGTON OFFICE:
771 CORPORATE DRIVE
SUITE 105
LEXINGTON, KY 40503
(859) 219-2228

LOUISVILLE OFFICE:
600 DR. MARTIN LUTHER KING JR. PLACE
ROOM 10728
LOUISVILLE, KY 40202
(502) 582-6301

OWENSBORO OFFICE:
423 FREDERICA STREET
ROOM 205
OWENSBORO, KY 42301
(270) 689-9005

Toll-Free 1-800-283-8583
http://bunning.senate.gov

United States Senate

September 9, 1999

The Honorable William S. Cohen
Secretary
U.S. Department of Defense
The Pentagon
Washington, DC 20301

Dear Mr. Secretary:

We are writing regarding the Department of Defense (DOD) program to upgrade locks for safes used to store classified information. As recent events have unfortunately shown, our government's record for protecting the nation's secrets has been highly deficient. Given this situation, we are concerned as to why DOD officials continue to adamantly resist lock upgrades, especially when Congress has expressed strong support for the retrofit program because of the substantive security concerns involved. We believe your personal involvement in this issue is necessary for its successful and proper resolution.

Specifically, we have been informed that the DOD is reluctant to extend its retrofit of Federal Specification FF-L-2740 compliant electronic locks to Defense contractors. We understand that the DOD has devoted approximately $10 million annually for the last six years to retrofit its internal mechanical locks, and now virtually all internal DOD mechanical locks have been replaced on containers storing classified materials. Unfortunately, the safes of Defense contractors holding classified materials continue to have old mechanical locks which can be easily defeated. Last year Congress provided funds to begin retrofitting contractor safes, but we understand that the DOD has not obligated $4.8 million of the FY99 appropriation for this purpose because it does not want to require contractors to upgrade. In addition, Congress is providing another $10 million in the FY00 appropriation to upgrade locks on contractor safes, further indicating our concern for national security and the commitment to this effort.

The rationale for the DOD's resistance in implementing the contractor lock retrofit program is not rigorous. Indeed, it is so weak as to be disrespectful of the serious, substantive security concerns that have motivated Congress to support lock upgrades. We do not understand how the DOD can be satisfied with a lower level of security for sensitive information in its contractors' possession than for the same information in its own possession. By contrast, since the Los Alamos debacle, the Department of Energy, under Secretary Richardson's leadership, has started a lock retrofit program which does not distinguish between classified information held by the department or a contractor. The DOD needs to do the same without further delay.

The DOD should institute the contractor lock upgrade program to substantially enhance the security of our nation at a reasonable cost. To begin this task, we expect the release and utilization of Congress's FY99 appropriation of $4.8 million for contractor lock upgrades. As

well, we also expect the DOD to use the $10 million in FY00 funds appropriated by Congress for contractor lock upgrades. We urge you to include this upgrade program in the DOD budget in the coming years until this lock retrofit program is complete. Attached is a White Paper providing an analysis of this issue.

We trust you will agree with the serious, substantive security concerns that have motivated Congress for years to appropriate funds for lock upgrades. We respectfully ask that you personally review this situation and implement the contractor lock program without further delay. We anxiously await your response regarding this issue of U.S. national security.

Sincerely,

Senator Jim Bunning

Senator J. Robert Kerrey

Senator Jon Kyl

Senator Mitch McConnell

Senator Charles S. Robb

Senator Jeff Sessions

Senator Richard C. Shelby

cc: Senator John W. Warner
Chairman
Senate Armed Services Committee

Senator Carl Levin
Ranking Minority Member
Senate Armed Services Committee

Senator Ted Stevens
Chairman
Senate Appropriations Committee
Subcommittee on Defense

Senator Daniel K. Inouye
Ranking Minority Member
Senate Appropriations Committee
Subcommittee on Defense

White Paper
Adhering to Security Equipment Standards

The Department of Defense (DOD) reports that it has largely completed the upgrading of its own locks within the department to meet the GSA-promulgated federal lock specification.

The federal lock specification – FF-L-2740 – was developed in 1989 by an interagency committee in response to vulnerabilities created by the advent of portable computing. Today, scores of millions of highly capable "laptops" exist, making it easy (a matter of minutes) for foreign intelligence agents to "crack" any DOD or Defense contractor safe having a mechanical lock. The 1989 specification provides that a safe lock should be secure enough to require at least 20-person-hours of effort to affect a "surreptitious entry" – that is, an entry undetectable even upon expert inspection. Surreptitious entry is what allows "insiders" to make repeated unauthorized entries into safes without being readily discovered by our security officials. No mechanical lock does or can meet the current federal lock specification.

As noted, DOD has retrofitted its own safes with electronic locks, but refuses to require Defense contractors to do the same, even though Congress has appropriated funds for this purpose - $4.8 million in FY99 appropriations, with $10 million to be appropriated in FY00. DOD should not, however, be satisfied with a lower level of security for sensitive information in its contractor's possession than for the same information in its own possession. Since the Los Alamos debacle, the Energy Department, under Secretary Richardson's leadership, has started a retrofit program which does not distinguish between information in the department's hands or that in one of its contractor's hands.

DOD officials argue that lock upgrades are not a high priority because the chief threat is posed not by burglars, but by "insiders". No one disputes that "insiders" pose the greatest threat. It is precisely for that reason that lock upgrades are important. Though better locks will not prevent an "insider" from misappropriating information in a safe to which he has authorized access, they can prevent him from stealing material in other safes at his work. This is of high value.

In asserting that lock upgrades are "not a priority" DOD officials have specified certain higher priorities, such as protection of information systems, forces and critical infrastructure. Safe locks, however, are a crucial element of security for all of these other priorities. Regarding computer security, for example, backup tapes are stored in safes and in especially sensitive projects, computer hard drives are removed nightly and stored in safes. It makes no sense to assert that computer security is a high priority and then to refuse to upgrade locks required to protect those tapes and hard drives.

Electronic locks meeting the federal lock specification are also enhanced with "clock chips" that provide an audit trail – reports on which combinations were used to open the locks on which days, what times, and when the locks were closed. This feature serves as an effective tool for detecting suspicious behavior, assisting investigations and holding individuals accountable for their actions. Private companies using electronic locks have enthusiastically embraced this audit trail feature.

Several billion dollars a year is spent securing classified documents. The primary security cost is supplemental controls, such as rent-a-cop services, alarms, fences and access control systems (a.k.a. security in-depth). They are expensive, but they are ineffective against the "insider". Safes with locks meeting the GSA standard are much less expensive and severely limit the damage an "insider" can do when "need to know" principles are properly applied. The federal government has spent approximately $15 million dollars this year on GSA-approved safes and locks. Given the minuscule percentage of our security budget needed to purchase proper storage equipment, the practice of using sub-standard equipment is undesirable and improper.

The DOD has countered lock upgrade advocates by saying it is unaware of any incidents in which its safes have been cracked; however, if foreign intelligence services, perhaps using insiders, are succeeding in making surreptitious entries of our safes, then by definition there would be no evidence of the incidents. We train our own intelligence personnel to defeat lock systems surreptitiously. We know that they do so successfully and that foreign intelligence agencies train their operatives similarly. We must assume they too are successful on occasion, even (perhaps especially) against us.

We are aware of two publicly reported examples where foreign intelligence services gave technology to an "insider" to enhance his ability to gather classified information surreptitiously. Published accounts of the Sergeant Johnson case report that technology was provided to the "insider" which identified the positions of the mechanical lock wheels allowing him to determine the combination to a vault storing classified material. In the Walker case, technology was reportedly provided that indicated the positions of mechanical cams on encryption machines allowing the decoding of highly sensitive "crypto' information.

There is a history in recent decades of "insiders" using technologies to gain access to information surreptitiously. We need to recognize that safe locks that can be defeated in minutes by laptop computers are not adequate. Furthermore, even if it were true that there is no history of foreign intelligence services compromising U.S. safes surreptitiously – an incredible proposition on its face – the ease in which new technology makes such compromises does justify a high priority for upgrading of safe locks.

A contractor lock retrofit program would cost approximately $45-60 million if done efficiently by issuing locks as government furnished materials. The DOD has tended to grossly overstate the program cost. In 1993, the DOD estimated $500 million as the price of a departmental lock retrofit program. That program is now nearing completion and the total spent to date has been approximately $59 million dollars.

LAMAR WALDRON

PO BOX 6638 Marietta, GA 30065 lamarwaldron@yahoo.com (770) 977-8655

March 9, 2006

Congressman Christopher Shays, Chairman
Subcommittee on National Security, Emerging Threats, and International Relations
U.S. House of Representatives
B-372 Rayburn House Office Building
Washington, D.C. 20515

Dear Mr. Shays:

I wanted to provide you with the following information for your March 14, 2006 Hearing regarding the recently-disclosed Reclassification Program at the National Archives. Those Reclassification efforts may have affected two important groups of records which remain unresolved from the work of the JFK Assassination Records Review Board, which was created by Congress as part of JFK Act, which Congress passed unanimously in 1992.

It would be a shame if those two groups of unresolved JFK records had been--or might in the future--be subject to Reclassification, before their contents had been even generally been made known to Congress and the American people. The unresolved records involve two groups, one of which consists of "well over one million CIA records" related to the assassination that remained unreleased as of 2000, according to a detailed report prepared that year by OMB Watch. The other unsolved group includes files the Secret Service admitted destroying in January 1995, copies of which might still exist in the files of other agencies. Both groups of records also impact the case of Secret Service Agent Abraham Bolden, whom some consider the first National Security Whistleblower--a general topic your subcommittee's brought welcome attention to last month.

1. Could any of the "well over one million CIA records" be Reclassified?

In December 2000, OMB Watch issued a report entitled "A Presumption of Disclosure: Lessons from the John F. Kennedy Assassination Records Review Board" (available online at ombwatch.org). As part of the report, they had interviewed "two...former Board members...a staff member" of the Board and "an employee of the National Archives and Records Administration who functioned as its liaison with the Board." One of them stated that "'well over a million CIA records' are still outstanding."

That raises an obvious question in regards to the Reclassification Program. Is it possible that the "million CIA records" which are still outstanding, and have not yet been made available to Congress, historians, or the American public, could be Reclassified? Could other files related to those records--such as the Foreign Relations of the United States (FRUS) series--be Reclassified?

According to one journalist, the Reclassification program has not involved the JFK Assassination records collections. However, several of the FRUS records not designated as assassination-related by the Board--and thus possibly not in the JFK collection--are related to the relevant CIA files in question. And the status of the "million CIA records" is unclear: Are they at the Archives--and if so, are they part of the JFK collection)--or are the segregated at the CIA? The essential question whether those "million CIA records"--or other records related to them--are subject in any way to the Reclassification program?

According to a 1999 article for the American Historical Association by John W. Carlin, at that time the Archivist of the United States, the CIA and FBI had a "memoranda of understanding with the" JFK Assassination Records Review Board "giving them until September 1999 to complete their contributions to the (JFK) collection." For reasons noted below, it is likely that the "million CIA records" were provided or identified during this additional year following the last meeting of the Review Board (henceforth referred to as the ARRB), in September 1998.

I realize one of your witnesses next week is Dr. Anna Nelson, a former member of the ARRB. However, according to an e-mail sent to several authors and historians by Washington Post editor Jefferson Morley, Dr. Nelson stated to him that she didn't know anything about the "million CIA records" referred to the OMB Watch Report. That would make sense if those records were provided during the year following her last meeting with the ARRB, and is an indication that she may not be able to shed further light on that particular subject.

The "million CIA records"--and whether they are, have been, or will be subject to Reclassification--is highly relevant to will of Congress as expressed in their 1992 JFK Act and in relation to other records which the CIA and other agencies have withheld from Congress in past decades, but which were finally declassified by the ARRB.

It seems odd that agencies like the CIA would be reclassifying files before ever explaining to Congress and the public why crucial records from 1963 about covert operations to assassinate Castro that were infiltrated by the Mafia were withheld from so many Congressional committees.

Among the four million pages of files which were declassified by the JFK Records Review Board before it ceased operations in September 1998 were those concerning John and Robert Kennedy's "Plan for a Coup in Cuba," and the CIA's supporting role in that operation, code-named AMWORLD. It should be noted that those records had been almost completely withheld from not only the Warren Commission, but from several Congressional investigations. Those include the House Select Committee on Assassinations (HSCA), the committees commonly referred to as the Church Committee, the Pike Committee, the Nedzi Committee, the Watergate Committee, and the Iran-Contra Committee. The term AMWORLD, or information from its files, appears nowhere in the reports of those Committees, even though AMWORLD was the largest CIA operation devoted to the overthrow of Castro in 1963, and it involved CIA personnel investigated or interviewed by all of those Congressional committees. It was especially relevant to the work of the HSCA and Church Committees, since CIA and FBI files confirm that AMWORLD had been infiltrated by associates of the two Mafia godfathers the HSCA determined had the motive and means to assassinate JFK, Carlos Marcello of Louisiana and Santo Trafficante of Tampa. Both of them later confessed their roles in JFK's death to associates, and Robert Kennedy himself told associates that Marcello was behind JFK's assassination.

The declassified term AMWORLD has never appeared in any Congressional report and did not appear in print for the public until November 2005, in a book-length study entitled "Ultimate

Sacrifice," by myself and Thom Hartmann. Likewise, that was the first time historians and the public were made aware that CIA files confirmed the Mafia infiltration of AMWORLD. Though a small number of AMWORLD documents were declassified in the early 1990s through the CIA Historical Review Program, it is my understanding that the staff of the ARRB had not been made aware of AMWORLD until about ten months prior to the end of their mandate. Several key AMWORLD documents were released in September 1998, but others bear release dates of January 1999. An August 24, 2004 search of the Archives online database for AMWORLD yielded 17 documents. A search on January 25, 2006 yielded 97 documents, though it's unclear if more AMWORLD documents were added to the collection or if they documents were there all along and were simply added to the online database.

The AMWORLD documents that have been released so far all discuss a vast number of people, meetings, and operations whose files have still not yet been released. Also, the CIA's copies of many of the "Plan for a Coup in Cuba" documents from 1963 (contained in the Archives Califano and Joint Chiefs files) have never been released. In addition, code-names and cover identities for CIA personnel investigated by several Congressional Committees--such as David Atlee Phillips and Manuel Artime--are revealed in AMWORLD files for the first time, having been withheld from the Congressional investigators looking into them. For all those reasons, I feel that the majority of the "one million CIA files" are related to AMWORLD and the Plan for a Coup in Cuba.

One of those related operations involved a Cuban exile organization organized by CIA officer David Atlee Phillips, called the DRE, whose members had a highly-publicized encounter with Lee Harvey Oswald in August of 1963. The CIA if currently fighting a lawsuit brought by Jefferson Morley of the Washington Post, who has sued for the release of those documents. The CIA has acknowledged that more than 1,000 exist, but refuses to turn them over. Further, in the late 1970s when the HSCA tried to identify the CIA of the DRE, the CIA claimed it couldn't find any such person, though it appointed a CIA officer to assist them, named George Joannides. It was only decades later that the HSCA's Executive Director, G. Robert Blakey, found out that Joannides himself had been the DRE's handler during 1963. Blakey stated to PBS "Frontline" in 2003 that because of that deliberate deception "I no longer believe that we were able to conduct an appropriate investigation of the Agency and its relationship to Oswald." He adds that "the Agency set up a process that could only have been designed to frustrate the ability of the committee in 1976-79 to obtain any information that might adversely affect the Agency."

In light of that still-unexplained CIA deception of Congress, and the CIA's refusal to release the documents about Oswald, the DRE, and Joannides it seems ill-advised to allow the CIA to reclassify documents without proper oversight, especially in light of the remaining "one million CIA files" that have yet to be released.

Just as historian Matthew Aid's recent article about the Reclassification Program showed some files were being reclassified simply to avoid embarrassing an agency (like the CIA's 1950 Korean report), the CIA probably withheld AMWORLD and the Plan for a Coup in Cuba documents from Congress to avoid embarrassment or focusing suspicion on some of their personnel who were involved with the Mafia. But the CIA wasn't the only agency withholding files from Congress--the DIA coordinated with AMWORLD and had a big role in the Plan for a Coup in Cuba, and almost none of their files on those matters have ever been released. Again, to allow the DIA and CIA to reclassify material without the proper oversight or justification seems ill-advised in light of their past history.

2. Could records being Reclassified shed light on JFK records destroyed in 1995?

The second group of records which could be adversely affected by the Reclassification Program are the 1963 records which the Final Report of the ARRB confirmed were destroyed in January 1995. These were destroyed by the Secret Service. While it is not clear from news reports if the Secret Service is involved in the Reclassification Program, that's not the point. The point is that other agencies, such as the CIA or DIA, may have had copies of the Secret Service files or--more likely--their own records from the time which could shed light on what was in the destroyed files. These files are highly relevant to the case of Abraham Bolden, the Secret Service agent who tried to become a whistleblower and wound up being sent to prison for six years.

It's remarkable that the document destruction described on Page 149 of the ARRB's Final Report has not received more attention from Congress, since it clearly shows how the will of Congress and the JFK Act was flaunted by the Secret Service. It says that:

> "...In January 1995, the Secret Service destroyed presidential protection survey reports for some of President Kennedy's trips in the fall of 1963. The Review Board learned of the destruction approximately one week after the Secret Service destroyed them, when the Board was drafting its request for additional information. The Board believed that the Secret Service files on the President's travel in the weeks preceding his murder would be relevant."

The Secret Service then gave the ARRB its explanation for the destruction. However, the ARRB's Final Report goes on to say that

> "...the Review Board sought information regarding a protective intelligence file on the Fair Play for Cuba Committee (FPCC) and regarding protective intelligence files relating to threats to President Kennedy in the Dallas area (the Dallas-related files were disclosed to the Warren Commission). The FPBCC and Dallas-related files apparently were destroyed and the Review Board sought any information regarding the destruction. As of this writing, the Service was unable to provide any specific information regarding the disposition of these files. The Secret Service submitted its Final Declaration of Compliance dated September 18, 1998, but did not execute it under oath. The Review Board asked the Service to re-submit its Final Declaration."

The January 1995 destruction of the files about JFK's trips just prior to Dallas take on added significance when you realized that shortly before that, in November 1994, the ARRB had been informed for the first time of an attempt to assassinate JFK in Tampa, Florida on November 18, 1963 (four days before Dallas). That attempt was covered up at the time because of National Security considerations surrounding the Coup Plan/AMWORLD. The Tampa attempt was withheld from the Warren Commission and all later Congressional committees. Only one small newspaper article about it appeared the day after JFK died, which I and my co-author uncovered after combing through thousand of pages of newspaper microfilm. I informed the ARRB about the Tampa attempt in November 1994, as did Tampa author Frank DeBenedictis. The fact that DeBenedictis and I provided written submissions to the ARRB in November 1994 is confirmed in the ARRB's FY 1995 Annual Report.

It's likely that other agencies, like the CIA, FBI, DIA, and others, had or have today information about the Tampa attempt, either their own information or copies of information obtained in 1963 from the Secret Service. I later interviewed the Tampa Police Chief from November 1963, who described the security effort to thwart the threat as being quite extensive and involving many agencies. That thought that the CIA or others might be allowed to reclassify information that

could shed light on that attempt seems to go against the will of Congress as expressed in the 1992 JFK Act.

It seems bizarre that a single November 1963 newspaper article contains quotes from a Secret Service report about the Tampa suspect, when the report itself no long exists--at least from the Secret Service. The FPCC document destruction referred to in the ARRB Final Report is also relevant, since a key suspect in the Tampa attempt was linked to the Tampa FPCC.

Ensuring that material in the files of other agencies related to the Tampa attempt or the Secret Service document destruction is not reclassified is very important, not just for history but for the case of former Secret Service agent Abraham Bolden. Agent Bolden tried to be a whistleblower, and was going to Washington, where he could have told Warren Commission staff about Secret Service laxity, an earlier plot to assassinate JFK in Chicago on November 2, 1963 (3 weeks before Dallas), and the Tampa attempt.

Instead, Bolden was arrested the day he arrived in Washington. Bolden had been an upstanding agent, but he was eventually convicted and sentenced to six years in prison even though his main accuser later admitted committing perjury against him, and Bolden's judge told the jury he thought Bolden was guilty. Bolden has been trying to clear his name ever since his release from prison. We present evidence in the book showing that Bolden was framed by Chicago Mafia associates of Santo Trafficante, including a CIA asset named Richard Cain whom CIA files show had infiltrated AMWORLD for the Mafia.

Any information which could help Bolden's case should not be subject to reclassification by the CIA, Secret Service, FBI or any other agency.

In conclusion, I would like to request that the above groups of documents be kept in mind as issues of reclassification are considered. I do realize that on occasion, there may be a legitimate need for agencies to reclassify certain material, especially in cases where the identity of a confidential informant or a covert US asset may be exposed. (In two instances where I have come across such information in files at the Archives, I have made Archives staff aware of it.)

However, stringent safeguards should be in place to make sure that agencies are not simply reclassifying information to avoid embarrassment. Independent historians, such as Dr. John Newman (a twenty year veteran of military intelligence) or Dr. David Kaiser of the Naval War College, could be used to review reclassification decisions to make sure they are justified.

In addition, before the agencies are given latitude to reclassify material on such a broad scale, shouldn't they be required to address the decades they withheld the crucial documents described above from Congress, and the material which is still withheld or was destroyed?

I appreciate your time and consideration of these matters.

Sincerely,

Lamar Waldron

Mr. SHAYS. We have two panels today and I will introduce the first panel. We have Professor Allen Weinstein, Archivist of the United States, National Archives and Records Administration; Mr. J. William Leonard, Director, Information Security Oversight Office, National Archives and Records Administration; Ms. Davi M. D'Agostino, Director, Defense Capabilities and Management, U.S. Government Accountability Office; Mr. Robert Rogalski, Acting Deputy Under Secretary of Defense, Counterintelligence and Security, Department of Defense; and Mr. Glenn S. Podonsky, Director, Office of Security and Safety Performance Assurance, U.S. Department of Energy. If all of you would stand, I will swear you in as is our practice.

Raise your right hands.

[Witnesses sworn.]

Mr. SHAYS. For the record, all the witnesses have responded in the affirmative. We again thank you for your patience in hearing our perspectives. It hopefully will help you sense where we are coming from and the kinds of points that you need to make.

As you know, we have a 5-minute rule, but I roll over the clock if you go over. I just don't want you to think you have to stop right at 5, but as close to 5 as you can will be appreciated, and we will start with you, Professor.

STATEMENTS OF ALLEN WEINSTEIN, ARCHIVIST OF THE UNITED STATES, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION; J. WILLIAM LEONARD, DIRECTOR, INFORMATION SECURITY OVERSIGHT OFFICE, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION; DAVI M. D'AGOSTINO, DIRECTOR, DEFENSE CAPABILITIES AND MANAGEMENT, U.S. GOVERNMENT ACCOUNTABILITY OFFICE; ROBERT ROGALSKI, ACTING DEPUTY UNDER SECRETARY OF DEFENSE, COUNTERINTELLIGENCE AND SECURITY, U.S. DEPARTMENT OF DEFENSE; AND GLENN S. PODONSKY, DIRECTOR, OFFICE OF SECURITY AND SAFETY PERFORMANCE ASSURANCE, U.S. DEPARTMENT OF ENERGY

STATEMENT OF ALLEN WEINSTEIN

Mr. WEINSTEIN. Chairman Shays, Mr. Van Hollen, members of the subcommittee, I wish to thank you for holding this very important hearing today on issues relating to information access restrictions and for inviting me to testify. I am especially pleased to be joined this afternoon as a witness before the subcommittee by my able colleague, Bill Leonard, who heads the Information Security Oversight Office [ISOO], an office within the National Archives and Records Administration. Mr. Chairman, I appreciate the opportunity for Mr. Leonard and myself to share with you and other members of the subcommittee NARA's response to the situation which we have confronted in the past several weeks.

In late February, in response to complaints received from a group of historians and researchers regarding agency classification activity which has resulted in a number of historical documents being withdrawn from the open shelves at the National Archives and Records Administration, I began several actions as part of a review of the reclassification of documents.

Weeks ago, the Information Security Oversight Office [ISOO], initiated an audit to identify the number of records withdrawn from the open shelves over the past several years, to identify who initiated the withdrawal action, and to identify the authorization and justification for the withdrawal. The audit involves consultation with both affected agencies and with members of the research community. The audit will result in a public report designed to provide the greatest feasible degree of transparency to this classification activity, and the audit will be available within the next 60 days.

ISOO will issue annual updates providing insight into any similar activity conducted in the future, and these updates will be included in ISOO's annual report to the President on implementing Executive Order 12958, as amended.

Mr. Chairman, these immediate steps on my part were followed by consultations with concerned researchers, after which I announced additional actions as part of the ongoing investigation into the withdrawal of previously declassified records at the Archives. These steps included the imposition of a moratorium on other agency personnel identifying for withdrawal for classification purposes any—I stress any—declassified records currently on the public shelves at the National Archives until our audit is complete.

I also called for a summit with national security agencies involved with these withdrawal efforts. At the summit with Federal agency officials on March 6th, I stressed the commitment of the National Archives to maintain a balanced approach by acknowledging the importance of protecting national security while at the same time recognizing the public interest in having archival records maximally available. I stressed the commitment of the National Archives to continue to work cooperatively with the agencies while urging the agencies to move swiftly on returning documents back to the open shelves when appropriate. I stressed also the need to consider creating a National Declassification Initiative to replace the current agency-centered approach to declassification. This new initiative, the Centralized Declassification Program, would be coordinated by the National Archives.

Representatives of the Federal agencies who attended this summit unanimously agreed to support the moratorium on identifying for withdrawal any new material currently on the open shelves at the Archives. They were also supportive in principle of the concept of the National Declassification Initiative.

Mr. Chairman and members of the subcommittee, Bill Leonard will provide further details concerning NARA's and specifically ISOO's response to the challenges of implementing our recent directives and proposals.

As the Archivist of the United States, however, I am here today to bear witness to the seriousness with which the National Archives treats its responsibilities in this area. At the National Archives, the core goals of our mission statement commit us to preserving and processing records for opening to the public as soon as legally possible and providing prompt, easy, and secure access to our holdings.

Mr. Chairman, members of the subcommittee, I place an extremely high value on maintaining public credibility, trust, and re-

spect for the process of classification and the process of declassification, respect which is earned by responsible stewardship, including efforts to ensure that no information—I stress, no information—is withheld unnecessarily.

Thank you, Mr. Chairman and members of the subcommittee, for your time and attention.

Mr. SHAYS. Thank you, and let me take this opportunity to thank you for all of your good work.

Mr. WEINSTEIN. Thank you.

Mr. SHAYS. Thank you, sir.

[The prepared statement of Mr. Weinstein follows:]

Statement

Professor Allen Weinstein

Archivist of the United States

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 14, 2006

Chairman Shays, Mr. Kucinich, and members of the subcommittee, I wish to thank you for holding this very important hearing today on issues relating to information access restrictions and for inviting me to testify. I am especially pleased to be joined this morning as a witness before the Subcommittee by my able colleague, Bill Leonard, who heads the Information Security Oversight Office (ISOO), an office within the National Archives and Records Administration (NARA).

Mr. Chairman, I appreciate the opportunity for Mr. Leonard and me to share with you and other members of the Subcommittee NARA's response to the situation which we have confronted in the past several weeks.

I said at the time that "Inappropriate declassification can subject our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations to potential harm. Inappropriate classification (and reclassification) needlessly disrupts the free flow of information and can undermine our democratic principles which require that the American people be informed of the activities of their Government. This is not an either/or challenge. Deliberate, continuous effort is required to succeed at both. The American people expect and deserve nothing less and the National Archives is determined to fulfill its role in this process." I meant what I said.

In late February, in response to complaints received from a group of historians and researchers regarding agency classification activity which has resulted in a number of historical documents being withdrawn from the open shelves at the National Archives and Records Administration, I began several actions as part of a review of the reclassification of documents.

Several weeks ago, the Information Security Oversight Office initiated an audit to:

- Identify the number of records withdrawn from the open shelves over the past several years;
- Identify who initiated the withdrawal action;
- Identify the authorization and justification for the withdrawal;
- Through a statistically significant sample, determine the appropriateness of the classification action (i.e. was the action in accordance with the terms and limitations of E.O. 12958 [as amended] and does the information satisfy the standards for continued classification?);
- Examine the effectiveness of our own internal processes and procedures and make improvements where required.

The audit involves consultation with both affected agencies and members of the research community. The audit will result in a public report designed to provide the greatest feasible degree of transparency to this classification activity and will be available within the next 60 days.

As part of its continuing responsibility to oversee the Executive branch's security classification system, ISOO will issue annual updates providing insight into any similar activity conducted in the future. These updates will address the same issues and entail the same methodology used in the current audit and will be included in ISOO's annual report to the President on implementation of E.O. 12958, as amended.

These immediate steps on my part were followed by consultations with concerned researchers, after which I announced additional actions as part of the ongoing investigation into the withdrawal of previously declassified records at the National Archives. These steps included:

- The imposition of a moratorium on other agency personnel identifying for withdrawal for classification purposes any declassified records currently on the public shelves at the National Archives until the audit is complete.
- A "summit" with national security agencies involved with these withdrawal efforts within the next week. The purpose of this meeting is to ensure the proper balance of agency authority to restore classification controls where appropriate and my obligation to ensure maximum access to archival records consistent with law, regulation and common sense.
- A call upon affected agencies to join me in restoring to the public shelves as quickly as possible the maximum amount of information consistent with the obligation to protect truly sensitive national security information from unauthorized disclosure.
- The initiation of a review of National Archives internal processes for implementing agency classification/declassification decisions and the implementation of improvements to ensure that the National Archives remains a catalyst for timely public access.
- Directing the Information Security Oversight Office to develop, in consultation with affected agencies, clear and concise standardized guidance, with an appropriately high threshold, that will govern any future withdrawal of records

from the open shelves for classification purposes. This guidance will be promulgated prior to allowing future removal of any records from the open shelves for classification purposes and will be publicly available.
- Requesting the recently constituted Public Interest Declassification Board, consistent with its charter, to independently advise me on this issue.

At the "summit" with Federal agency officials on March 6, I stressed the following points:

- The commitment of the National Archives to maintain a balanced approach, by acknowledging the importance of protecting national security and at the same time recognizing the public interest in having archival records available;

- The commitment of the National Archives to continue to work cooperatively with the agencies, while urging the agencies to move swiftly on returning documents back to the open shelves, when appropriate;

- The need to establish a protocol and standards for the review of documents that agencies feel have been incorrectly placed on the open shelves;

- The need to consider creating a National Declassification Initiative to replace the current agency-centric approach to declassification. This proposal may address the bureaucratic structure, resources and policies needed to create a centralized declassification program coordinated by the National Archives.

Representatives of the Federal agencies attending the "summit" unanimously agreed to support the moratorium on identifying for withdrawal any new material that is currently on the open shelves at the National Archives. They also agreed to work towards creating new procedures for the review of materials and were supportive in principle of the concept of a National Declassification Initiative. Many agencies, however, acknowledged challenges to meeting both the December 2009 deadline for declassification of most documents more than 25-years old, in accordance with Executive Order 12958, as amended, and reexamining the previously withdrawn documents.

Mr. Chairman and members of the Subcommittee, Bill Leonard will provide further details concerning NARA's and specifically ISOO's response to the challenges of implementing our recent directives and proposals. As the Archivist of the United States, however, I am here today to bear witness to the seriousness with which the National Archives treats its responsibilities in this area. I will close my prepared remarks by stating to you what I said to the agency officials gathered in the conference room at NARA last week.

First, I want to thank the Office of the Director of National Intelligence for stating that "[the intelligence agencies will] continue to work with the National Archives to strike a balance between protecting truly sensitive national security information from

> unauthorized disclosure and ensuring that the public receives maximum access to unclassified archival records."
>
> As for the National Archives, the core goals of our mission statement commit us to preserving and processing records for opening to the public as soon as legally possible and providing prompt, easy and secure access to our holdings.

Mr. Chairman, I note in conclusion that I have placed (and continue to place) an extremely high value on maintaining public credibility, trust and respect for the process of classification and declassification, respect which is earned by responsible stewardship, including efforts to ensure that no information is withheld unnecessarily.

Thank you, Mr. Chairman and members of the Subcommittee for your time and attention.

Mr. SHAYS. Mr. Leonard.

STATEMENT OF J. WILLIAM LEONARD

Mr. LEONARD. Thank you, Mr. Chairman, Mr. Waxman, Mr. Van Hollen, other members of the subcommittee. I want to thank you for holding this hearing this afternoon on issues relating to information access restrictions as well as for inviting me to testify today.

The classification system and its ability to restrict the dissemination of information, the unauthorized disclosure of which would cause harm to our Nation, its citizens, and our institutions, represent the fundamental tool at the government's disposal to provide for the common defense. 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, which obtain assistance from 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.

As with any tool, the classification system is subject to misuse and misapplication. When information is improperly declassified or is not classified in the first place, although clearly warranted, our citizens, our democratic institutions, our homeland security, our interactions with foreign nations can be subject to potential harm. Conversely, too much classification, or the failure to declassify information as soon as it no longer satisfies the standards for continued classification, or inappropriate reclassification, unnecessarily obstructs effective information sharing and impedes an informed citizenry, the hallmark of our democratic form of government.

In the final analysis, inappropriate classification activity of any nature undermines the integrity of the entire process and diminishes the effectiveness of this critical national security tool. Consequently, inappropriate classification or declassification puts today's most sensitive secrets at needless increased risk.

Recent attention focused on withdrawal of previously declassified records from the open shelves of the National Archives exemplifies how the classification system can be misapplied. While an audit of this activity by my office is still underway and I do not want to presuppose final results, at this time, we see the need to address a number of issues that I have outlined in detail in my written statement.

In response to these challenges, I am pleased to report that the principal agencies involved in conducting classification reviews of records accessioned into the National Archives have agreed in principle to create a pilot National Declassification Initiative with the objective of more effectively integrating the work they are doing in this area. This initiative is intended to address the policies, procedures, structure, and resources needed to create a more reliable executive branch-wide declassification program. While the details of this proposal need to be further developed and implemented during

the weeks and months to come, I do anticipate significant progress in this area.

As Director of ISOO, I believe the keys to success of a National Declassification Initiative are to ensure that it has the authority, the expertise, and the resources to ensure that decisions to either declassify or to continue the classification of historically valuable permanent records of the Federal Government are appropriate and reflect the best informed judgment of all parties. There are a number of examples where a concerted executive branch-wide approach has worked in the past.

Furthermore, I believe that a National Declassification Initiative could assist in the development of standardized guidelines and protocols, provide a forum for agencies to better understand the various dynamics entailed in assessing and determining the appropriate action to take following a declassification review, and assure greater consistency in results. This initiative, representing a confederation of existing agency authorities, expertise, and resources, could also help fill critical training voids for agency personnel involved in declassification reviews. Ideally, we would eventually streamline the multiple independent agency reviews of the same material and therefore be substantively more efficient and effective than the current declassification review process.

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

Mr. SHAYS. Thank you very much.

[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 14, 2006

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.

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.

The classification system and its ability to restrict the dissemination of information the unauthorized disclosure of which would result in harm to our nation and its citizens represents a fundamental tool at the Government's disposal to provide for the "common defense." 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 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.

As with any tool, the classification system is subject to misuse and misapplication. When information is improperly declassified, or is not classified in the first place although clearly warranted, our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations can be subject to potential harm. Conversely, too much classification, the failure to declassify information as soon as it no longer satisfies the standards for continued classification, or inappropriate reclassification, unnecessarily obstructs effective information sharing and impedes an informed citizenry, the hallmark of our democratic form of government. In the final analysis, inappropriate classification activity of any nature undermines the integrity of the entire process and diminishes the effectiveness of this critical national security tool. Consequently, inappropriate classification or declassification puts today's most sensitive secrets at needless increased risk. .

Recent attention focused on the withdrawal of previously declassified records from the open shelves of the National Archives exemplifies how the classification system can be misapplied. While an audit of this activity by my office is still underway and I do not want to presuppose final results, at this time we see the need for the following:

- Develop an Executive branch-wide approach to declassification of records that better integrates individual agency efforts, is more reliable in results, and is more efficient in process
- Enhance agency understanding of each other's sensitive information
- Provide additional training that develops the needed understanding
- Establish centralized databases and other resources to facilitate sound declassification decisions
- Provide for greater consistency in the level of review applied to records
- Preclude redundancies in security reviews
- Increase the interface between declassification reviews done under the Executive order and those for other requests for access to information such as the Freedom of Information Act (FOIA)
- Establish centralized priorities
- Achieve greater rationalization of resources
- Improve oversight.

In response to these challenges, I am pleased to report that the principal agencies involved in conducting classification reviews of records accessioned into the National Archives have agreed, in principle, to create a pilot National Declassification Initiative, with the objective of more effectively integrating the work they are doing in this area. This initiative is intended to address the policies, procedures, structure and resources needed to create a more reliable Executive branch-wide declassification program. The details of this proposal need to be further developed and implemented during the weeks and months to come.

As Director of ISOO, I believe the keys to the success of a National Declassification Initiative are to ensure that it has the authority, expertise and resources to ensure the decisions to either declassify or continue the classification of historically valuable

permanent records of the Federal government are appropriate and reflect the best informed judgments of all parties. There are a number of examples where a concerted Executive branch-wide approach has worked in the past two decades, such as the Iran-Contra, POW/MIA, Chile-Pinochet, and Nazi War Crimes reviews.

Furthermore, I believe that a National Declassification Initiative could assist in the development of standardized guidelines and protocols, provide a forum for agencies to better understand the various dynamics entailed in assessing and determining the appropriate action to take following a declassification review, and ensure greater consistency in results. This initiative, representing a "confederation" of existing agency authorities, expertise, and resources, could also help fill critical training voids for agency personnel involved in declassification reviews. Ideally, it would eventually streamline the multiple, independent agency reviews of the same material, and therefore be substantially more fiscally prudent than the current declassification review process.

Recognizing that a focus of this hearing includes policies and procedures for handling Sensitive But Unclassified (SBU) information, it is important to articulate recent initiatives by the President to ensure the robust and effective sharing of terrorism information vital to protecting Americans and the Homeland from terrorist attacks. To that end, this past December the President announced a set of guidelines and requirements that represent a significant step in the establishment of the Information Sharing Environment (ISE) called for by section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). Specifically, in order to promote and enhance the effective and efficient acquisition, access, retention, production, use, management, and sharing of SBU information, including homeland security information, law enforcement information, and terrorism information, the President has mandated the standardization of procedures for designating, marking, and handling SBU information across the Federal Government. Clear milestones and accountability for achieving this goal have been laid out for the entire Executive branch.

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 at this time.

Mr. SHAYS. Ms. D'Agostino.

STATEMENT OF DAVI M. D'AGOSTINO

Ms. D'AGOSTINO. Good afternoon, Mr. Chairman and members of the subcommittee. I am pleased to be here today before you to discuss GAO's work on how the Departments of Energy and Defense, DOE and DOD, manage information that is unclassified but sensitive.

DOE and DOD use the designations, as you mentioned, Mr. Chairman, OUO and FOUO, respectively, to refer to this information. My testimony is based on our report that you released today here at this hearing on managing sensitive information at those Departments. Those Department base their programs, in large part, on the exemptions under the Freedom of Information Act [FOIA], that deal with information that is not national security classified but otherwise may be exempt from public release.

In this report, we reviewed the policies, procedures, and criteria the Departments use to manage OUO and FOUO information. We also looked at the Departments' training and oversight programs related to this and determined the extent to which those programs provide assurances that personnel properly identify and mark information.

In summary, DOE and DOD both have policies in place to implement their programs, but our analysis of these policies showed a lack of clarity in some key areas that could lead to inconsistencies and errors. First, DOD policies remain unclear as to which office is in charge of DOD's FOUO programs, since responsibilities shifted in October 1998 to what is now the Under Secretary of Defense for Intelligence. DOD officials have told us that at the end of January 2006, they started to coordinate a revised regulation that will emphasize management of the FOUO program.

Second, unlike DOE requirements, DOD policies do not require staff marking a document to note the FOIA exemptions used as a basis for designating it FOUO. In our view, if DOD required personnel to take the extra step of including the reason they are marking the document FOUO at the time they create it, it would help ensure that the personnel has made a thoughtful determination and improve the oversight of the program.

Third, both Departments' policies are unclear regarding what point a document should be marked as OUO or FOUO. If a document might contain such information but is not marked when it is created, you run the risk that the document might be mishandled and that risk increases.

Fourth, neither Departments' policies identify what would be an inappropriate use of the FOUO or OUO designation. Without such guidance, the Departments cannot be confident that their personnel will not use these markings to conceal mismanagement, inefficiencies, or administrative errors, or to prevent embarrassment.

Finally, neither Department has an agency-wide requirement that personnel be trained before they designate documents as OUO or FOUO, nor do they conduct oversight to ensure that information is appropriately identified and marked. Without training or oversight, neither Department can assure itself that personnel are complying with their own policies. We recommended that both Depart-

ments clarify their policies and guidance in these areas and establish training and oversight systems to conduct oversight periodically.

DOE and DOD agreed with most of our recommendations in their comments on our draft report. DOD did disagree that personnel designating a document as FOUO should also mark the document with the FOIA exemption or the reason that may apply. We continue to believe this recommendation has merit because it would cause personnel to make a more thoughtful determination before marking the document, and since it is provisional, it would not prejudice a separate independent decision to release or deny the release of a document under a FOIA request.

In closing, the lack of clear policies and effective training and oversight in DOE's and DOD's programs could result in over- and under-protection of unclassified yet sensitive government documents. Having clear policies and procedures in place can mitigate the risk of program mismanagement and help the Departments assure the OUO-FOUO information is appropriately marked and handled.

Mr. Chairman, members of the subcommittee, this concludes my oral statement. I would be happy to respond to any questions.

Mr. SHAYS. Thank you. There will be questions. Thank you so much.

[The prepared statement of Ms. D'Agostino follows:]

United States Government Accountability Office

GAO

Testimony

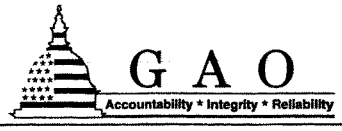
Before the Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. EST
Tuesday, March 14, 2006

MANAGING SENSITIVE INFORMATION

DOE and DOD Could Improve Their Policies and Oversight

Statement of Davi M. D'Agostino, Director
Defense Capabilities and Management, and
Gene Aloise, Director
Natural Resources and Environment



GAO-06-531T

March 14, 2006

GAO
Accountability Integrity Reliability

Highlights

Highlights of GAO-06-581T, a testimony to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives

MANAGING SENSITIVE INFORMATION

DOE and DOD Could Improve Their Policies and Oversight

Why GAO Did This Study

In the interest of national security and personal privacy and for other reasons, federal agencies place dissemination restrictions on information that is unclassified yet still sensitive. The Department of Energy (DOE) and the Department of Defense (DOD) have both issued policy guidance on how and when to protect sensitive information. DOE marks documents with this information as Official Use Only (OUO) while DOD uses the designation For Official Use Only (FOUO). GAO was asked to (1) identify and assess the policies, procedures, and criteria DOE and DOD employ to manage OUO and FOUO information; and (2) determine the extent to which DOE's and DOD's training and oversight programs assure that information is identified, marked, and protected according to established criteria.

What GAO Recommends

In its report issued earlier this month, GAO made several recommendations for DOE and DOD to clarify their policies to assure the consistent application of OUO and FOUO designations and increase the level of management oversight in their use. DOE and DOD agreed with most of GAO's recommendations, but partially disagreed with its recommendation to periodically review OUO or FOUO information. DOD also disagreed that personnel designating a document as FOUO should mark it with the applicable FOIA exemption.

www.gao.gov/cgi-bin/getrpt?GAO-06-581T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Davi D'Agostino at (202) 512-5431 or Gene Aloise at (202) 512-3841.

What GAO Found

As GAO reported earlier this month, both DOE and DOD base their programs on the premise that information designated as OUO or FOUO must (1) have the potential to cause foreseeable harm to governmental, commercial, or private interests if disseminated to the public or persons who do not need the information to perform their jobs; and (2) fall under at least one of eight Freedom of Information Act (FOIA) exemptions. While DOE and DOD have policies in place to manage their OUO or FOUO programs, our analysis of these policies showed a lack of clarity in key areas that could allow inconsistencies and errors to occur. For example, it is unclear which DOD office is responsible for the FOUO program, and whether personnel designating a document as FOUO should note the FOIA exemption used as the basis for the designation on the document. Also, both DOE's and DOD's policies are unclear regarding at what point a document should be marked as OUO or FOUO and what would be an inappropriate use of the OUO or FOUO designation. For example, OUO or FOUO designations should not be used to conceal agency mismanagement. In our view, this lack of clarity exists in both DOE and DOD because the agencies have put greater emphasis on managing classified information, which is more sensitive than OUO or FOUO.

In addition, while both DOE and DOD offer training on their OUO and FOUO policies, neither DOE nor DOD has an agencywide requirement that employees be trained before they designate documents as OUO or FOUO. Moreover, neither agency conducts oversight to assure that information is appropriately identified and marked as OUO or FOUO. DOE and DOD officials told us that limited resources, and in the case of DOE, the newness of the program, have contributed to the lack of training requirements and oversight. Nonetheless, the lack of training requirements and oversight of the OUO and FOUO programs leaves DOE and DOD officials unable to assure that OUO and FOUO documents are marked and handled in a manner consistent with agency policies and may result in inconsistencies and errors in the application of the programs.

Mr. Chairman and Members of the Subcommittee:

We are pleased to be here today to discuss our work on how the Departments of Energy (DOE) and Defense (DOD) use the designations Official Use Only (OUO) and For Official Use Only (FOUO), respectively, to manage information that is unclassified but sensitive. My testimony today is based on our report issued earlier this month entitled *Managing Sensitive Information: Departments of Energy and Defense Policies and Oversight Could Be Improved* (GAO-06-369). This report (1) identified and assessed the policies, procedures, and criteria that DOE and DOD employ to manage OUO and FOUO information; and (2) determined the extent to which DOE's and DOD's training and oversight programs assure that information is identified and marked according to established criteria.

In summary, both DOE and DOD base their programs on the premise that information designated as OUO or FOUO must (1) have the potential to cause foreseeable harm to governmental, commercial, or private interests if disseminated to the public or persons who do not need the information to perform their jobs; and (2) fall under at least one of eight Freedom of Information Act (FOIA) exemptions.[1] (See the appendix for a list and description of the exemptions of FOIA.) Both agencies have policies in place to implement their programs. However, our analysis of these policies showed a lack of clarity in key areas that could allow inconsistencies and errors to occur. Specifically:

- It is unclear which DOD office is responsible for the FOUO program, and whether personnel designating a document as FOUO should note the FOIA exemption used as the basis for the designation on the document.
- Both DOE's and DOD's policies are unclear regarding at what point a document should be marked as OUO or FOUO and what would be an inappropriate use of the OUO or FOUO designation. For example, OUO or FOUO designations should not be used to conceal agency mismanagement.

[1]Freedom of Information Act (5 U.S.C. sec. 552). FOIA exemption 1 solely concerns classified information, which is governed by Executive Order; DOE and DOD do not include this category in their OUO and FOUO programs since the information is already restricted by each agency's classified information procedures. In addition, exemption 3 addresses information specifically exempted from disclosure by statute, which may or may not be considered OUO or FOUO. Information that is classified or controlled under a statute, such as Restricted Data or Formerly Restricted Data under the Atomic Energy Act, is not also designated as OUO or FOUO.

In addition, while both DOE and DOD offer training on their OUO and FOUO policies, neither DOE nor DOD has an agencywide requirement that employees be trained before they designate documents as OUO or FOUO. Moreover, neither agency conducts oversight to assure that information is appropriately identified and marked as OUO or FOUO. This lack of training requirements and oversight leaves DOE and DOD officials unable to assure that OUO and FOUO documents are marked and handled in a manner consistent with agency policies and may result in inconsistencies and errors in the application of the programs.

We recommended that both agencies clarify their policies and guidance to identify at what point a document should be marked as OUO or FOUO and to define inappropriate uses of these designations. We also recommended that DOD clarify its policies as to which office is responsible for the FOUO program and that it require personnel designating a document as FOUO also to note the FOIA exemption they used to determine that the information should be restricted. With regard to training and management oversight, we recommended that both DOE and DOD require personnel to be trained before they can designate information as OUO or FOUO, and that they develop a system to conduct periodic oversight of OUO or FOUO designations to assure that their policies are being followed.

In commenting on our draft report, DOE and DOD agreed with most of our recommendations, but DOD disagreed that personnel designating a document as FOUO should also mark the document with the FOIA exemption used to determine that the information should be restricted. DOD expressed concern that an individual may apply an incorrect or inappropriate FOIA exemption and thus cause other documents that are created from the original to also carry the incorrect FOIA exemption or that the incorrect designation could cause problems if a denial is litigated. However, we believe that citing the applicable FOIA exemptions when marking a document will cause the employee to consider the exemptions and make a thoughtful determination that the information fits within the framework of the FOUO designation. Also, when the public requests documents, before DOD releases or denies release of the documents, FOIA experts review them, at which time an incorrect initial designation should be corrected. Our recommendation was intended to better assure appropriate consideration of the FOIA exemptions at the beginning of the process and we continue to believe that this recommendation has merit.

DOE and DOD Lack Clear OUO and FOUO Guidance in Key Aspects

Both DOE and DOD have established offices, designated staff, and promulgated policies to provide a framework for the OUO and FOUO programs. However, their policies lack sufficient clarity in important areas, which could result in inconsistencies and errors. DOE policy clearly identifies the office responsible for the OUO program and establishes a mechanism to mark the FOIA exemption used as the basis for the OUO designation on a document. However, our analysis of DOD's FOUO policies shows that it is unclear which DOD office is responsible for the FOUO program, and whether personnel designating a document as FOUO should note the FOIA exemption used as the basis for the designation on the document. Also, both DOE's and DOD's policies are unclear regarding at what point a document should be marked as OUO or FOUO, and what would be an inappropriate use of the OUO or FOUO designation. In our view, this lack of clarity exists in both DOE and DOD because the agencies have put greater emphasis on managing classified information, which is more sensitive than OUO or FOUO information.

DOE's Office of Security issued an order, a manual, and a guide in April 2003 to detail the requirements and responsibilities for DOE's OUO program and to provide instructions for identifying, marking, and protecting OUO information.[2] DOE's order established the OUO program and laid out, in general terms, how sensitive information should be identified and marked, and who is responsible for doing so. The guide and the manual supplement the order. The guide provides more detailed information on the applicable FOIA exemptions to help staff decide whether exemption(s) may apply, which exemption(s) may apply, or both. The manual provides specific instructions for managing OUO information, such as mandatory procedures and processes for properly identifying and marking this information. For example, the employee marking a document is required to place on the front page of the document an OUO stamp that has a space for the employee to identify which FOIA exemption is believed to apply; the employee's name and organization; the date; and, if applicable, any guidance the employee may have used in making this

[2]DOE Order 471.3, *Identifying and Protecting Official Use Only Information*, contains responsibilities and requirements; DOE Manual 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, provides instructions for implementing requirements; and DOE Guide 471.3-1, *Guide to Identifying Official Use Only Information*, provides information to assist staff in deciding whether information could be OUO.

determination.[3] According to one senior DOE official, requiring the employee to cite a reason why a document is designated as OUO is one of the purposes of the stamp, and one means by which DOE's Office of Classification encourages practices consistent with the order, guide, and manual throughout DOE. Figure 1 shows the DOE OUO stamp.

Figure 1: DOE's OUO Stamp

OFFICIAL USE ONLY

May be exempt from public release under the Freedom of Information Act (5 U.S.C. 552), exemption number and category: _____

Department of Energy review required before public release

Name/Org: _____ **Date:** _____

Guidance (if applicable): _____

Source: DOE.

With regard to DOD, its regulations are unclear regarding which DOD office controls the FOUO program. Although responsibility for the FOUO program shifted from the Director for Administration and Management to the Office of the Assistant Secretary of Defense, Command, Control, Communications, and Intelligence (now the Under Secretary of Defense, Intelligence) in October 1998, this shift is not reflected in current regulations. Guidance for DOD's FOUO program continues to be included in regulations issued by both offices. As a result, which DOD office has primary responsibility for the FOUO program is unclear. According to a DOD official, on occasion this lack of clarity causes personnel who have FOUO questions to contact the wrong office. A DOD official said that the department began coordination of a revised Information Security regulation covering the FOUO program at the end of January 2006. The new regulation will reflect the change in responsibilities and place greater emphasis on the management of the FOUO program.

[3]DOE classification guides used for managing classified information sometimes include specific guidance on what information should be protected and managed as OUO. When such specific guidance is available to the employee, he or she is required to mark the document accordingly.

DOD currently has two regulations, issued by each of the offices described above, containing similar guidance that addresses how unclassified but sensitive information should be identified, marked, handled, and stored.[4] Once information in a document has been identified as for official use only, it is to be marked FOUO. However, unlike DOE, DOD has no departmentwide requirement to indicate which FOIA exemption may apply to the information, except when it has been determined to be releasable to a federal governmental entity outside of DOD. We found, however, that one of the Army's subordinate commands does train its personnel to put an exemption on any documents that are marked as FOUO, but does not have this step as a requirement in any policy. In our view, if DOD were to require employees to take the extra step of marking the exemption that may be the reason for the FOUO designation at the time of document creation, it would help assure that the employee marking the document had at least considered the exemptions and made a thoughtful determination that the information fit within the framework of the FOUO designation. Including the FOIA exemption on the document at the time it is marked would also facilitate better agency oversight of the FOUO program, since it would provide any reviewer/inspector with an indication of the basis for the marking.

In addition, both DOE's and DOD's policies are unclear as to the point at which the OUO or FOUO designation should actually be affixed to a document. If a document might contain information that is OUO or FOUO but it is not so marked when it is first created, the risk that the document could be mishandled increases. DOE policy is vague about the appropriate time to apply a marking. DOE officials in the Office of Classification stated that their policy does not provide specific guidance about at what point to mark a document because such decisions are highly situational. Instead, according to these officials, the DOE policy relies on the "good judgment" of DOE personnel in deciding the appropriate time to mark a document. Similarly, DOD's current Information Security regulation addressing the FOUO program does not identify at what point a document should be marked. In contrast, DOD's September 1998 FOIA regulation, in a chapter on FOUO, states that "the marking of records at the time of their creation provides notice of FOUO content and facilitates review when a record is

[4]DOD 5400.7-R, *DOD Freedom of Information Act Program* (Sept. 4, 1998); DOD 5200.1-R, *Information Security Program* (Jan. 14, 1997); and interim changes to DOD 5200.1-R, *Information Security Regulation, Appendix 3: Controlled Unclassified Information* (Apr. 16, 2004).

requested under the FOIA."[5] In our view, a policy can provide flexibility to address highly situational circumstances and also provide specific guidance and examples of how to properly exercise this flexibility.

In addition, we found that both DOE's and DOD's OUO and FOUO programs lack clear language identifying examples of inappropriate usage of OUO or FOUO markings. Without such language, DOE and DOD cannot be confident that their personnel will not use these markings to conceal mismanagement, inefficiencies, or administrative errors, or to prevent embarrassment to themselves or their agency.[6]

Neither DOE nor DOD Requires Training or Conducts Oversight

While both DOE and DOD offer training to staff on managing OUO and FOUO information, neither agency requires any training of its employees before they are allowed to identify and mark information as OUO or FOUO, although some staff will eventually take OUO or FOUO training as part of other mandatory training. In addition, neither agency has implemented an oversight program to determine the extent to which employees are complying with established policies and procedures.

OUO and FOUO Training Is Generally Not Required

While many DOE units offer training on DOE's OUO policy, DOE does not have a departmentwide policy that requires OUO training before an employee is allowed to designate a document as OUO. As a result, some DOE employees may be identifying and marking documents for restriction from dissemination to the public or persons who do not need to know the information to perform their jobs, and yet may not be fully informed as to when it is appropriate to do so. At DOE, the level of training that employees receive is not systematic and varies considerably by unit, with some requiring OUO training at some point as a component of other periodic employee training, and others having no requirements at all.

[5]DOD 5400.7-R, C4.1.4, p.43.

[6]Similar language is included in DOD's policies regarding protection of national security information (DOD 5200.1-R, *Information Security Program* (Jan. 14, 1997), sec. C2.4.3.1). DOE's policy for protecting national security information (DOE M 475.1-1A) makes reference to Executive Order 12958, *Classified National Security Information*, as amended, which also has similar language.

DOD similarly has no departmentwide training requirements before staff are authorized to identify, mark, and protect information as FOUO. The department relies on the individual services and field activities within DOD to determine the extent of training that employees receive. When training is provided, it is usually included as part of a unit's overall security training, which is required for many but not all employees. There is no requirement to track which employees received FOUO training, nor is there a requirement for periodic refresher training. Some DOD components, however, do provide FOUO training for employees as part of their security awareness training.

Oversight of OUO and FOUO Programs Is Lacking

Neither DOE nor DOD knows the level of compliance with OUO and FOUO program policies and procedures because neither agency conducts any oversight to determine whether the OUO and FOUO programs are being managed well. According to a senior manager in DOE's Office of Classification, the agency does not review OUO documents to assess whether they are properly identified and marked. This condition appears to contradict the DOE policy requiring the agency's senior officials to assure that the OUO programs, policies, and procedures are effectively implemented. Similarly, DOD does not routinely conduct oversight of its FOUO program to assure that it is properly managed.

Without oversight, neither DOE nor DOD can assure that staff are complying with agency policies. We are aware of at least one recent case in which DOE's OUO policies were not followed. In 2005, several stories appeared in the news about revised estimates of the cost and length of the cleanup of high-level radioactive waste at DOE's Hanford Site in southeastern Washington. This information was controversial because this multibillion-dollar project has a history of delays and cost overruns, and DOE was restricting a key document containing recently revised cost and time estimates from being released to the public. This document, which was produced by the U.S. Army Corps of Engineers for DOE, was marked Business Sensitive by DOE. However, according to a senior official in the DOE Office of Classification, Business Sensitive is not a recognized marking in DOE. Therefore, there is no DOE policy or guidance on how to handle or protect documents marked with this designation. This official said that if information in this document needed to be restricted from release to the public, then the document should have been stamped OUO and the appropriate FOIA exemption should have been marked on the document.

In closing, the lack of clear policies, effective training, and oversight in DOE's and DOD's OUO and FOUO programs could result in both over- and underprotection of unclassified yet sensitive government documents. Having clear policies and procedures in place can mitigate the risk of program mismanagement and can help DOE and DOD management assure that OUO or FOUO information is appropriately marked and handled. DOE and DOD have no systemic procedures in place to assure that staff are adequately trained before designating documents OUO or FOUO, nor do they have any means of knowing the extent to which established policies and procedures for making these designations are being complied with. These issues are important because they affect DOE's and DOD's ability to assure that the OUO and FOUO programs are identifying, marking, and safeguarding documents that truly need to be protected in order to prevent potential damage to governmental, commercial, or private interests.

Mr. Chairman, this concludes GAO's prepared statement. We would be happy to respond to any questions that you or Members of the Subcommittee may have.

GAO Contacts and Staff Acknowledgments

For further information on this testimony, please contact either Davi M. D'Agostino at (202) 512-5431 or dagostinod@gao.gov, or Gene Aloise at (202) 512-3841 or aloisee@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals making key contributions to this testimony included Ann Borseth, David Keefer, Kevin Tarmann, and Ned Woodward.

Appendix: FOIA Exemptions

Exemption	Examples
1. Classified in accordance with an executive order[a]	Classified national defense or foreign policy information
2. Related solely to internal personnel rules and practices of an agency	Routine internal personnel matters such as performance standards and leave practices; internal matters the disclosure of which would risk the circumvention of a statute or agency regulation, such as law enforcement manuals
3. Specifically exempted from disclosure by federal statute	Nuclear weapons design (Atomic Energy Act); tax return information (Internal Revenue Code)
4. Privileged or confidential trade secrets, commercial, or financial information	Scientific and manufacturing processes (trade secrets); sales statistics, customer and supplier lists, profit and loss data, and overhead and operating costs (commercial/financial information)
5. Interagency or intra-agency memoranda or letters that are normally privileged in civil litigation	Memoranda and other documents that contain advice, opinions, or recommendations on decisions and policies (deliberative process); documents prepared by an attorney in contemplation of litigation (attorney work-product); confidential communications between an attorney and a client (attorney-client)
6. Personnel, medical, and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy	Personal details about a federal employee such as date of birth, marital status, and medical condition
7. Records compiled for law enforcement purposes where release either would or could harm those law enforcement efforts in one or more ways listed in the statute	Witness statements; information obtained in confidence in the course of an investigation; identity of a confidential source
8. Certain records and reports related to the regulation or supervision of financial institutions	Bank examination reports and related documents
9. Geographical and geophysical information and data, including maps, concerning wells	Well information of a technical or scientific nature, such as number, locations, and depths of proposed uranium exploration drill-holes

Sources: FOIA and GAO analysis.

[a]As noted earlier in this report, classified information is not included in DOE's and DOD's OUO and FOUO programs.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER

Mr. SHAYS. Mr. Rogalski.

STATEMENT OF ROBERT ROGALSKI

Mr. ROGALSKI. Good afternoon, Chairman Shays and distinguished members of the subcommittee. I appreciate the opportunity to meet with you today to discuss how DOD handles both classified and sensitive information.

Within DOD, my office is responsible for developing policies that address both controlled unclassified information, which we refer to as CUI, and classified national security information. This responsibility is executed on behalf of the Secretary of Defense and the Under Secretary of Defense for Intelligence, two of the Department's designated senior agency officials in accordance with Executive Order 12958, as amended, Classified National Security Information.

As I stated earlier, the Department uses a generic term, controlled unclassified information, to refer to all unclassified information that has been determined to require, for various reasons, some type of protection or control. CUI markings such as FOUO serve to inform DOD personnel that the information may qualify for withholding from public release and require some degree of safeguarding. It does not mean it is automatically withheld. It must first go through a review process before a release or denial determination is made.

We agree with the GAO that there are areas where our FOUO program could be strengthened. As they have recommended, we are updating our CUI policy on how we handle FOUO and are improving training within the Department.

Classification of national security information is, of course, more of a challenge because of the balance that must take place between the need for proper safeguarding and the need for openness that is fundamental to our society. While we understand the need for openness, we also have a responsibility to the American public to protect information that ensures our continued freedom. We in the Department also have the added challenge of ensuring sound classification principles are applied in a high-tempo operational environment.

We may sometimes take a more conservative approach to classification so as not to endanger personnel and operations. That is why the Department is committed to ensuring that our classifiers take their responsibilities seriously, are well trained, and are accountable for their actions.

There are a number of things the Department has done to clarify and emphasize classification management. The Secretary of Defense and the Under Secretary of Defense for Intelligence have both conveyed their personnel commitment to a strong information security program. Classification authorities have been reminded of their responsibility to properly classify information. Training requirements have been issued, and positions requiring original classification authority are subject to continuous review with the goal of reducing those positions. Additionally, since fiscal year 2004, DOD has reduced original classification decisions approximately 33 percent.

The DOD Director of Security meets quarterly with senior security personnel from the military departments, defense agencies, and combatant command and emphasizes, among other things, their responsibility to have a strong classification management program. The Defense Security Service Academy is working on new training courses to enhance classification and declassification, to include computer-based training that will be more accessible to a larger audience. We just conducted a DOD-wide security managers' conference last week where we were able to convey to an audience of approximately 800 DOD security professionals updates and reminders on classification management and CUI policies that they will take back to their organizations.

I would like to add that we support the National Archives on recent actions that have been taken with regard to the declassification effort. We support the moratorium on pulling records off the open shelves until ISOO completes their audit. We also support establishing a standard protocol for pulling records. We believe establishing a National Declassification Center will facilitate uniform declassification decisions. Obviously, authorities and resources will need to be addressed.

In closing, the Department has solid policies in place that are relevant and upon which we can continue to build. We have accomplished much to bring education and emphasis to important classification management issues to reduce over-classification. We will reemphasize current markings and review of CUI-FOUO. The Department takes its responsibility to protect information very seriously and strives to achieve the right balance between proper safeguarding and the need for openness in our democracy.

Again, I thank you for the opportunity to brief you on the Department's policies and look forward to the discussion on this important topic.

Mr. SHAYS. Thank you, sir.

[The prepared statement of Mr. Rogalski follows:]

WRITTEN STATEMENT
For
HOUSE OF REPRESENTATIVES
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS, AND INTERNATIONAL RELATIONS
"DROWNING IN A SEA OF FAUX SECRETS: POLICIES ON HANDLING OF CLASSIFIED AND SENSITIVE INFORMATION"
(March 14, 2006)

Good afternoon, Chairman Shays, Congressman Kucinich, and distinguished members of the subcommittee.

I appreciate the opportunity to discuss the Department of Defense's (DoD) policies and practices with regard to the identification and safeguarding of classified national security information and controlled unclassified information (CUI).

Within DoD, my office is responsible for developing policies that address both classified and controlled unclassified information. This responsibility is executed on behalf of the Secretary of Defense and the Under Secretary of Defense for Intelligence who is the Department's designated Senior Agency Official (SAO) in accordance with Executive Order (EO) 12958, as amended, "Classified National Security Information."

My discussion today will focus on the Department's policies on CUI, the draft Government Accountability Office (GAO) report No. 06-369 entitled, "MANAGING SENSITIVE INFORMATION: Departments of Energy and Defense Policies and Oversight Could Be Improved," classified information (to include reclassification) and, finally, the relevance and efficacy of current regulations, guidance, training and procedures that govern classification, reclassification, and the application of CUI designations, including the use of the FOUO (For Official Use Only) marking.

CUI POLICY

"Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation's progress depends on the free flow of information. Nevertheless, throughout our history, the national defense has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations." This is a direct quote out of the preamble to Executive Order 12958, as amended, "Classified National Security Information." This same concept, to a lesser degree, also applies to controlled unclassified information.

The Department of Defense uses the generic term "controlled unclassified information" (CUI) to refer to all unclassified information that has been determined to require, for various reasons, some type of protection or control. This information is often called "sensitive but unclassified" (SBU) information by others. Because of the large volume of information that may be CUI, the initial identification and designation as CUI is done by the individual who generates a document.

FOUO is the largest category of CUI within the DoD. Documents are marked FOUO when the information is deemed by the originator to be potentially eligible for withholding from public release if requested under the Freedom of Information Act (FOIA) (Section 552 of Title 5, U.S.C., as amended) exemptions 2 through 9.

At this point it is important to note that marking CUI serves to inform DoD personnel that the information may qualify for withholding from public release and it requires some degree of safeguarding. It does not mean it is automatically withheld without review. All DoD information, whether marked as CUI or not, is specifically reviewed for release when public disclosure is desired by the Department such as a security review or requested by others under the provisions of the FOIA. Any erroneous designation as FOUO is identified and corrected in this review process and

the information released as appropriate. Thus, information is not withheld from public release based solely on the initial markings applied by the originator. The Department has an extensive appeal process to ensure that release is done based on appropriate criteria.

CUI also has specific safeguarding requirements which are less stringent than what is required for classified, for example, store in a locked desk drawer versus a General Services Administration (GSA) certified security container and, when in a network environment, Information Technology controls are correspondingly less restrictive.

However, we do believe improvements can be made in how we handle CUI as mentioned in the GAO Report.

DRAFT GAO REPORT

In our official February 7, 2006 response to GAO, we agreed with their recommendation to clarify policy regarding the use of the FOUO designation, which is one of our primary subcategories of CUI, and including it in our oversight activities. We also agreed with the need for more robust training. However, we disagreed with placing the applicable FOIA withholding exemption on the document when it is first created. Besides the fact that

FOIA exemptions are not determined until the document is requested under the FOIA, this could create problems if the wrong exemption was cited. It is then possible that other documents that are derivatively created from this document would also carry the incorrect FOIA exemption or that the incorrect designation could cause problems if a denial is litigated. Also, due to the possibility of FOIA exemptions not being applicable over the passage of time, not designating FOIA exemptions on documents would ensure the greatest possible release to the public.

CLASSIFIED NATIONAL SECURITY INFORMATION POLICY

Classification is a challenge because of the balance that must take place between the need for proper safeguarding and the need for openness that is fundamental to our democracy. While we understand the need for openness we also have a responsibility to the American public to protect information that ensures our continued freedom. We in the Department also have the added challenge of ensuring good classification principles are applied in a high tempo operational environment. We may sometimes take a more conservative approach to classification so as not to endanger personnel and operations. That is why the Department is committed to ensuring that our classifiers take their responsibility seriously, are well trained, and are accountable for their actions.

The identification and designation of classified information is accomplished according to the classification criteria in EO 12958, as amended, by trained original classification authorities (OCA) having functional responsibility over the information. The decision making process is a best judgment based on all of the variables at the time an original decision is made. Key to the decision is whether release of the information would cause damage to national security. That is why we have implemented rigorous training requirements for the original classifiers so that they fully understand the classification process and their responsibilities, to include the prohibitions. The Department has a large number of classification guides codifying original classification authority decisions.

Declassification of classified information occurs when the appropriate OCA determines that the information can no longer cause damage to national security. Declassification reviews are prompted by a number of things, to include: requests for mandatory declassification review; records eligible for automatic declassification; Freedom of Information Act (FOIA) requests; and, in the event of actual or possible compromise of information. Another key declassification activity is the completion of our review of records eligible for automatic declassification by December 31, 2006. In addition to the automatic declassification provisions of Executive Order 12958, as amended,

the Secretary of Defense has directed we make every effort to declassify information as soon as it no longer meets the criteria for classification.

As set forth in Executive Order 12958, as amended, agency heads, are permitted to reclassify information in certain circumstances. However, DoD rarely exercises this option. For example, since the establishment of the Under Secretary of Defense for Intelligence in 2003, he has only reclassified information once.

Essential to effective implementation of the classification management program is training and oversight. All personnel who are cleared and handle or generate classified information are trained on their responsibilities. The purpose of the Defense Security Service Academy is to train our security professionals who in turn train personnel throughout DoD. I invite you and your staff to visit the Academy at Linthicum, Maryland. Additionally, oversight is directed to occur at every level of the Department to ensure classified information is correctly identified and marked, appropriately safeguarded, and declassified at the earliest possible date.

RELEVANCE AND EFFICACY OF CURRENT CLASSIFICATION AND CUI POLICY

All of our security policies have come under close scrutiny to ensure they are clear, consistent, relevant, efficient, and do not impede the necessary sharing of information. The Department is also involved in national efforts to do the same. We are participating in the Information Security Oversight Office revisions to EO 12958, as amended, to address the Weapons of Mass Destruction Commission recommendation regarding information sharing and the Department of Homeland Security's efforts to standardize CUI procedures for terrorism, homeland security and law enforcement in response to the requirements of Section 1016(D) of the Intelligence Reform and Terrorism Prevention Act (IRTPA).

There are a number of things the Department has done to clarify and emphasize classification management already:

- **The Secretary conveyed a message to all DoD Components of his personal commitment to a strong information security program, reminding classification authorities of their responsibility to properly classify information. He also prohibited the use of drafts and working papers as sources for derivative classification.**

- **The Under Secretary of Defense for Intelligence, DoD's senior agency official, subsequently issued training requirements for**

original and derivative classifiers. The Department's goal is to ensure there is a uniform thought process applied to each classification decision.

- **The Under Secretary of Defense for Intelligence requested a review of positions requiring original classification authority. While we have reduced some, we will continue the campaign to reduce them even further.**

- **The DoD Director of Security chairs a meeting of the DoD Security Directors Group quarterly consisting of senior security personnel from the Military Departments, Defense Agencies and Combatant Commands and emphasizes, among other things, their responsibility to have a strong classification management program.**

- **The DoD Director of Security conducted a video broadcast emphasizing classification management that was made available to all DoD Components through the Defense Security Service Academy news network.**

- **The Department conducted oversight visits of Combatant Commands with ISOO to determine if information had been**

appropriately classified, and made classification management a point of emphasis during outbriefs with the senior leadership.

- **We continue to work with Defense Security Service Academy on updating and reinforcing the training requirements which are key to a successful program. The Defense Security Service Academy has been working on new training courses to further enhance classification and declassification, to include computer-based training that will be more accessible to a larger audience.**

- **DoD is establishing a certification program for its security professionals which will include training in classification management.**

- **We chair a DoD Declassification Management Panel of DoD Components to share best practices, learn about problems, and plan the future of DoD's declassification efforts.**

We just conducted a DoD-wide security managers' conference last week where we were able to convey to an audience of approximately 800 security professionals updates and reminders on classification management and CUI policies.

Also, the Department is conducting a study to help develop security policy for the 21st century. As part of that study, we will look at what professionals from various sectors outside the Department, such as academia and industry, are doing to safeguard information.

In closing, the Department has solid foundational policies in place that are still relevant and on which we can continue to build. We have also accomplished much to bring education and emphasis to important classification management issues to reduce overclassification. Furthermore, the Department will pursue increased training on CUI. The Department takes its responsibility seriously and continues to strive to reach the right balance between properly safeguarding and the need for openness that is fundamental to our democracy.

Again, I thank you for the opportunity to brief you on the Department's policies and look forward to the discussions on this important topic.

Mr. SHAYS. Mr. Podonsky.

STATEMENT OF GLENN S. PODONSKY

Mr. PODONSKY. Thank you, Mr. Chairman and members of the subcommittee, for inviting me to testify regarding the Department of Energy's policies and practices for the protection of sensitive unclassified information as they relate to the information contained in the GAO report, "Managing Sensitive Information: Departments of Energy and Defense Policies and Oversight Could Be Improved."

Classified and other sensitive information are among the national security-related assets in our custody that we protect in accordance with the requirements of law, regulations, and national policies. After reviewing the GAO report, the Department agrees with all of the findings contained. They were accurate and we concur that the report's recommendations should be implemented.

Before I discuss issues of specific interest to this subcommittee, I would briefly like to describe my office's responsibilities in this area. Our Federal and contractor-line managers at all levels of the Department are responsible for ensuring that our information is properly protected. My office has a broad range of responsibilities associated with protecting information within the Department. These include developing Department-wide information protection policies addressing the identification, marking, and protection of classified information and the various categories of sensitive unclassified information; conducting formal document control training; providing technical assistance to sites to improve their information protection programs; and providing independent oversight to assess the effectiveness of the information protection programs throughout the Department.

In 2003, as a direct result of the recommendation by the Commission on Science and Security, known as the Hamre Report, the Department established its first agency-wide process for identifying and protecting sensitive information that we call "Official Use Only," [OUO]. This information is defined as classified information that has the potential to damage governmental, commercial, or private interests and which may be exempt from public release under the FOIA.

The purpose of our OUO program is to provide a means to control sensitive unclassified information and protect it from inappropriate disclosure; limit information protected from disclosure to that which is legally exempt under FOIA; provide guidance for consistent and accurate identification of OUO information; standardize the identification, marking, and protection of OUO information; and facilitate the appropriate sharing of unclassified information.

Access to OUO information is not overly restrictive. OUO information may be provided to individuals inside or outside the Department that need the information to perform their job or other DOE-authorized activity. Since OUO information is not classified, a security clearance is not required. The only requirement is a need to know. Overall, our OUO program is intended to provide a formal, workable process to identify, control, and protect certain sensitive unclassified information while making that information readily available for legitimate use.

We believe our program will be even more effective with the implementation of the GAO recommendations contained in their report. As previously stated, we found that the report was a fair evaluation of the Department of Energy's program and the findings to be accurate as well as useful.

In response to the GAO report, we are revising our order and manual to define inappropriate uses of OUO designation. We are revising our program directives to require specific initial and refresher training, clearly identify the scope and content of that training, and assign responsibilities for ensuring that the training is developed and conducted. We are developing a process to evaluate the identification, marking, and protection of OUO information and incorporate that process into our independent oversight program. We are also modifying our policy directives to require the incorporation of similar evaluations into line management, field oversight, and local self-assessment activities.

Turning just for a moment to our congressionally mandated effort to review documents released to the National Archives by other agencies under the Atomic Energy Act. The Department of Energy controls the dissemination and declassification of restricted data, which can be defined as nuclear weapon design, nuclear material production, and naval reactor information, loosely. We have dual responsibility with the Department of Defense for formerly restricted data, which is information concerning the military utilization of nuclear weapons.

During our review of records at NARA, we have never reclassified information that was declassified. The restricted data and formerly restricted data information that we found was classified at the time of the Executive Order 12958, classified national security information when it was issued, and remains classified. We have ensured that these documents are properly marked and protected as restricted data or formerly restricted data.

In conclusion, Mr. Chairman, we want to assure you and the members of the subcommittee, the Department strives to protect all sensitive information in our possession as required and permitted by applicable laws, regulations, and Executive orders. Our OUO program is designed to provide a reasonable level of protection to sensitive unclassified information while still accommodating our own and others' needs to use that information to conduct business and to address the legitimate and recognized needs of the public to have access to that information. We believe our responses to the GAO recommendations will strengthen our program's ability to achieve those goals. Thank you.

Mr. SHAYS. Thank you, gentlemen.

[The prepared statement of Mr. Podonsky follows:]

Testimony of Glenn S. Podonsky
Director, Office of Security and Safety Performance Assurance
U.S. Department of Energy
Before the
Subcommittee on National Security, Emerging Threats, and International Relations
Committee on Government Reform
U.S. House of Representatives
March 14, 2006

Mr. Chairman and members of the Subcommittee, thank you for inviting me to testify regarding the Department of Energy's policies and practices for the protection of sensitive unclassified information, particularly as they relate to the information contained in the Government Accountability Office (GAO) Draft Report number GAO-06-369, "Managing Sensitive Information: Departments of Energy and Defense Policies and Oversight Could Be Improved." Classified and other sensitive information are among the national security-related and other government assets in our custody that we rigorously protect in accordance with the requirements of law, regulations, and national policies. We take our responsibilities in this area seriously, as we do our responsibilities to protect other national assets and interests. After reviewing the GAO draft report, the Department agreed that the findings contained in the draft report were accurate and fully concurred with all the report's recommendations. Before I discuss the issues of specific interest to the Subcommittee, I would like to briefly describe my office's responsibilities in this area.

The Office of Security and Safety Performance Assurance has a broad range of responsibilities associated with protecting information within the Department. These include: developing Department-wide information protection policies addressing the identification, marking, and protection of classified information and the various categories of sensitive unclassified information; conducting formal document control and protection training at our National Training Center; providing technical assistance to individual sites to improve their information protection programs; and providing independent oversight to determine the effectiveness of

information protection programs and practices throughout the Department. While Federal and contractor line managers at all levels in the Department are responsible for ensuring that our information is properly protected, my office provides policies and training to assist them, and provides oversight to ensure effective implementation.

DOE's Management of Sensitive Unclassified Information

The Subcommittee has asked me specifically to address our policies and practices for managing Official Use Only information, including the effectiveness of our training programs in assuring the identification and protection of sensitive records in accordance with established criteria. Congress, through the Freedom of Information Act (FOIA), has provided for public access to agency records upon request. Acknowledging that for a variety of reasons some categories of information need to be protected from public disclosure, Congress, in that same Act, established the authority and basis for exempting some information from public disclosure.

As a direct result of a recommendation made by the Commission on Science and Security (the Hamre Commission), in 2003 the Department established its first uniform agency-wide process for identifying and protecting sensitive information that we call Official Use Only information. This information is defined as unclassified information that has the potential to damage governmental, commercial, or private interests, and which may be exempt from public release under the FOIA. Prior to 2003, various Departmental elements had established internal processes and procedures for handling sensitive unclassified information referred to by various designations, including Official Use Only, but they did not apply agency-wide and were not standardized. In 2003 the Department issued a series of policy and implementation guidance documents – including an Order, a Manual, and a Guide – that formally established a uniform Department-wide program for identifying and protecting Official Use Only information. The purpose of our Official Use Only program is to: provide a means to control sensitive unclassified information and protect it from inappropriate disclosure; limit information protected from disclosure to that which is legally exempt under the FOIA; provide guidance for consistent and accurate identification of Official Use Only information; standardize the identification, marking

and protection of Official Use Only information; and facilitate the appropriate sharing of unclassified information.

The first thing I'd like to explain about the Official Use Only program is how an Official Use Only determination is made. There are two primary criteria for making an Official Use Only determination. The first criterion is whether or not the information has the potential to damage governmental, commercial, or private interests if released to persons who do not require it to do their jobs or other DOE-authorized activities. The second criterion is whether or not the information may fall under a FOIA exemption. I want to emphasize that an Official Use Only designation merely alerts individuals in possession of the information that it is sensitive, that it must be adequately controlled and protected, and that it must be reviewed prior to release – it does not mean that the information is automatically exempt from disclosure if requested under the FOIA. If the information is requested, the determination as to whether it can be released is made by an FOIA Authorizing or Denying Official based on a formal review.

Employees can determine that an unclassified document contains Official Use Only information if the employee's office has cognizance over the document – that is, if the document originated in their office, was produced for their office, or is under the control of their office. An Official Use Only determination is either based on formal guidance promulgated by a program office or made by an employee using the criteria of potential damage and the requirements of the FOIA.

Formal guidance can be issued in a variety of formats. Classification guides, in some instances, contain specific guidance for making Official Use Only determinations. For example, certain operational information, such as routine protective force deployment plans for facilities that do not possess Category I quantities of Special Nuclear Material is protected as Official Use Only. In the absence of guidance, an employee may make a determination based on the two criteria. While no formal certification is required to make Official Use Only determinations, the information necessary to guide decision-making for such determinations is available in Departmental-wide policy and guidance, program office policy and guidance, and various forms of local information security training.

If information is determined to be Official Use Only, the document or other medium in or on which it is contained must be appropriately marked. In addition to the obvious Official Use Only page markings, the first page must contain a marking identifying the FOIA exemption category that may be applicable, the requirement for review prior to public release, the name of the person making the determination, the date of determination, and any applicable guidance upon which the determination was based. In short, our system requires personnel to be accountable for their Official Use Only decisions.

Access to Official Use Only information is not overly restrictive. Official Use Only information may be provided to individuals – inside or outside of the Department – that need the information to perform their job or other DOE-authorized activity. Since Official Use Only information is not classified, a security clearance is not required; the only requirement is a need to know.

We require reasonable precautions for the protection of Official Use Only information. For example, it must be stored in secure buildings or in locked containers such as filing cabinets, desk drawers, or briefcases. We also require reasonable but simple precautions when reproducing, mailing, destroying, and electronically transmitting Official Use Only information, all aimed at ensuring the information is available only to authorized persons.

An Official Use Only determination is not necessarily permanent or irreversible. There are several ways in which Official Use Only information can be decontrolled. For example, the employee who made the original determination, or that employee's supervisor, may reevaluate the information and determine that it is not, or is no longer, Official Use Only. A program office may determine that certain program-related information is no longer Official Use Only and revise its guidance accordingly. Finally, upon a review resulting from a FOIA request for the information, a FOIA Authorizing Official may determine that the information may be released to the public.

Overall, our Official Use Only program is intended to provide a formal, workable process to identify, control, and protect certain sensitive unclassified information while making that information readily available for legitimate use. While we believe our program is effective in

helping us meet these goals, the GAO identified several areas that can be improved. As previously stated, we found the report to be a fair evaluation of our program and the findings to be accurate, and we fully concur with all recommendations.

The first recommendation is to clarify our guidance regarding the point in time at which a document should be marked as Official Use Only and to define inappropriate uses of the Official Use Only designation. Our response is to revise our Order and Manual to address these two points.

The second recommendation is to assure that all employees authorized to make Official Use Only determinations receive appropriate training before they make such determinations. Providing appropriate Official Use Only program training has been and remains the responsibility of line managers at the local level, with support and guidance from cognizant Headquarters organizations. Admittedly the form and content of that training has varied widely from location to location within the Department. As a result we are going to revise our program directives to require specific initial and refresher training, clearly identify the scope and content of that training, and assign responsibilities for ensuring that the training is developed and conducted.

The final recommendation is to conduct periodic oversight of Official Use Only program implementation. Our response is to develop a process to evaluate the identification, marking, and protection of Official Use Only information and incorporate that process into our Independent Oversight Program. We will also modify our policy directives to require the incorporation of similar evaluations into line management field oversight and local self-assessment activities. These actions will provide formal program oversight at several levels, and we believe will achieve the results the GAO is seeking.

Historical Records Review at National Archives and Records Administration

The Subcommittee has asked that I also address the Department's ongoing Congressionally-mandated effort to review documents released to the National Archives and Records Administration (NARA) by other agencies.

Under the Atomic Energy Act, the Department of Energy (DOE) controls the dissemination and declassification of Restricted Data, which can be loosely defined as nuclear weapon design, nuclear material production, and naval reactor information. We have dual responsibility, with the Department of Defense, for Formerly Restricted Data, which is information concerning the military utilization of nuclear weapons.

In 1995, when President Clinton signed Executive Order (EO) 12958, *Classified National Security Information*, it contained a key provision for the automatic declassification of National Security Information records of permanent historical value that were 25 years old or older, except for those documents that fell within certain specific exempt categories. Under EO 12958, the DOE and other agencies reviewed and released records which were then processed by NARA and placed on the open shelves where they were available to the public.

In 1996, Congress, concerned that DOE documents subject to the automatic declassification provisions of EO 12958 might contain Restricted Data, passed Public Law (PL) 104-106, which required the page-by-page review of DOE documents prior to release. Subsequently, Congress passed Section 3161 of the National Defense Authorization Act for Fiscal Year 1999 (PL 105-261), known as the Kyl Amendment, which required the DOE to develop a plan to prevent the inadvertent release of Restricted Data and Formerly Restricted Data through other agency records. The resulting plan, the Special Historical Records Review Plan, coordinated with NARA and the Information Security Oversight Office (ISOO), requires all departments and agencies to review their records page by page with reviewers trained by the DOE to recognize Restricted Data and Formerly Restricted Data, unless the records are highly unlikely to contain Restricted Data and Formerly Restricted Data. Since 1999, the DOE has trained over 2,000

Federal and contractor employees of other Government agencies to recognize Restricted Data and Formerly Restricted Data.

These programs ensured documents were reviewed by trained personnel prior to their release, but did not address documents already declassified and available to the public. The subsequent Lott Amendment (PL 106-65, Section 3149) applied the requirements of the Kyl Amendment to records already processed by NARA and the other agencies, including records that had already been made available to the public. The resulting Supplement to the Special Historical Records Review Plan, again coordinated with NARA and ISOO, required the DOE to survey records on the open shelves in order to identify those that were likely to contain Restricted Data or Formerly Restricted Data. Based on this mandate, we surveyed 213 million pages and withdrew thirty-seven million pages for audit examination. To date, we have returned approximately 35 million pages to the open shelves after NARA removed the documents that DOE identified as containing Restricted Data and Formerly Restricted Data. The approximately 2 million pages remaining are scheduled to be complete by the end of 2006.

Because the reclassification of documents is of particular concern to the Subcommittee, I would like to take a moment to address the issue. During our review of records at NARA, we have never reclassified information that was declassified. The Restricted Data and Formerly Restricted Data information that we found was classified at the time the Executive Order was issued and remains classified. We have, therefore, simply ensured that these documents are properly marked and protected as Restricted Data or Formerly Restricted Data. Our program was developed in close coordination with NARA.

Since 2000, we have submitted 20 reports to Congress (Committees on Armed Services) and the National Security Council (Assistant to the President for National Security Affairs) regarding the inadvertent release of Restricted Data and Formerly Restricted Data under EO 12958, which detail the ongoing findings of our reviews. Examples of classified information that we have identified during these reviews include information related to nuclear weapon design, special nuclear material production, radiological warfare, military utilization of nuclear weapons, and

Naval Nuclear Propulsion Information. We redact these reports to remove classified information and make the unclassified copies available to the public.

Concluding Remarks

I want to assure the members of the Subcommittee that the Department earnestly strives to protect all sensitive information in our possession as required and permitted by applicable laws, regulations, and Executive Orders. In determining how to protect information, as in determining how to protect our other national security assets, we apply a graded approach. That is, more valuable (or harmful to national security interests should it fall into the wrong hands) information is afforded a greater and more restrictive level of protection than is information of lesser value. Our Official Use Only program is designed to provide a prudent and reasonable level of protection to sensitive unclassified information while still accommodating our own and other's needs to use that information to conduct business, and to address as well the legitimate and recognized needs of the public to have access to that information. We believe our responses to the GAO recommendations will strengthen our program's ability to achieve those goals.

Thank you.

Mr. SHAYS. I am going to call on Mr. Waxman first, with the concurrence of Mr. Kucinich, but I just want to say for the record, I think we have a huge problem and I will be looking to you all to help us figure out how we get headed in what I would call the right direction. So I would like to come out of this knowing what we could be doing about it.

At this time, the chair would call on Mr. Waxman. Mr. Waxman, you will have the floor for 10 minutes.

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

I want to focus my questions on the allegations of researchers who claim that the administration has been secretly removing documents from the National Archives that have already been declassified. Mr. Weinstein and Mr. Leonard, can you help us understand what is going on here? What agency is in charge of this program today?

Mr. WEINSTEIN. That is a difficult question to answer. Let me explain why, Mr. Waxman. There has been speculation about the National Archives having secret agreements with various, multiple Federal agencies authorizing the re-review of declassified documents. I would like to clarify for the record that to the best of the knowledge of the Archivist, NARA has one classified Memorandum of Agreement pertaining to the issue of re-review, one.

The Memorandum of Agreement [MOA], is with a component of the Department of Defense and remains classified. The MOA is procedural in nature and deals with such things as proper archival procedures for handling accessioned records, recording any decisions made by the agency, and ensuring that the records are managed according to NARA requirements, and I cannot say anything more about the MOA, which gets to the heart of your question, I am afraid, in an open session because it contains classified information.

Mr. WAXMAN. So what——

Mr. SHAYS. Are you sure it is actually sensitive information?

Mr. WEINSTEIN. I was told classified, Mr. Chairman.

Mr. WAXMAN. Therefore, would one assume it is the Department of Defense that is taking the action, since that is the only group you have a Memorandum of Understanding?

Mr. WEINSTEIN. As I recall your question, it went to the heart of who was in charge of this process.

Mr. WAXMAN. Who are the agencies in charge of the program, the whole process of reclassifying these documents?

Mr. WEINSTEIN. That is what this audit is determined to find out, and if you can bear with us until the audit is completed, I think we will have an answer that will——

Mr. WAXMAN. So we don't know who it is, but can you tell us what authority they are operating under to pull these documents from the shelves? These documents were already declassified. What authority do they have to do this?

Mr. LEONARD. Just to buildupon what Professor Weinstein indicated, in addition to the Department of Defense activity, Mr. Podonsky indicated that the Department of Energy has been conducting re-review of material at the National Archives since the late 1990's, as well as on occasion the Central Intelligence Agency has done it, as well, too.

If there is a common thread, this does not address every——

Mr. WAXMAN. Let me ask the question——

Mr. LEONARD. Sure.

Mr. WAXMAN [continuing]. And then we will see if you have a direct answer to the question, and if you don't, why. We don't know exactly who is doing this and you have not been able to respond to us under what authority they are doing it.

Mr. LEONARD. I was just about to get to that, Mr. Waxman.

Mr. WAXMAN. OK.

Mr. LEONARD. The authority that they are doing it under is under the framework of the Executive order. Only agencies that have originated the information have the authority to declassify it. So one of the most common situations that has arisen is where, for example, if an agency declassifies its own records but it contains information that belongs to another agency and they did not afford that other agency the opportunity to review those records prior to the declassification action, pursuant to the order, that is not classification under proper authority, and so——

Mr. WAXMAN. So this isn't pursuant to a Memorandum of Understanding with the National Archives. It is pursuant to an Executive order?

Mr. LEONARD. Yes, sir.

Mr. WAXMAN. OK. Now, it is hard to still, even with that explanation, understand how these examples we have of records from 50 years ago would be changed——

Mr. LEONARD. The simple answer is they don't. The exemplars that were provided to my office early this year as well as that has received coverage in the press, those exemplars clearly do not adhere to the classification standards of the order and are inappropriate——

Mr. WAXMAN. Well, let me——

Mr. LEONARD [continuing]. And—I am sorry——

Mr. WAXMAN [continuing]. Turn to the questions I have about the audit itself that you are going to be doing.

Mr. WEINSTEIN. Congressman, could I respond just a half-a-second to that?

Mr. WAXMAN. Yes.

Mr. WEINSTEIN. In response to Mr. Leonard's advice that he has just given to you, to me, and in response to the situation, I took the actions which I took, which were based obviously on the fact that I could see no sensible use in classifying things that are 50 years old that have already been declassified.

Mr. WAXMAN. Well, you called a halt to any further removal of documents while you conduct your audit, is that right?

Mr. WEINSTEIN. Yes, that is correct.

Mr. WAXMAN. What was it that led you to decide to take this measure? Why did you conclude that these agencies should stop what they are doing until you examined their actions?

Mr. WEINSTEIN. Well, to begin with, Congressman, I wasn't aware of their actions and it was important for me to become aware of those actions. I learned about their actions from the New York Times, the way the American public did. Having been Archivist for a year, that struck me as being a rather impossible and ab-

surd way to learn to know what is happening at your own agency and I acted immediately.

Mr. WAXMAN. So you acted immediately and you stopped any removal of documents, and I am certainly pleased you are investigating the matter. Researchers are saying that there is an interagency memorandum and the only one that you are aware of is the one that the National Archives has with the Department of Defense?

Mr. WEINSTEIN. Component of the Department of Defense, yes, sir.

Mr. WAXMAN. And what does that Memorandum of Understanding say?

Mr. WEINSTEIN. Well, as I indicated, Congressman, I would be happy to discuss this in a closed session, but unfortunately, for this discussion, it contains classified information which I am not prepared to discuss in open session.

Mr. WAXMAN. And why is it classified?

Mr. WEINSTEIN. Pardon?

Mr. WAXMAN. Why is it classified?

Mr. WEINSTEIN. Why is it classified?

Mr. WAXMAN. Yes.

Mr. WEINSTEIN. I don't know.

Mr. WAXMAN. Is there something in the Memorandum of Understanding itself that will harm national security if it gets out?

Mr. WEINSTEIN. I think I probably have to stand by my previous answer, Congressman.

Mr. WAXMAN. That you can't say that in open session.

Mr. WEINSTEIN. I would be happy to discuss it in a closed session.

Mr. WAXMAN. Has there been any discussion within the administration about declassifying this Memorandum of Understanding, if you know?

Mr. WEINSTEIN. That I know of? Yes, I would say there has been.

Mr. WAXMAN. And who wanted the MOU released and who didn't want it released?

Mr. WEINSTEIN. Let me say that if it was released, I would have no trouble in conveying it, and that is as far as I would go on that square.

Mr. WAXMAN. Does the MOU include any mechanisms to check against officials making these absurd classification decisions?

Mr. WEINSTEIN. That is tough for me to answer, Congressman, as you might appreciate given what I said previously.

Mr. WAXMAN. Mr. Chairman, given these responses and since so many of the details about this program remain classified, we are left with some significant questions. I would like to make two requests. First, Mr. Chairman, would the subcommittee send a request for the classified MOU that governs this program? And second, could the subcommittee also request a classified briefing on this program with all the relevant agencies to obtain answers to these pressing questions?

Mr. SHAYS. That will happen. We will do that. It makes sense. I am almost tempted to just tell my counsel, respond in a way, as well, because I am finding this—I don't know, Mr. Weinstein, if part of your answers are almost the exact kind of problem that we are trying to make in this hearing. Is the reason why some infor-

mation isn't being responded to Mr. Waxman because they would embarrass people or is there a legitimate reason to classify or to suggest that this can't be said publicly?

Mr. WAXMAN. He's caught in a catch-22 because——

Mr. SHAYS. I know he is, but in a way, the bottom line is, there is almost an absurdity of going into having a classified hearing about something that is sensitive but unclassified.

Mr. WAXMAN. But the MOU is presumably classified.

Mr. WEINSTEIN. Yes, sir.

Mr. WAXMAN. So we want to get, one, a copy of the MOU——

Mr. SHAYS. Right.

Mr. WAXMAN [continuing]. And I hope you support that request——

Mr. SHAYS. Yes.

Mr. WAXMAN [continuing]. And second, we ought to get a classified briefing on this program, this whole program, because it is not just based on the MOU, but it seems to be based on some Executive order and all other agencies are involved——

Mr. SHAYS. Let me——

Mr. WAXMAN [continuing]. And we ought to see what is so pressing that——

Mr. SHAYS. I am going to start first to ask that it be declassified, that we can have it in a public setting. If it can't be declassified, then we will have a classified setting hearing. But you can be assured that there is going to have to be some real justification as to why it needs to be classified. Are you comfortable with that?

Mr. WAXMAN. With your request that it be declassified and given to us, and if that is refused, you will request that it be given to us even though it is classified and hold a classified hearing on it.

Mr. SHAYS. Right—no—yes—[laughter]—let me explain what I am asking. I am asking my staff to do this as counsel or someone with legal expertise because I find some of this almost silly and absurd. I find some of this destructive to our country, and I think what Mr. Waxman wants is very, very important, but I don't want to start doing the very thing that I am finding others doing. I don't want to start to suggest that some things need to be behind closed doors when, in fact, maybe they shouldn't be, and so that is what I am wrestling with.

Mr. HALLORAN. Thank you, Mr. Chairman. For the record, to the Archivist, will the Archives provide the subcommittee under classified cover a copy of the Memorandum of Understanding, of Agreement?

Mr. WEINSTEIN. It is my understanding that is entirely appropriate, but I would like to turn to my counsel, if I may, just to be sure that I am not misstating anything here.

[Pause.]

Mr. WEINSTEIN. One of the things about not being a lawyer, counselor, is one has to consult. The classifying authority, I have been told, is with the classifying agency, which would have to authorize the—without further action by the subcommittee, the release of the classified Memorandum of Agreement.

Mr. HALLORAN. But you can't tell us to whom such a request would be directed?

Mr. WEINSTEIN. I suppose what we would do would be to convey your request to the classifying agency and try to get an immediate response so that we can accommodate the subcommittee.

Mr. LEONARD. Again, it is a Department of Defense component, so it makes it very easy.

Mr. WAXMAN. So the classified agency is a Department of Defense component, is that——

Mr. WEINSTEIN. That is what I said in my statement.

Mr. ROGALSKI. Mr. Chairman, the MOU does belong to the Department of Defense in conjunction with NARA. We have received a FOIA request for that MOU. We are looking at that now to see if it can be sanitized. But let me assure you that the rationale for classifying that was done in accordance with what the Executive order determined by the original classification authority.

So we certainly have no objection to providing you a classified briefing on that MOA. We do not have a problem and we are going through the process of seeing can it be sanitized now and being presented to you in an open forum. So that is happening as we speak. But again, I want to assure you that the basis for the classification, again, in my opinion, after reviewing that, was sound and between NARA and us. We can provide that to you.

Mr. SHAYS. So the bottom line you are stating is that it was your recommendation that it be classified, or, excuse me, that you concurred with the recommendation of others that it be classified?

Mr. ROGALSKI. My office concurred with the classification decision done by the original classification authority responsible for that document, that is correct.

Mr. SHAYS. And you think it would be unlikely that if we asked that it be reviewed to be declassified, it would be unlikely it would be declassified?

Mr. ROGALSKI. We can certainly review that and determine but I don't want to give you a document with all black lines on it, redacted.

Mr. SHAYS. No——

Mr. ROGALSKI. I want to give you something that is beneficial——

Mr. SHAYS. And we don't want a sanitized version. We want the real thing and we will do it——

Mr. WAXMAN. Mr. Chairman, let us get both, because it may take them too long to figure out how to——

Mr. SHAYS. OK.

Mr. ROGALSKI. And we have no problem briefing you on the rationale, the MOU and the rationale for the classification decision.

Mr. SHAYS. I think Mr. Waxman's suggestion is important. Let us get the sanitized version that can be made public and then we would like to see the real McCoy. It will be a good opportunity for us to decide as a subcommittee whether we think there was justification for it being classified. I think that we will ask all the subcommittee members to see this document so that we—in the subcommittee to get their views, and we will issue a statement on what we think about that document and the justification we heard.

Mr. LEONARD. If I could just add, it will be withheld, I presume, Mr. Chairman——

Mr. SHAYS. Well, it may be sensitive but unclassified.

Mr. LEONARD. And if I could just add something here to further shed some light on the issue, again, the audit that is currently underway, and I don't want to presuppose any final results, but I can tell you one of the things that we ascertained very early on, the exemplars that were provided to our office and were released to the media and whatever, those exemplars were not pulled pursuant to that MOA. They were done—action taken quite a few years ago.

Mr. SHAYS. At this time, the chair would recognize——

Mr. WAXMAN. Mr. Chairman, there is then the question of who did those and why——

Mr. LEONARD. They were pulled by the CIA and they were pulled in response to a serious breakdown in quality control back in about the year 2000, where information that clearly was inappropriate for release ended up being released, and in an attempt to clean that up, it went too far the other way.

Mr. SHAYS. With all due respect, about the year 2000, there is a big difference between the year 2000 and the year 2001. Was it in 2000?

Mr. LEONARD. I believe it was the year 2000, yes, sir.

Mr. SHAYS. So it was the previous administration in that case?

Mr. LEONARD. Yes, sir.

Mr. WAXMAN. The same CIA Director. [Laughter.]

Mr. WEINSTEIN. Mr. Chairman, if I could just add, what Bill Leonard has just mentioned gets to the heart of the complexity that I was discussing with Congressman Waxman of who did what, when, and related to your initial question. We hope to have as many answers to that question as we can put them into the audit and we will look forward to getting you a copy of that audit.

Mr. LEONARD. And actually, if I could just add, I mean, the whole confusion, the awkwardness and whatever cries out for transparency in this process. That is the one thing that we are committed to providing, not only transparency going back to 1995 for all such activity but continuing transparency for a number of good reasons. No. 1, to ensure that any action taken along these lines is absolutely, positively necessary because people know that people will be watching, but even more so, to prevent perceptions being created that, quite frankly, harm the Nation, harm the process, and are understandable but yet are unfortunate.

Mr. SHAYS. Let me just say, I happen to have taken off my jacket. I was feeling a little warm. I would want any of our witnesses to feel that they could do the same thing. I don't want a double standard. I am being serious. If you would like to take off your jackets or coats, feel free.

Mr. Van Hollen.

Mr. VAN HOLLEN. Thank you, Mr. Chairman. As you said, this whole process seems to have sort of an Alice in Wonderland quality to it.

Let me just make sure I understand the memo. The memo is between the Archives and an agency of DOD, is that right?

Mr. LEONARD. Yes.

Mr. VAN HOLLEN. What was the classification level of that memo? Is it secret? Is it top secret?

Mr. LEONARD. I believe it is secret.

Mr. VAN HOLLEN. Secret, OK. Now, as I understand it, there were many documents that were reclassified outside of that particular agreement.

Mr. LEONARD. That is correct.

Mr. VAN HOLLEN. In other words, there were other government agencies that came in and reclassified documents, is that right?

Mr. LEONARD. Yes, sir.

Mr. VAN HOLLEN. OK, and those include the CIA and DOE?

Mr. LEONARD. That is correct.

Mr. VAN HOLLEN. Were there any others?

Mr. LEONARD. Not that I have identified yet, but again, that is the whole purpose of the audit, is to fully flesh that out.

Mr. VAN HOLLEN. All right. Now let me just focus on that category for a moment——

Mr. LEONARD. Sure.

Mr. VAN HOLLEN. I understand this memorandum apparently regulates how the Archives deals with an agency of DOD, but let us take DOE, for example, since we have a representative from DOE here at the table and we don't have a CIA representative.

Mr. LEONARD. Sure.

Mr. VAN HOLLEN. If DOE wants to go back, they can reclassify documents under the Executive order, as I understand it, which they were the original classifier of, is that right?

Mr. LEONARD. Actually, the situation with DOE is even more unique since, as Mr. Podonsky explained, their information which pertains to nuclear weapons is actually outside the scope of the Executive order and is classified pursuant to statute, the Atomic Energy Act.

Mr. VAN HOLLEN. OK, so let me just make sure I understand. So you are saying the Executive order doesn't apply to DOE at all?

Mr. LEONARD. It doesn't apply to DOE, at least with respect to restricted data and formerly restricted data which deals primarily with nuclear weapons, yes, sir.

Mr. VAN HOLLEN. OK. So if DOE has documents that they originate at DOE, they are at the Archives now, right?

Mr. LEONARD. Yes, sir.

Mr. VAN HOLLEN. Now, they want to come in and reclassify documents. First of all, let me figure out how they got declassified to begin with. As I understand it, technically, DOE as the classifying agency, even under this other authority, are they still the ones that have the authority to declassify it and are they only ones that have the declassification authority?

Mr. LEONARD. They have the authority, and what happens in that case is what happens in other cases, as well, too, this kind of information will appear in another agency's record, for example, the Department of State, and when they go to declassify it, the person who does it does not necessarily recognize that, hey, wait a minute, there is information here that belongs to another agency. I can't take unilateral action on it.

Mr. VAN HOLLEN. I understand. I understand that. So when DOE is going in to reclassify, the first question I have is, are they going in to reclassify DOE information that has been declassified by the State Department or other agencies, or have they also gone in to reclassify DOE information that they originally declassified?

Mr. LEONARD. That is right on, because what has—again, our audit is in process, but one of the key issues that has come out very early on is that when agencies are re-reviewing for a specific purpose, if they come across additional information that they believe was inappropriately declassified, that likewise is being put aside.

Mr. WEINSTEIN. Let me add a little complexity even beyond that, Congressman Van Hollen, if I can. It is fair to say that we are learning more with each day of doing this audit, and it is fair to say that in my position as Archivist, I am learning even more because until the news media provided me with that information, that was my first knowledge of this program and all of its complexities and I am not sure I have the complete handle on the story now. As a result of this audit, I hope to have it, and when I have it, obviously, the subcommittee will have it, as well.

Mr. VAN HOLLEN. Thank you and I appreciate that. I understand. With the audit so far or with your research into this so far, you have discovered instances where the DOE has reclassified information that they themselves declassified? Just yes or no, if that is——

Mr. LEONARD. That they themselves have declassified?

Mr. VAN HOLLEN. That they had originally declassified, and they have gone back to reclassify that.

Mr. LEONARD. It is unclear. I am not too sure if I have that depth of understanding.

Mr. PODONSKY. Let me, since it is a hypothetical, let me just—I recognize it is a hypothetical, but again, as I said in my testimony, the Department of Energy has not gone back into the National Archives and reclassified anything that was declassified. However, what we were asked to do in 1996 by the Congress is to go back in and take a look at all the records from other agencies that may have had RD or FRD, and then the Kyl amendment went in and said also go in and train other agencies to know how to look for RD or FRD, and then the Lott amendment said go in and also take a look at all documents that were already previously taken off the shelf at NARA. So hypothetically, we could be the agency that was doing it, but we are not.

Mr. LEONARD. Congressman, let me answer the question, try to be as direct as I can to your question. The Executive order has a very high threshold that if an agency declassifies information and for whatever reason changes their mind, they have a very high threshold to meet. Agencies to date have represented to me that they have never done that. Based upon what I know to date, I don't think that is necessarily the case. I think they have, in fact, done that for a variety of reasons, may not have understood it to be that, but I do believe that there have been instances where agencies have gone back and reclassified information that they themselves have previously declassified without meeting the threshold that is spelled out in the Executive order.

Mr. VAN HOLLEN. OK. Let me just also briefly try and understand the process by which this happens. Let us say that the CIA or DOE, say they want to come back and take a look at whether other agencies have declassified information that they were the original classifiers of. What do they do, come over to the Archives, they knock on the door and say, where are our files, and they go

in? Does the Archives have any ability to make an independent determination about whether what these agencies are doing is appropriate or not appropriate?

Mr. LEONARD. The delineation of responsibilities is when records enter to the National Archives and when they are accessioned into the Archives, they are under the control and the custody of the National Archives. They belong to the Archives. So no agency can just simply come in and rifle through records on their own.

Mr. VAN HOLLEN. That is why you can have a moratorium?

Mr. LEONARD. The information that is contained in those records, when it is classified information, the classification authority over that information remains with the agency, and so when agencies exercise declassification authority or reclassification authority or say that this was declassified improperly, that is an authority that they have that the Archives does not have. The Archives cannot classify information on their own, and so the Archives is hard pressed from that perspective to challenge an agency with respect to exercising their classification authority.

Mr. VAN HOLLEN. Thank you, Mr. Chairman. I have a lot more questions, but I don't want to take up any more time, but thank you.

Mr. SHAYS. Thank you for your questions.

At this time, the chair would recognize Mrs. Maloney.

Mrs. MALONEY. I want to thank you, and I would like to ask the representative from the Department of Defense this question, Mr. Rogalski. I want to give an example of one audit and how there was no appeal process and then really ask all Members, where is the appeal process when there is a redaction.

I cite the publicized case of the Iraqi oil money, the audit for the United Nations, where DOD had an audit through the DCAA, the contracting audit agency, about the overcharges, and in that audit they concluded that there was an overcharge to our government of over $200 million. During the audit and during the time that it was handed over to the United Nations and to the public, absolutely everything that mentioned the overcharge was redacted. It was reported in the paper that the audit was handed over to Halliburton and Halliburton made all the redactions, handed it back to DOD, and no one questioned this. It finally came out in the press. I would like to put this article into the record of this hearing.

But my question is, I think that obviously this was an inappropriate redaction of information. Overcharging is illegal. It is wrong. It is our taxpayer money. In this case, it was the Iraqi oil money. It is a report to the United Nations. But when waste and abuse appears in our government, we don't want to have it redacted so that we can move forward watching taxpayers' money more appropriately.

And my question really to the panel, and I will start with DOD, since that happened to have been a DOD contracting audit under DCAA, where is the appeal process? Where is the appeal process? Say I am a reporter, or even a staff member on this subcommittee, or a Member of Congress, and I see that everything in the report is redacted. Who do I appeal to that is an independent government professional who can decide whether it is in government's interest, the public interest, the taxpayer interest, the honesty interest to

have that information revealed to government and to the appropriate overseers to correct it so that money is not wasted in the future?

Mr. ROGALSKI. I am not familiar with the cases you describe, ma'am, but I can certainly take the question for the record and get that back to you if you would like more information on it.

Mrs. MALONEY. I will send it to you in writing. It was reported in the press widely.

Mr. ROGALSKI. OK. There is an appeal process. We have FOIA offices throughout the Department of Defense. People are trained. They are familiar with the exemptions and people are allowed to go and appeal that determination once that document is released and——

Mrs. MALONEY. And how do they appeal it? Do you need a lawyer to appeal?

Mr. ROGALSKI. No, ma'am. They can come in as a citizen or whatever——

Mrs. MALONEY. Take this example, that everything is redacted. I mean, to me, I think it is scandalous that it was given back to Halliburton and they are the ones who redacted it and that DOD then accepted it. But say I get a paper on a contract and everything is redacted. I mean, how do I appeal? I don't know what was in it. I can just say the entire page is redacted. The purpose of the audit was overcharges. Why in the world are you redacting overcharges, or what are the bases on which you can appeal? It has to have certain standards, right?

Mr. ROGALSKI. Well, the standards are what is required under the FOIA, those exemption categories, and have we provided the rationale for that when you come in with that appeal. There are certain examples of where you see it, as you described earlier, blacked out, and I think those are wrong. Mistakes have been made. But I think part of us and what we are doing is having an education process, so before it is released for FOIA, people are doing the right thing. And we agree. We need more rigor in the process. I will not deny that. So——

Mrs. MALONEY. What I don't like about this, I just came from a meeting earlier this morning with whistleblowers and there is no protection for whistleblowers, particularly in defense and national security. They were saying that if they don't toe the party line, then they lose their job, they lose their clearance, and they are made the evil ones.

So here you are appealing to another person within the same department that shows a mismanagement in that department. That employee may know that their higher-ups may strip them of their jobs, their standing, their clearance, which has happened to 75 members of the government that are part of this organization that I met with earlier this morning. See, you are appealing to a group of people who are not covered under the Whistleblower Protection Act. In other words, if you don't toe the party line, you know, obviously someone wanted to cover up that these overcharges were there. Otherwise, they would have just put it out in the public to begin with. In other words, it is not working, and to say we should be more rigorous is not answering the problem. So I would like some comments from others.

I think one of the biggest responsibilities all of us have is to maintain the faith and trust of the American people in our government, and when they read stories like this, it is upsetting to them. It sounds like their government wants to cover things up. And I would say that I think one of the strongest parts of our government is our ability to look at our problems, discuss them publicly, and make corrections. We certainly have made a lot of them in New York with the September 11th, with our security, to notice what we are doing wrong, to discuss it publicly, and then go forward.

But things like this, these massive redactions for which no one really can appeal—people tell me when they appeal, they are appealing to the same agency. They just say, our redactions are appropriate. Get lost. There is really no independent place to go. I am not trying to point fingers at anybody, at any administration or any party or any department. I am just saying that I think this is a problem and if this continues, there is a lack of faith in the system. And when there is a lack of faith in the system, you have cynicism, you have people that don't support their government, and you have problems.

You know, I am really seriously very disturbed about it and I would like to hear from anybody on the panel or any of my colleagues if they have an answer to this problem.

Mr. WEINSTEIN. Can I address that?

Mrs. MALONEY. Certainly.

Mr. WEINSTEIN. Congressman Maloney, what you are describing is obviously not a satisfactory situation, but let me give you a little personal response to what I take is a very personal reaction on your part. I am here today because I felt the head of the National Archives and Records Administration should be here, not simply the able, skilled professional, my colleague Bill Leonard, who is reflective of the other able, skilled professionals at this table.

I am here because what the researchers and historians uncovered about a month ago is not a tolerable situation, not a situation that should be tolerated, and I have done what I can within the agency to bear witness to the need for change and the need for immediate change and the need for a genuine effort to persuade the public and to persuade our colleagues in this town of both parties, of both Houses of Congress, in the media, whomever, that we are on the case, that we are going to find out what happened and that information will become public, and that with the support, I am pleased to say, at the moment, of not just the researchers who brought forth this material, but with the support of the agencies that have been involved, as well, and I would like to keep that there because I think this is a moment when good changes can be made that please this country.

But what recourse can we have? Often we don't have legal recourse, but we have a bully pulpit. We have the ability to speak out within government and to use that ability, and that is what I am trying to do here and that is what I suspect that my colleagues elsewhere in the government are also trying to do.

So I respect your question. I don't have an answer to it because I don't have the technical answer to where——

Mrs. MALONEY. I appreciate all your work, and I have done a lot of work with Archives. You have done a great job and we appre-

ciate it. But I would like to ask Ms. D'Agostino with the Government Accountability Office, a nonpartisan factual organization—you do a great job for the American people—I see this as a problem. Do you have any solution to it of how do you appeal in any case? You could put it in the EPA, where someone goes in and closes down a business and they say it is, "an illegal business," and then they redact the entire report on how they came to that decision. How does that small business person appeal? Members of the press tell me that if they ever question a redacted report that they receive from anybody, that it is like you are talking to a blank wall.

Then another thing that I see in government that I find extremely disturbing is when they say it is under investigation. Therefore, we can't give you any information. That happens all the time. Many investigations on contracts or abuses on whatever, they will say, oh, we have referred it to our IG. It is under investigation. And for the next 5 years, you can't get any information. That is absolutely wrong and it happens all the time.

I had a case today, an EPA case where they are investigating something, so my constituent cannot get any information and they may not be able to get information for 10 years because it is under investigation and the investigation may never end. May she answer?

Mr. SHAYS. Yes, and then we need to move on.

Mrs. MALONEY. OK.

Ms. D'AGOSTINO. We actually run into ongoing investigation issues in our work for the Congress, as well, so there is not very much that we can do about it. We usually have to stand down and wait for an investigation to be completed before we can then do our work, so this happens to us, as well, even with our very broad authority.

But basically, in terms of appeals, the first step would be to make a FOIA request and request that a document be reviewed under——

Mrs. MALONEY. But I am talking about FOIA requests, when the FOIA requests come back completely redacted.

Ms. D'AGOSTINO. Right, and these appeals can be done through the judicial system. So you can take the issue to court.

Mrs. MALONEY. To court?

Ms. D'AGOSTINO. That is an option.

Mrs. MALONEY. But most people can't afford to go to court.

Mr. PODONSKY. Mrs. Maloney.

Mr. SHAYS. Why don't you respond and then I am going to ask my questions.

Mr. PODONSKY. In the Department of Energy, Mrs. Maloney, if something was requested under the FOIA and the recipient is not satisfied, we have a separate office called the Office of Hearings and Appeals that reports directly to the Secretary and that would give your constituents the opportunity to go separate from the office that was responsible for redacting the document to begin with.

Mrs. MALONEY. And do all agencies have it, or is this unique to the Department of Energy?

Mr. PODONSKY. I don't know what the other agencies have.

Mrs. MALONEY. Thank you.

Mr. SHAYS. I am going to yield myself time now to say that my focus—I think the whole issue of reclassification is interesting, but not really the issue that concerns me. I tend to think some is understandable. In one sense, I can explain it.

I think there was a dispute between the President and Congress, I think in one or two instances, and the reason it was pretty focused on the Department of Energy was there was sensitive information given out that related to things that could be very destructive involving nuclear information. I understand that. But I think it is somewhat stupid, because I think once it is out, it is out. So that is not what really bothers me.

What bothers me is what we had in previous hearings, where even from the Department of Defense, our witness there said up to 50 percent was over-classified and the outside organizations were in the 50 to 90 percent range. What that says to me is that people who need this information won't get it.

What bothers me, though, is the whole concept of "For Official Use Only," but really the more broad category of "Sensitive But Unclassified," SBUs. That is what I want to spend my time talking about.

Ms. D'Agostino, even your agency is a major offender here. No, seriously. I mean, we are almost asking you to investigate yourself because almost everything you provide us is "For Official Use Only." I am exaggerating slightly, but it is true. Tell me why.

Ms. D'AGOSTINO. Well, the GAO does not have classification authority, and as a result——

Mr. SHAYS. So let me translate. You do not have the capability to classify anything.

Ms. D'AGOSTINO. Correct. We give the documentation that we receive from other agencies the same protection that they do. In other words, we can't question their classification, say, of an FOUO document. I mean, we can question it, but basically if they say, look, this is FOUO and we have done a security review on your draft report and it is FOUO, then GAO must stand by——

Mr. SHAYS. Why is that? Maybe I need a little bit of an education on the whole concept of "Sensitive But Unclassified." It is in the statute. There is a process. What is the process that justifies anyone talking about "Sensitive But Unclassified?"

Ms. D'AGOSTINO. I mean, I am prepared to talk about the FOUO category, but basically, that is based in large part in statute in the FOIA, the Freedom of Information Act, and the folks who have the authority to designate information as FOUO are the folks in the executive branch who provide us the information.

Mr. SHAYS. Is it anybody? Could I write a document and say this is "Sensitive But Unclassified?"

Ms. D'AGOSTINO. In the Department of Defense, what our understanding is is the personnel of the Department are empowered to designate information——

Mr. SHAYS. Who empowers them?

Ms. D'AGOSTINO. They are empowered under the regulation that DOD follows for FOUO, the security regulation.

Mr. SHAYS. I am sorry, I am not clear. Are you clear about this? You are looking at me like——

Ms. D'AGOSTINO. No, no, no, no, no. I am just saying that GAO doesn't classify information.

Mr. SHAYS. Let's get you out of the picture. Tell me about——

Ms. D'AGOSTINO. Well, you were concerned that we were a big offender——

Mr. SHAYS. Well, I am concerned, but I don't want it to block you being comfortable telling me information. I am wrestling with the fact that it is almost like we have invented, like the executive branch has invented this process to which they then can run anywhere they want with it if they have it. Are you saying that when Congress passed the Freedom of Information law, we empowered this concept of "Sensitive But Unclassified?"

Ms. D'AGOSTINO. I didn't do a review of all "Sensitive But Unclassified." I mean, we focused our work on the OUO and——

Mr. SHAYS. OK. Let us do OUO. Talk to me about them.

Ms. D'AGOSTINO. Again, DOE and DOD have their regulations and their programs that govern this, and information generated by personnel within those Departments that they believe fits within——

Mr. SHAYS. Mr. Rogalski, maybe you can walk me through it, and then Mr. Podonsky.

Mr. ROGALSKI. They Department of Defense has a regulation called Information Security Regulation. We do not have, like we do original classification authorities, anyone in the Department of Defense is authorized to make that FOUO determination based on the guidance that is contained in the information——

Mr. SHAYS. Could you say that again? Everyone in the Department of Defense? How many employees do you have?

Mr. ROGALSKI. Two-and-a-half million cleared people, something like that, but let me finish my sentence.

Mr. SHAYS. Sure. I am sorry. I shouldn't interrupt you.

Mr. ROGALSKI. Subject to a review by their supervisor. So there is an inherent responsibility for supervisors in the Department of Defense to ensure that their employees are following the guidance contained in any regulation, directive, instruction we have in the Department. So we have an Information Security Regulation that specifies what are the criteria for applying the FOUO marking. It talks about the FOIA, the nine exemption categories. The first one that automatically exempts is if it is classified. And one of the things the GAO report recommended and we strongly endorse is we need better training among our employees within the Department of Defense.

So I think the way to achieve, I think, the balance you are looking for and the right thing to do is to put more rigor, have more standardized training, have uniformity across the Department, and so we recognize that and we have agreed to that in the GAO report and we are combining—we are including updated guidance in the rewrite of that 5201(R) regulation, the information for deregulation that is going to be published this year.

So to answer your question, employees have the authority, subject to, like anything in the Department, review by their supervisor.

Mr. SHAYS. Bottom line, every employee can designate it, but a supervisor has to sign off?

Mr. ROGALSKI. It is not a sign-off per se, but it is a review. If a member of my staff generates a document, whether it is FOUO or classified, it——

Mr. SHAYS. There is a difference. There is a difference. The implication I had from listening to, and that is why I wanted to say it and I appreciate you clarifying it, was we may have 2 million-plus employees, but their supervisor has to, I thought, basically approve it. It is possible the supervisor never even sees it, correct?

Mr. ROGALSKI. There is that possibility, but again, if that is an issue or problem, I believe that can be overcome through proper training, the supervisors understanding what their responsibilities are. But you are correct.

Mr. SHAYS. OK. Mr. Podonsky.

Mr. PODONSKY. Relative to your question, Congressman Shays, prior to 2003, the Department had over 20 different markings for sensitive information. The Office of Classification went forward with, in implementing the recommendation of the Hamre Commission report that I mentioned in my testimony, to bring that down to one, OUO, and as the GAO report recognized and I also say it in my testimony, we fully agree with we need to do a much better job of defining who has the authority to do the OUO, the training to make sure that it is done properly, and most important of all, to have an independent oversight of what is being done with those documents. So every part of the recommendations in the GAO report hit the heart of the issues at the Department of Energy.

I would say that we have a very able, professional, nonpolitical staff responsible for classification of documents, the OUO situation in the Department was not dissimilar to the Department of Defense other than the magnitude is much smaller because we only have 15,000 employees, of which 5,000 are classifiers, and our experience is mostly it is the 5,000 classifiers that are doing the OUO markings.

Mr. SHAYS. I have questions for each of you. Ms. D'Agostino, I would like to know what is your response to DOD's objections to a GAO recommendation that DOD mark FOUO documents with the appropriate Freedom of Information Act, FOIA, exemption?

Ms. D'AGOSTINO. Well, I guess we separate the two processes that——

Mr. SHAYS. Put the mic a little closer to you.

Ms. D'AGOSTINO. I am sorry.

Mr. SHAYS. No, I can hear you, but move it a little closer.

Ms. D'AGOSTINO. OK. If you think about a document as having a life cycle from the time it is created and marked by the person who created it, you have one separate process that deals with marking it to the time when, say, a FOIA request is made and this document comes through a totally separate process to be reviewed by a totally different group of people to determine whether or not it can be released to the public.

So the marking is a handling advisory, cautionary, almost, mode for this document that tells people, you need to be careful with this information and handle it according to the rules. Then there is a completely separate process to decide, that is triggered by a FOIA request, whether or not this information, regardless of how it is marked, is releasable to the public, and the front-end process has

no impact on the process to decide to release the information. So if there is a mistake made in the marking, or let us say it should have been marked and wasn't marked, it has no bearing on the decisionmaking that is done to release to the public under the FOIA request.

This is why we do not believe that the Department of Defense argument that it provided in its comments on this particular recommendation is very strong.

Mr. SHAYS. OK. Mr. Rogalski, maybe just a response.

Mr. ROGALSKI. Sure. When we looked at the GAO recommendation, we looked at the investment that they were suggesting we do by having people make that FOIA exemption up front when that FOUO determination is made. Some considerations to that we looked at were, one, if that document was created in 1998 and then someone comes in with a FOIA request in 2005, that FOIA exemption applied in 1998 may be different. Therefore, we question what is the utility of having a FOIA exemption placed on the document at the date of creation.

Second, our Office of General Counsel and the FOIA Office felt that if there was some type of litigation, an improper FOIA exemption was made on that, that could jeopardize anything that came up in a litigation. So that was our rationale on why we believe that we did not see the investment worth the return for putting that FOIA exemption on at the date of creation of that document.

Mr. SHAYS. Let me ask counsel to respond.

Mr. HALLORAN. Thank you. So the two rationale you pointed out, if the document is not going to be given out, why mark it at all at that point? If you are not going to specify why it may be nondisclosable, don't you invite abuse?

Mr. ROGALSKI. Obviously, there is information in the Department of Defense that does not meet any threshold for being classified, but there is information that, based on the Information Security Regulations deserves some type of protection less of classification. What that does, it provides a degree of protection for that information. It advises that DOD employee, I just can't take this document, if it is unclassified or not marked FOUO, now I can just put it on the street, give it to a reporter, or whatever. So that FOUO provides a gate, if you will, before that information can be released. If it were not marked, then it presupposes you can release it, even though in the Department we have a security review for documents before they are released.

Mr. HALLORAN. It is a gate without any reference to why there might be a gate, and the Department of Energy apparently hasn't had the legal problems DOD fears, have you?

Mr. PODONSKY. No.

Mr. HALLORAN. Because, as Ms. D'Agostino said, the FOI review process as to what exemption it might apply for is an absolutely separate and independent determination of what someone might estimate when the marking is made. I just don't see the legal peril it puts you in.

Mr. ROGALSKI. Well, fortunately or unfortunately, I am not a lawyer, so I think I need to take that as a question for record, have our FOIA office and our Office of General Counsel take that question and get back to you with a response, if that is suitable for you.

Mr. SHAYS. That would be fine. I would just like, before I go to Mr. Kucinich and then the next panel, I would like some observations from Mr. Weinstein and Mr. Leonard on what we have just been talking about.

Mr. WEINSTEIN. Which specific aspect, Mr. Chairman?

Mr. SHAYS. Just the questions that I have been asking. If you have no reaction, then you don't have to respond.

Mr. WEINSTEIN. I will pass to Mr. Leonard on that.

Mr. LEONARD. The whole issue of "Sensitive But Unclassified," basically, from our perspective, there are two broad categories. There are specific information that the Congress has told executive branch agencies they must protect. As a Federal employee, I am liable from sanctions or even criminally for disclosure of certain kinds of Privacy Act information, protected critical infrastructure information, things along those lines. The list goes on and on where there are statutorily based restrictions and a lot of that information ends up with an FOUO designation on it, and in a way, it is a notification to a Federal employee that, hey, this is the stuff that you can be held subject to sanctions for if you improperly disclose.

On top of that, there is another broad category of purely discretionary information that agencies can withhold under the FOIA if they choose, but they could also disclose. You know, there is such a wide disparity of information covered under this broad umbrella. Quite frankly, from someone who has almost 35 years' experience in the government, I have yet to be able to comprehend it to the point where I am comfortable and I think that is the biggest problem that the average Federal worker has in terms of there is just such a wide array of information that can be covered under this from different perspectives that the impulse is, well, what can I get into least trouble for?

Mr. SHAYS. One of the things that I thought when I was elected to Congress when I had a briefing, that I would actually learn something I hadn't read in the New York Times, and I will never forget a Member of Congress, after being briefed and we were told solemnly that this was classified and so on, so the Member of Congress stood up and said, now this is classified, this is classified, this is classified, and he had about 10 items, and then he took a New York Times article and just read it point by point and each one of those articles was covered.

I have read some things that are designated "Sensitive But Unclassified" that I think could be very awkward, not embarrassing but awkward and uncomfortable and not appropriate for someone to see, so I don't even want to imply that once in a while, I haven't read things that say "Sensitive But Unclassified" and think, gosh, this should be classified.

My general view is that we have an absurd system and I think, Professor, you realize that we have some huge problems. What we would like to do is we would like to augment what others have done in terms of appraising this and come up with some very concrete suggestions on how to reform this system.

Mr. Rogalski, I think to allow the employee to be able to say something is classified and then say a supervisor, I mean, the definition of a supervisor is kind of interesting and I want to just un-

derstand that process more because it doesn't seem logical to me that the system would be working this way. So I think there has to be more to the story.

At any rate, Mr. Weinstein?

Mr. WEINSTEIN. Just a few final thoughts, Mr. Chairman. I am really looking forward to the completion of the audit and getting that audit to you because the beginnings of any, I think, serious assessment that the Congress can do might be—it might be useful for your and your colleagues——

Mr. SHAYS. We will wait to do our report until after, but we are going to combine the whole issue of classification with civil liberties and a few other issues. The bottom line is, any administration that wants more authority has to have more oversight, and part of the oversight has to be that you have access to information and that everything isn't just hidden from the public and even Congress.

At this time, the chair would recognize Mr. Kucinich.

Mr. KUCINICH. Thank you very much, Mr. Chairman I think the chair is well spoken when he points out the inevitable political character of the classification system, and his comments are well taken when you consider that you can be told in closed session certain things are classified and then read about them the next day.

One of the reasons why I, as a Member of Congress, stopped taking the so-called Secrecy Oath right after you take your oath of office that enables you to go to the, "classified" briefings is that so many of the sessions I would go to, I would end up reading the next day. But as a Member of Congress, because I went to that session, I couldn't talk about it because of the oath that I took with respect to the secrecy.

So there is an overtly political character to the control of information, and I mentioned several examples in my opening statement where both classification and declassification of documents were done in an overtly political manner and I think this was particularly evident with the memo written by former Counterterrorism Chief Richard Clarke to Condoleezza Rice warning about the al Qaeda threat that was made public right before she testified to Congress on the administration's pre-September 11th intelligence knowledge.

I would like to ask a few questions here. Mr. Podonsky, how long have you worked for the Department of Energy?

Mr. PODONSKY. Twenty-two years.

Mr. KUCINICH. You are aware that the Department of Energy was one of the first Federal agencies to re-review documents that had already been released, particularly over allegations of Chinese spying in the 1990's? Are you aware of that?

Mr. PODONSKY. No, I am not aware of that.

Mr. KUCINICH. OK. In your work at the Department of Energy, did you ever have anything to do with the Wen Ho Lee case?

Mr. PODONSKY. The answer is yes. We had an independent oversight group go out for former Secretary Richardson to take a look at what the circumstances were.

Mr. KUCINICH. Was there any time at which classified documents relating to that case were withheld from public disclosure, said documents which may have been exculpatory of Mr. Wen Ho Lee?

Mr. PODONSKY. I believe I have third-party information that says, yes, that is true, because there was an ongoing FBI investigation.

Mr. KUCINICH. See, that is what I mean about the inherent political nature of classification. I would like to ask Mr. Leonard, I also mentioned the case of Luis Posada Carriles and the administration's justification of the NSA eavesdropping program and the Harmony Program. What other examples do you know of where the regular classification and declassification processes have been ignored or misused for political reasons? Any others you want to cite?

Mr. LEONARD. There is a basic premise in the Executive order that recognizes that information, even if it is disclosure, could reasonably be cause to, or expected to cause damage to national security, that information as a matter of discretion for an agency head can, in fact, be declassified if there is a compelling public interest to do so. The issue, then, I guess, obviously becomes who determines what is the public interest, and I think that is a responsibility that we all have as government officials, but ultimately, I tend to think that the public, then, will be the ultimate arbiter in terms of what is in their interest or not.

Mr. KUCINICH. There is another dimension there. It is not just classification or declassification, it is redaction, as well. You know, we haven't gotten into that too much, but with a pen, you can change the character of something that is released as being unclassified when actually the essential nature of the communication is kept from the public or remains classified. I mean, would you explain to me your concerns about the policies regarding redaction?

Mr. LEONARD. That is a very real concern. As a matter of fact, there are some people who use that as an excuse not to redact and instead withhold the document in its entirety for that very reason. Redactions, without a doubt, if not properly applied, can, in fact, change the gist of a document, can change the gist of the information as conveyed, and can leave the reader, at the very least, with an incomplete understanding of what is being discussed in the record, and quite possibly maybe even an incorrect understanding of what is in the record. So redaction is a very important tool. Again, the alternative is to withhold documents in their entirety, which I don't believe would likewise serve the public well, and so it is a tool that, when used properly, can be beneficial to all.

Mr. KUCINICH. Let me ask you something. What possible reason can you think of that documents from the 1940's and the 1950's still remain classified?

Mr. LEONARD. Well, let me give you two examples. The exemplars that were provided to me several months ago by the group of historians, absolutely nothing was contained in those. On the other hand, there is information even decades old—for example, one of the things that is repeatedly recognized——

Mr. KUCINICH. Well, 40 or 50 years ago, or 60 years ago.

Mr. LEONARD [continuing]. Repeatedly recognized as a shortcoming in our intelligence capability is the ability to recruit human sources. To recruit human sources, we need to be able to, as a government, as a Nation, to be able to assure those individuals total and complete confidentiality, not just today, not just tomorrow, but quite possibly for decades, and that——

Mr. KUCINICH. But forever kind of begins when you are dead, right?

Mr. LEONARD. Well, when you are asking someone to betray their Nation, when you are asking someone to betray their loyalty, when you are asking someone to put themselves not only in physical jeopardy but quite possibly their family and maybe even in some parts of the world their descendants, it is asking a lot and the concern is, and I believe justifiable, is it makes it increasingly difficult to recruit the human sources of today that we so desperately need as a Nation unless we can, in fact, assure them total and complete confidentiality for a period that is reasonable.

Mr. KUCINICH. I just would like to make a comment on this. I know you have to get to the other panel. It seems to me what drives this overall debate about classification and declassification is not simply a question of where the pendulum is swinging with respect to democracy or something less than democracy. There is also a dimension of fear here.

You know, when Francis Scott Key wrote the "Star Spangled Banner," he drew an equation. He asked if the star spangled banner yet waves over the land of the free and the home of the brave. He drew a connection between freedom and bravery, between democracy and courage. We have to remember who we are as a Nation. We are forgetting the really fearless nature of the American character which enables us to go about our business without worrying about whether secrets are going to be unearthed. We are kind of forgetting who we are as a country.

Mr. WEINSTEIN. Could I make a comment? Thirty-one years ago, I won what was probably one of the earliest Freedom of Information Act lawsuits against the FBI for files of historical interest, and my record on access issues is fairly clear-cut all of my professional life as a historian. But I have come to believe very strongly, as I think you and the chairman and others do, that the real question is striking the appropriate balance, that there are such things as legitimate things that for periods of time should be kept secret, whether it is scientific inventions or whatever, the identify of American agents or whatever this would be, and that the real issue becomes one of striking the balance.

One of your late colleagues who was a friend of mine and a friend of yours, I am sure, Senator Moynihan, did a little book on secrecy and pointed out some of the complexities of that issue, and it is to this subcommittee's enormous credit that it is trying to wrestle with these very complex issues and come up with some good solutions.

But I think we would all agree, would we not, that there is a balance that has to be drawn, that there are some things that are not political, but that perhaps deserve for a period of time the protection of legitimate national security constraints. I say that with all respect. It is what we are trying to do at the Archives, first of all, by getting the facts out, and I can assure this subcommittee that it will have every fact that we have at our command as soon as this report is available.

Mr. KUCINICH. I thank the gentleman. I would just like to respond by thanking him for his service, but also pointing out that

it is becoming increasingly aware that secrecy is the enemy of democracy.

Mr. SHAYS. Let me thank each of the witnesses and ask, is there anything that you want to put on the record before we go, a question that we should have gotten into that you wanted to put on the record?

Mr. LEONARD. The only thing I would like to add, Mr. Chairman, is you mentioned oversight and the need for effective oversight, and I couldn't agree with you more, especially from an organization with the word in my name, title. But in any event, I am pleased to remind folks that we now have a Public Interest Declassification Board. It is up and running. It is operational. It has five members appointed by the President. It has four members appointed by the Hill leadership. The Board had its first meeting several weeks ago. They are going to meet again the first of April. From all indications, this is a group that is intending to be very aggressive in all regards in terms of exercising oversight.

One of the things that I would be remiss in not mentioning is we are still two short of a full complement of membership. Specifically, we have the five appointees from the President and two out of the four from the Hill leadership. To the extent we could get a full complement——

Mr. SHAYS. What are the two leaders that——

Mr. LEONARD. One is from the Speaker and the other is from the Senate Minority Leader.

Mr. SHAYS. We will contact both offices.

Mr. LEONARD. I appreciate that very much, sir.

Mr. SHAYS. By tomorrow, we will contact both offices and let them know we think that we need to move along.

I know each of you in your own ways are concerned about this issue. First, to have the Archivist be willing to appear not as a separate panel, to me demonstrates a very fine quality which I want to thank you for being willing to participate. To the others, given that you are in that capacity, I want to thank our two government agencies because I know that both you know we have problems and want this system to work well and ultimately have the best interests of our country at heart. I appreciate that, and obviously, I always appreciate the good work of the Government Accountability Office, and Mr. Leonard, thank you so much for your contribution.

The bottom line is, if you could help us make some constructive suggestions, it would be to your best interest because our suggestions might be followed and therefore it would be nice that they be things that would make sense.

But the bottom line for me is we have to have more openness. The majority of the American people are truthful. They will have you do the right thing. When we hide so much from the American people, we hurt them and I get mixed signals from my own constituents because they don't have the facts that they need to have. I think that is true for other Members, as well.

So thank you all very much. I appreciate your participation today. Thank you.

We are going to close with our second panel. It is Mr. Thomas Blanton, executive director, National Security Archive, George

Washington University; Dr. Anna Nelson, distinguished historian in residence, American University; and Mr. Matthew Aid.

Mr. Rogalski, I just need to put on the record, you had mentioned something about 30 percent reduction. You are going to get the answer to that?

Why don't you stay standing so I can swear you in. Thank you. Raise your right hands.

[Witnesses sworn.]

Mr. SHAYS. I would note for the record all three of our witnesses responded in the affirmative.

We will start with you, Mr. Blanton. Obviously, your full statement is in the record. My general practice is, if you are the second panel, you get to have longer opening statements if you choose. You had the length of the others. But if you also deal with what you maybe heard in the first panel, that would be helpful. Mr. Blanton.

STATEMENTS OF THOMAS S. BLANTON, DIRECTOR, NATIONAL SECURITY ARCHIVE, GEORGE WASHINGTON UNIVERSITY, WASHINGTON, DC; ANNA K. NELSON, DISTINGUISHED HISTORIAN IN RESIDENCE, AMERICAN UNIVERSITY, WASHINGTON, DC; AND MATTHEW M. AID, WASHINGTON, DC

STATEMENT OF THOMAS S. BLANTON

Mr. BLANTON. Mr. Chairman, thank you very much for having us here. We are dealing with two of those "Houston, we have a problem" problems, and there is a very interesting connection between the two and my organization, the National Security Archives, is right in the middle of it. We are the people who filed that Freedom of Information request for that classified memorandum that you just asked for and we hope to have a sanitized version, the law said 20 working days, but we have learned our lessons on waiting for that. But when we get one, we will be glad to give one to you and see if the Freedom of Information Act works faster than congressional agency relations. Sometimes, it does.

But I wanted to point out one key point that no doubt you saw when Congressman Waxman was asking questions of the Archivist of the United States, that the Archivist of the United States wasn't in charge of the reclassification process, hadn't even known about it. That is an interesting signal because it bears precisely on the problem that you focused on on sensitive unclassified information. The agencies are in charge.

The agencies rolled the National Archives at least four times that I am aware of since 1996. The Department of Energy went first, when they found some mistakes in the release of information. According to Steve Garfinckel, Bill Leonard's predecessor, most of those mistakes related not to nuclear weapon design information, but rather to the obsolete cold war locations of nuclear weapons overseas. But we as taxpayers have spent tens of millions of dollars reviewing tens of millions of pages—kind of a full-employment program for reviewers, to pull out a few handfuls of items that might be useful to a Khadafi, and that program, I think, needs more oversight, but it is a paradigm of transparency compared to what the intelligence agencies have pulled off at the National Archives.

They watched, I think, the Department of Energy do this with the help of some amendments from Members of Congress and decided, oh, we would like that prerogative, too. We would like to go back and look at our own intelligence files, because mistakes were made. You heard that immortal Washington phrase, I think, earlier in the hearing today. "Mistakes were made." Well, those mistakes, we now know because of what Matthew Aid did in his research, those mistakes were of the variety, gosh, we didn't get to look at that before it came out. That is our document. We have an equity in that document, and that is a huge problem, the same problem that we found on the "Sensitive But Unclassified."

I just want to say here that our modus operandi is to file Freedom of Information Act requests and try to hold the government accountable, and so in answer to the questions that you posed over a year ago at your first hearing entitled, "Pseudo-Classifications," and we actually as a kind of "imitation, the sincerest form of flattery," named our report on the "Sensitive But Unclassified" program "Pseudo-Secrets." That is a tribute to you and this subcommittee. We filed Freedom of Information requests over the last year with 40-some-odd different major Federal agencies that together include more than 90 percent of the—95, 97 percent of the Freedom of Information Act requests that get processed and we got responses from most of them, but not all, and then we went and supplemented that with a lot of Web research.

We now have data on 37 agencies and what their policies actually are. You said earlier today that you had real trouble getting numbers. In fact, we have some numbers on this reclassification program. Fifty-five-thousand pages have been pulled out. That is the good news. We at least know the dimension of the problem. Nobody knows on "Sensitive But Unclassified." When you asked the agencies to tell you, they said, oh, we can never figure that out. That would cost too much, take too long. Nobody knows.

We thought at least through Freedom of Information requests we could at least find out how many separate policies were there and what was in those policies and how were employees being trained and guided and instructed on labeling records, and our conclusions are on page 6 of my prepared testimony and I think they are a little dismaying and should be dismaying to this subcommittee, and they are right on point to your questions, Mr. Chairman.

In 37 Federal agencies, we found 28 different, distinct policies governing "Sensitive But Unclassified" information with little, if any, coordination between agencies. Even though a lot of agencies shared the same words on their markings, like "Official Use Only" shows up a lot, "For Official Use Only," "Official Use Only," whatever, but not the guidelines, not the substance, not the internals of the procedures. None of the agency policies showed any monitoring, any oversight on the use or the impact of these policies. Only eight of the agencies actually had authorization from statute for their policy on "Sensitive But Unclassified," sensitive unclassified information.

Mr. SHAYS. And DOD would be one of them?

Mr. BLANTON. That is correct. DOE, as well, actually, which I think the GAO report very usefully points out. But, in fact, if you look back in the appendix of our report, you will see that DOD ac-

tually has three markings for sensitive unclassified information. Two of them are authorized by statute, but the other one is purely internal and that is the one that any employee can use. DOE has two markings for sensitive unclassified information. One of them is statutory. The other one is purely internal and any employee can use it. You get some really staggering notion of the dimension of the problem if you have 2.5 million employees in the Department of Defense, 180,000 in the Department of Homeland Security.

None of the policies featured a challenge or appeal mechanism for dealing with the markings, challenging the markings on any of these documents. Only one of the policies even contained a sunset, that a marking could only last for a maximum of 10 years. It was really striking to me, because you asked Mr. Leonard, what is the maximum sunset in the Presidential Executive order on classification, "Top Secret" is for 10 years or a date certain. This is fascinating. You are raising any employee can stamp document marking restriction to the level of "Top Secret" in terms of its duration. It is extraordinary.

Eight agencies effectively allow any employee to do this. DOD and DHS are the two biggest.

Only 7 of these policies, 7 out of 28 policies, have the kind of qualifier that is written into the Executive order that says, you can't mark documents this way, you can't hide them in this way if you are covering up embarrassment, malfeasance, mismanagement, illegality, etc., only 7 out of 28.

Finally, 11 agencies report no policy at all on their internal—we believe some of those agencies have such markings, use such markings, but they have no policy at all.

The bottom line is of all this, I think you can conclude by the diversity of policies and the lack of coordination and the lack of any kind of commonality, the decentralized nature of the administration, I think neither Congress nor the public can tell for sure whether these kind of markings and safeguards are actually protecting our security or being abused for administrative convenience or cover-up. That is the bottom line.

How would you fix it? You started last year. You started asking agencies, how many are there? I mean, even to just get a handle around the problem, poor GAO couldn't take on the whole government. They had to just take on two departments and they still don't know how many "Official Use Only" and "For Official Use Only" documents there are. There could be millions. There could be billions. We don't know.

Congress is going to have to order the agencies to report it. That is the only way you get this data. We didn't get cost data on classification until an amendment from the House of Representatives went into the appropriations bills in 1994 and 1995 and said, agencies, report how much you are spending to keep your documents classified, on safes, on clearances, physical security, computer security, everything. That is how we know today we are spending $7 billion on classification. That is the kind of question that has to be asked. I think you are going to have to legislate it. I think that is what you have already found over the last year.

Second, you are going to have to set some limits. Good parents set limits. Good congressional subcommittees set limits. You are

going to have to set some limits, and that includes on the number of people who can put these kind of markings on documents, and you have to set some limits like sunsets, duration limits, and you are going to have to have some kind of appeal mechanism, challenge mechanism for insiders and outsiders for these kinds of markings. Otherwise, it is totally out of control.

I think, third, you are going to have to move to rules across agencies, common rules, common standards, common criteria. You have to have that prohibition on using these markings to cover up embarrassment, malfeasance, criminality, because without that, even the internal reformers, and I count a number of the people on that previous panel as internal reformers, just don't have a lever against the overuse, against the abuse, as your counsel asked.

I think those are the bottom lines on the "Sensitive But Unclassified" information. I just want to finish with a comment about the reclassification program, because I think the commonalities here are pretty interesting.

Congressman Waxman mentioned a document on balloon drops this morning from 1948, widely published. In my prepared testimony, I had planned to just read out a sentence from that document about how, don't do them in winter, you know, unfavorable launch conditions, landing conditions, off-target and people can't find the leaflets on the ground when there is snow. But if I read that out, it would put everybody in the room at legal jeopardy according to the No. 2 person in the Department of Justice, Paul McNulty, who is bringing a prosecution over in Virginia right now for unauthorized possession of classified information.

This is the danger when the agencies get a hold of the process and drive it. I think the same impetus that led to this reclassification program is leading to that kind of prosecution, that kind of vast overreach, invitation for selective prosecution, invitation for abuse. It is just wrong in a system that you have established minimum 50 percent is over-classified.

So how do you stop a bureaucratic takeover? Well, the good news is, out at the National Archives, we have a couple of good examples of things that worked, things that changed the rules, things that moved stuff out in the public record. Congresswoman Maloney sponsored one of them on the Nazi War Crimes Act. Dr. Nelson, to my left, was on the Kennedy Assassination Records Review Board. Those processes worked to force documents out of the government because, A, they had a law behind them; B, they had an independent audit board to hold the agencies' feet to the fire; and C, they set a different standard of review, particularly for intelligence information, like those Nazi war criminals who were hired.

Mr. SHAYS. Thank you——

Mr. BLANTON. My last point is just simply if we don't establish those mechanisms, then I will see you next year with some new embarrassments from the front page.

Mr. SHAYS. Thank you very, very much.

[The prepared statement of Mr. Blanton follows:]

Testimony by Thomas S. Blanton,
Director, National Security Archive,
George Washington University
www.nsarchive.org

14 March 2006

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

Mr. Chairman and distinguished members, thank you for having this hearing today, during the week that Americans are celebrating as Sunshine Week. I'm reminded of that fundamental point made by a Princeton professor named Woodrow Wilson in his landmark study titled *Constitutional Government*, published in 1885. Wilson remarked that "*The informing function of Congress should be preferred to its legislative function. The argument is not only that discussed and interrogated administration is the only sure and efficient administration, but more than that, that the only really self-governing people is that people which discusses and interrogates its administration.*"

Of course, Mr. Wilson changed his mind once he got to the White House. But that's another story.

We are here today to discuss and interrogate our government about two of what I'd call "Houston, we got a problem" problems. One of them is the fact that securocrats have been scouring the open shelves of the National Archives for 50-year-old documents they can stamp secret again. We know some of the dimensions of the

problem: 40 million plus pages reviewed, and 55,000 pages of previously open records shoved back into the vault.

At least we have numbers here. For the other "Houston, we got a problem," we don't even know how big and bad it is. Government agencies are slapping new unclassified markings on records, like "Sensitive But Unclassified" or "Sensitive Security Information" or "Limited Official Use" and no one really knows how many records are covered, or for how long, and there are practically none of the limits that we do have in the security classification world.

I don't want to say we have figured out how to run a classification system. Despite the best efforts of public servants like William Leonard, the evidence you have produced in these hearings, Mr. Chairman, shows that we are far from any kind of rational, efficient, cost-effective, credible security classification system. You pressed one of Secretary Rumsfeld's deputies over and over on the question of how much over-classification there is, and she finally conceded that it was a "50-50" problem. Other folks who know have even higher estimates, like Governor Tom Kean, who read the latest Bin Ladin and counterterrorism information while he was head of the 9/11 commission, and said afterwards that 75% of what he saw that was classified should not have been.

And this is in a system that has checks and balances. There are government-wide standards for classifying, in statutes like the Atomic Energy Act and in the key Executive Order (12958 amended by 13292). There is an audit agency, the Information Security Oversight Office, reporting annually to the President and the public. There is the Interagency Security Classification Appeals Panel, ISCAP, which has brought far more rigor to the agencies' judgments over what should be classified and what should not. There are cost data, gathered by the Office of Management and Budget as ordered by Congress, totaling more than seven billion dollars last year. There are court cases, which rarely overrule government claims, but always provide a venue that forces additional review, and usually, additional documents to be released.

In the sensitive unclassified information field, there are no such checks and balances. After last year's hearing, Mr. Chairman, you asked one of the witnesses, Admiral McMahon of the Department of Transportation, how many times DOT had labeled records "for official use only" or similar designations. The Admiral wrote back, "During the period in question, we did not keep records of restricted information designations other than national security classifications." He reported only two uses of the "sensitive security information" label since DOT had begun keeping records on that in January 2005. (Maybe keeping records had a downward effect on how often the stamp was applied.) But on "for official use only," "we have no record of how many times."

I want to applaud this Subcommittee, Mr. Chairman, for commissioning the Government Accountability Office to study this problem. The GAO study of the Transportation Security Administration and its new "Sensitive Security Information" policy, completed in June 2005, found that "accountability and consistency" were lacking and that "clear policies and oversight" were needed. The new GAO study released at today's hearing shows that the Energy Department and the Defense Department had policies on "official use only" but lacked clarity in those policies, lacked training requirements, and lacked oversight to make sure the markings were appropriate and consistent.

The GAO's findings, and the testimony of knowledgeable officials like William Leonard of ISOO, move us towards some better, if not yet best, practices on handling sensitive unclassified information.

My own organization, the National Security Archive at George Washington University, has developed our own particular way to study government behavior. We file Freedom of Information Act requests, then compare what comes back – a Freedom of Information Audit. Sometimes we wait years – our latest audit of federal backlogs on Freedom of Information requests shows that some agencies have stalled so long that the requests would be old enough for drivers' licenses in most states.

We decided to look at the sensitive unclassified information issue back in 2002 when we came up with surprising results from an Audit. We had asked agencies how they responded to the infamous memo from Attorney General Ashcroft in October 2001 declaring the end of the discretionary release. Mr. Ashcroft told agencies, if you can find any exemption to claim, we'll back you up. We found very diverse responses across the government, ranging from a few agencies who saw the memo as a "radical change" for FOIA, all the way to a few agencies who asked us, "What Ashcroft memo? Could you send us a copy?" But many agencies mentioned another memo altogether as the key order they were following to scale back public information.

This was the so-called Card Memo, authored by White House Chief of Staff Andrew Card in March 2002, right after a front page story in the *New York Times* reported the government was still making publicly available "formerly secret documents that tell how to turn dangerous germs into deadly weapons." The Card Memo, together with an attached joint memo from ISOO and the Justice Department, directed agencies to take a hard look at how they were identifying and protecting information relating to weapons of mass destruction, including chemical, biological, radiological and nuclear weapons.

We sent Freedom of Information Act requests to each of 35 major federal agencies in January 2003 for copies of their responses to the Card Memo. Only the CIA and AID have failed to answer, three years later. Overall, the Card Memo had precisely the advertised effect: 10 agencies reported removing material from their Web sites, and 16 provided documents showing increased emphasis on using exemptions to the Freedom of Information Act. But 9 agencies told us they had no responsive documents – is it possible that they failed to report back as required to Mr. Card or to the Department of Homeland Security?

I do want to point out that a number of the agency changes in response to the Card Memo were entirely reasonable. Some agencies established task forces that developed clear criteria for what should be posted on the Web and what should not. Some agencies used the review to enhance their cyber-security and firewall

protections. Two agencies – the Environmental Protection Agency and the Department of Defense – even took the opportunity to remind employees to recognize both the risks and benefits of the free exchange of information.

But the Card Memo audit flagged for us the remarkably wide range of agency initiatives focused on protecting sensitive unclassified information – what William Leonard has called a "patchwork quilt" of guidelines and procedures and practices. Our next step was to file Freedom of Information requests about those agency policies. No one could tell how many documents were being marked with sensitive unclassified markings, but surely we could count the number of agency policies, find out on what authority they were based, and get some real comparative data on what they had in common and what was different.

So in February 2005, the month before this Subcommittee held its hearing on "Pseudo-Classification," as the Chairman has memorably named the phenomenon, we filed Freedom of Information requests with 43 agencies for their directives, training materials, guides, memoranda, rules and regulations on sensitive unclassified information. We now have results, through answers to our requests and from on-line research in agency Web sites, for 37 agencies across the federal government.

Those are the results we are releasing today, here at this hearing, and on our web site at www.nsarchive.org. Our title borrows from your own, Mr. Chairman: "*Pseudo-Secrets: A Freedom of Information Audit of the U.S. Government's Policies on Sensitive Unclassified Information.*" I appreciate the Subcommittee's including the full report in today's hearing record. And I must give credit where credit is due: This report is the work of extraordinary persistence in filing Freedom of Information requests and following them up, carried forward on the Card Memo by Barbara Elias, the tenacious director of our Freedom of Information Project, and on agency policies by Kristin Adair, our able Freedom of Information Associate, who also prepared the several drafts of this report. Archive general counsel Meredith Fuchs directed the entire effort

over the past three years and served as executive editor of the report.

In those 37 major federal agencies, our Audit found:

- 28 different, distinct policies on sensitive unclassified information with little, if any, coordination between agencies.
- No agency monitors or reports on the use or impact of these sensitive unclassified information policies.
- Only 8 agencies' policies are authorized by statute and implemented by regulation.
- No challenge or appeals mechanism for questioning the markings exists in any of the policies.
- Only one policy contains a "sunset" provision for the sensitive unclassified markings – at the Agriculture Department – but the maximum duration of 10 years is the same as for Top Secret information in the classification system.
- 8 agencies effectively allow any employee to slap protective markings on records, including the largest single department other than Defense, Homeland Security (more than 180,000 employees).
- Only 7 policies include cautions or qualifiers against using the markings to conceal embarrassing, illegal or inefficient agency actions (in the classified system, this is an explicit prohibition).
- 11 agencies report no policy on sensitive unclassified information (these agencies may use "official use only" and similar markings, but not – apparently – to protect information that is sensitive because of its security implications, which was the core of our Audit).

You can draw your own conclusions, but we believe that the diversity of policies, the ambiguous and incomplete guidelines, the lack of monitoring, and the decentralized administration of information controls on sensitive unclassified information – all of which is evident in our Audit results – means that neither the Congress nor the public can really tell whether these sensitive unclassified information policies are actually working to safeguard our security, or are being abused

for administrative convenience or coverup. So what do we recommend?

First, let's get some hard numbers. How many officials can apply these markings? How many records are they marking? How often do these markings affect releases (or withholdings) under the Freedom of Information Act? We have this kind of data for the formal security classification system, thanks to ISOO's tracking and sampling and data collection; and the first step towards reform of the pseudo-secrecy system is to get a handle on the numbers.

Second, let's set some limits, not just on the number of officials who can apply the stamps, although that would be a good start. Every agency needs a mechanism for both insiders and outsiders to challenge the pseudo-secret markings and appeal agency use of such restrictions. Every marking needs a sunset, a limited duration.

Third, let's make some rules across all the agencies. For one, the rules need to prohibit using pseudo-secret markings to cover evidence of maladministration, malfeasance, or embarrassment. For another, the rules need to detail the criteria that agencies should use before they can apply such markings, along with uniform handling and protection standards.

There is much more in our report on Pseudo-Secrets, including detailed Appendices with agency-by-agency breakdowns. I look forward to working with this Subcommittee, with you, Mr. Chairman, and with our colleagues at GAO and ISOO, as all of us struggle with this enormous problem.

In the meantime, we have another problem we're working with ISOO to clean up. You asked me to say a few words about this front-page story, how government reviewers out at the National Archives have been pulling previously open records off the shelves and reclassifying them. I know the agencies claim this is not reclassifying, just their correction of previous inadvertent and mistaken releases, but call it what you want, I call it counterproductive, destructive to the credibility of the information security system overall, and all too

telling about the current spate of secrecy mania we're seeing in the federal government.

My own staff had come across this phenomenon of reclassification probably a dozen times in the last few years. Archival boxes at the National Archives in College Park that we had looked at a few years back, now filled with withdrawal sheets instead of the documents. But so many disparate collections were involved – Mexico, Soviet Union, nuclear proliferation, Cuba, and more – that we blamed the other various re-review programs that have been going on since 1998.

The Department of Energy was the first to take on the task of putting toothpaste back in the tube. Partly because of the controversy over alleged Chinese spying in the 1990s, up to and including the Wen Ho Lee case, Energy started re-reviewing documents that had already been released. Energy found – in the immortal Washington phrase – "mistakes were made." Congress responded with the Kyl-Lott amendment in 1998 setting up a formal re-review process with actual budgets and regular reporting. Over the years, this effort has pulled more than 5,000 pages of documents containing what Energy describes as Restricted Data and Formerly Restricted Data related to nuclear weapons. Skeptics including William Leonard's predecessor at ISOO, Steve Garfinkel, have described the process as a waste of taxpayers' money, since the vast majority of pages pulled from the files have no information that would actually aid a terrorist or a would-be proliferators, but rather contain location information for U.S. nuclear deployments abroad during the Cold War.

Skeptics to the contrary notwithstanding, the rest of the bureaucracy looked on with awe at Energy's success. Money from Congress to take over control of government-wide declassification? Now we know that is what the intelligence agencies pioneered starting in 1999, based on their finding "mistakes" in the release of State Department intelligence bureau documents. Of course, most of the mistakes were of the "nobody asked me" variety; the CIA and other intelligence agencies wanted their say, and the current agency-

centric rules require referrals to the point of an almost-endless daisy chain of review and re-review.

The intelligence re-review seems to have escalated in its reach after 2001. Possibly a major encouragement came from President Bush's executive order in November 2001 giving former Presidents and (for the first time) former Vice-Presidents the power to stall indefinitely on release of their White House records – even though the law actually gave that authority to the Archivist of the United States. Seeing the National Archives get rolled bureaucratically by the White House certainly did not signal the spy agencies to restrain themselves and focus their attention on fighting terrorism rather than re-fighting the Cold War and reclassifying the old files.

We might never have connected the dots without Matthew Aid, that enterprising historian of intelligence. His testimony will explain how he did it, but as soon as he came to us, the light bulb went on. His examples of idiotic secrecy were what journalists call TGTC – too good to check – but Matthew had checked them all out.

Let me read you one. This is one of the documents that is now missing from the boxes on the shelves, all that's left in the box is a sheet that says "withdrawn" – sorry, it's a secret.

The document reports that if you're dropping propaganda by balloons over enemy territory, don't do it in winter because of "increased risk in launching due to unfavorable ground conditions; less favorable wind conditions which may result in depositing the load over neutral territory, and considerably less effect in the target areas due to difficulty of finding the leaflets on snow-covered ground."

I have to warn you, Mr. Chairman, according to the number 2 fellow at the Justice Department today, Paul McNulty, you are in legal jeopardy right now. Everyone in this room is now in unauthorized possession of classified information. Mr. NcNulty has said such unauthorized possession is a criminal violation of the Espionage Act. Doesn't matter that it's 50 years old. Doesn't matter that they can't prove any damage to U.S. national security. Doesn't matter that

you're a Congressman or you're a journalist or you're a citizen. Mr. McNulty said – and a federal judge named T.S. Ellis III astonishingly agreed – "anyone" who comes into unauthorized possession of classified information is liable for criminal prosecution.

That's the government's excuse for prosecuting two lobbyists from the American Israel Public Affairs Committee for receiving (through their ears) classified information about Iran. Anybody who read the *Washington Post* yesterday (13 March 2006) is now in possession of more highly classified information about Iran than anything those AIPAC lobbyists were told. And right now, here in Washington and around this country, FBI agents who should be chasing Osama bin Ladin's buddies are chasing journalists and career public servants who just blew some whistles. This approach is an invitation to selective prosecution and abuse of power.

I strongly suspect that the bureaucratic takeover by CIA out at the National Archives, assisted by the other intelligence agencies, comes from the same obscure insiders who are pushing the official secrets act and the AIPAC prosecution and, like CIA director Porter Goss, would like to see journalists hauled into court about their reporting of national security matters that CIA would prefer to keep in the dark.

The CIA has the money to take over the declassification process like this, and hardly ever experiences a debate about how much it is spending, because the CIA budget is secret, and doesn't go through the bargaining process that the National Archives has to suffer with. The CIA also has the National Security Act of 1947 with a mandated shroud over sources and methods, with no cost-benefit requirement or prohibition on using that claim to cover up criminality, embarrassment, or inaccuracy. Compare that inadequate language to the restrictions President Bush has maintained in his Executive Order on classification. So sources like Manuel Noriega have used their cover and apparent protection to aggrandize power, smuggle drugs and murder opponents. Sources like the Guatemalan colonel Alpirez have used their cover and protection to cover up the murder of an American citizen. Sources like the now-infamous Curveball

pitched lies about Iraq weapons of mass destruction and the secrecy kept challengers and fact-checkers at bay.

The credibility of the classification system is at issue here. When the security system itself loses that credibility, we lose our ability to protect our real secrets. When even the mundane is classified, we're applying the two-edged sword of secrecy to our own law enforcement and national defense efforts, and keeping ourselves from connecting the dots. When we keep our citizens in the dark, then we as citizens can neither protect ourselves nor pitch in to protect others – the way those passengers on Flight 93 stormed the cockpit and saved lives right here on Capitol Hill.

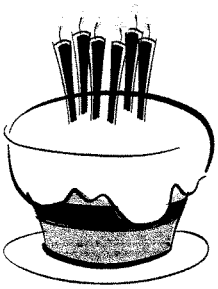
To fix the problem we're facing at the National Archives, not just over-classification but over-re-classification, we will need to do more than just applaud the national declassification initiative that Archivist Alan Weinstein and ISOO director William Leonard are recommending. They are exactly right that continuing the current agency-centric approach to declassifying historic records is a recipe for more inefficiency and more inappropriate classification.

We do have some best practices we can call on for lessons about how to do it right. Look at the tremendous successes we have seen with the Nazi War Crimes Interagency Working Group, and the Kennedy Assassination Records Review Board. Those efforts succeeded in lifting the cold, dead bureaucratic hand from historic records for three reasons:
1. They had a law behind them that clearly stated the goal, release of these historic records.
2. They had an audit board, independent and nonpartisan, that held the agencies' feet to the fire.
3. They had a different standard of review for intelligence documents, one in which the undefined phrase "sources and methods" which comes from the 1947 National Security Act did not trump all the other governmental and public interests in these records.

We can replicate these successes in the new Declassification Initiative, as long as that effort has the resources to bring all the agencies to the table. Congress needs to authorize, for all classified documents more than 25 years old (the time period given in President Bush's Executive Order after which the threat of automatic declassification looms), new standards of review like those that worked for the Kennedy assassination records and for the Nazi War Crimes documents. The latter included the only CIA names files that have ever been declassified, I should note, with absolutely no damage to U.S. national security. And those files dated back to the 1940s and 1950s, just like the documents that we now know have been shoved back into the vaults.

I thank you for your attention, Mr. Chairman and members of the Subcommittee, and I welcome your questions.

A FOIA REQUEST CELEBRATES ITS 17th BIRTHDAY



A Report on Federal Agency FOIA Backlog:

Oldest Unanswered Freedom of Information Act Requests Were Filed in 1989

March 2006

The National Security Archive
www.nsarchive.org

The George Washington University
Gelman Library, Suite 701
2130 H Street, NW
Washington, D.C. 20037
Phone: 202/994-7000
Fax: 202/994-7005
nsarchiv@gwu.edu

DECLASSIFIED
TOP SECRET

A FOIA REQUEST CELEBRATES ITS 17th BIRTHDAY

A Report on Federal Agency FOIA Backlog: Oldest Unanswered Freedom of Information Act Requests Were Filed in 1989

Executive Summary

In an effort to identify the oldest unanswered Freedom of Information Act (FOIA) requests in the federal government, the National Security Archive used the FOIA itself to ask more than 60 federal agencies for copies of their ten oldest pending FOIA requests. The results are astonishing—requests as old as 17 years remain unanswered, some agencies are unable even to identify their oldest requests, and agency backlogs are significantly more chronic and extensive than the agencies' annual reports to Congress indicate.

The oldest FOIA request unearthed by the Archive's Audit was submitted in March 1989 to the Department of Defense by a graduate student at the University of Southern California, asking for records on the U.S. "freedom of navigation" program. So much time has elapsed since the initial submission of that request that the requester, William Aceves, is now a tenured professor at California Western School of Law. Other agencies that have requests more than 15 years old include the Central Intelligence Agency, the U.S. Air Force, the National Archives and Records Administration, and the Department of Energy. The CIA claims four of the oldest ten pending FOIA requests in the government—from November 1989, May 1987 (Received at the CIA 1990), January 1991, and February 1991.

These results are even more shocking because many of the same ancient requests had turned up in the Archive's 2003 Freedom of Information Act Audit. [LINK TO 2003 Audit] The 2005 Audit reveals that 60 requests identified by agencies as their oldest pending requests in 2003 still have not been answered. Although the 2003 Audit called attention to certain agencies' shameful processing failures, many of these FOIA offices continue to let their oldest requests linger.

The oldest request uncovered in the Archive's 2003 Audit, a 1987 letter from San Francisco Chronicle reporter Seth Rosenfeld on FBI activities in Berkeley, California, was not provided by the FBI in their latest list of oldest pending requests, indicating that the FBI now considers this request closed. According to Mr. Rosenfeld, the November 1987 request, which clarified an earlier 1981 request, has not yet completely been fulfilled. The FBI has provided Mr. Rosenfeld more than 200,000 pages over the past 25 years, and provided responsive documents as recently January 31, 2006, but has not completed processing.

Another request designated in 2003 as one of the oldest in the federal government was an October 1989 request to the CIA, submitted by Lancaster Pennsylvania's *Intelligencer Journal* for documents related to James Howard Guerin and his business ventures. According to James Bamford's bestselling book *Body of Secrets*, Guerin ran a company in the 1970s and '80s that served as a cover between the National Security Agency (NSA) and South African intelligence services that allowed the NSA to monitor Soviet naval activity off the Cape of Good Hope, while overriding official U.S. sanctions on South Africa's apartheid government. Bobby Ray Inman, head of NSA from 1977-1981 and Deputy Director of the CIA from 1981-1982, served on the board of Guerin's company in 1982. In August 2004, almost a year after the Archive published its 2003 Audit and almost fifteen years after the *Intelligencer Journal's* initial request

National Security Archive © 2005

to the CIA, the newspaper received a final response from the CIA saying the agency *had not found any documents* and was closing the request.

In some situations, agencies can reasonably justify a processing delay by citing interagency coordination and security review backlogs. In the case of the *Intelligencer Journal's* request for information pertaining to James Howard Guerin, however, no explanation was offered to justify the need for fifteen years to conduct an unsuccessful initial search for such a clear FOIA request. Additionally, it seems likely that the CIA would have documents on Guerin, a man convicted of smuggling $50 million in arms into South Africa and a total $1.4 billion in international fraud. Guerin was directly tied to U.S. intelligence agencies and maintained a longstanding relationship with the former head of the NSA.

Overall, four of the ten oldest pending FOIA requests in the federal government identified in the 2003 Audit were identified as still currently pending. This figure does not include several 1987-89 requests that were provided by agencies in both 2003 and 2005 as among their oldest requests, but were either requests received on referral from other agencies or requests suspended for several years in litigation. Such requests, despite their age, are counted in the Archive's audits from the date the requests were received by the agency that provided the requests to the Archive, not the date of the initial request letter. The inter-agency referral system is a significant source of delay, but the Archive chose not to attribute such delays to the agency ultimately responsible for processing the request. As for legal battles, the length and reason for the delays is fact-specific and not necessarily a sign of agency non-responsiveness. It is also important to keep in mind, though, that these 1987-1989 requests asked the government for documents before the collapse of the Soviet Union, and the requesters are still waiting for a response.

The data generally shows that the FOIA backlog problem has not improved over the past three years. Most agencies have a similar backlog today as they did in 2003. By analyzing the age and date range of the ten oldest requests provided, the Archive ranked agencies that have reduced their backlog, maintained the same backlog, or increased their backlog. The data shows that some agencies successfully processed all of their oldest requests since the Archive's initial Audit and maintain a less significant backlog. Most agencies, however, maintain a backlog similar to or older than in 2003, and several continue to fail at processing their oldest requests, some of which date back ten or fifteen years.

Other highlights of the Archive's 2005 FOIA Audit include:

- **Six agencies or components have the same single oldest request today that they had in 2003**: Air Force Education and Training (Oldest request from June 1994), Air Force Materiel Command (May 1999), Central Intelligence Agency (May 1987), Department of Defense (January 1987), DOT/Federal Aviation Authority (February 1997), and the National Archives and Records Administration (March 1990).

- **Agencies have not established adequate FOIA request tracking systems.** In their latest responses, some agencies identified requests that should have been included in their 2003 ten oldest requests response, but for unknown reasons such requests were not identified as pending even though their dates indicate they were open and pending in 2003. For example, the Defense Intelligence Agency's current ten oldest included requests dated October 19, 1995, March 18, 1996, June 4, 7, 8 and June 12 1996. These requests were pending in 2003 and should have been considered as some of the oldest requests at the agency in 2003, but were not provided to the Archive in 2003 as part of the DIA's 10 oldest requests. The DIA provided other younger requests in 2003, including an August 1, 1996 letter. Similarly, the Department of Energy reported its oldest request in 2005 was a July 16, 1990 request, but in 2003 it reported its oldest was dated May 14, 1991. A similar situation is reflected in the

National Security Archive © 2005

National Archives, FBI and Securities and Exchange Commission responses, which in 2005 included requests that should have been, but were not, part of their 2003 responses. All of these requests referenced in this paragraph were sent directly to the agency and were not held up in an interagency referral system. These disparities between the 2003 and latest response may reflect improved agency FOIA recordkeeping or may indicate that agencies are generally failing to adequately and consistently track their FOIA requests.

- **Agencies are failing to effectively administer their FOIA programs and communicate with requesters.** Agency records regarding pending FOIA requests are not consistent with requesters' expectations. Some agencies' ten oldest requests fail to reflect requests that FOIA requesters believe are open and being processed. For example, the Archive never received a response from the DOT/Federal Railroad Administration (FRA) in response to its request for the oldest pending requests at FRA in 2003. A new request was filed with FRA in 2005 for copies of their oldest requests as of 2005, but FRA's response did not include the Archive's pending 2003 request, which would have been its oldest request. Additionally, Army Intelligence and Security Command, one of the agencies that showed the greatest backlog reduction between 2003 and 2005, according to their responses to the Archive's Audit requests (from October 1989 – October 1999 in 2003 to December 1996 – April 2005 in 2005), did not include several requests the National Security Archive believes are still open and pending. National Security Archive records indicate that over 30 requests are pending with Army Intelligence and Security Command that pre-date April 2005 and thus should be part of the response. Discrepancies between agency data and requester data supports the conclusions that the tracking and monitoring of FOIA administration is not being adequately conducted at certain agencies and that there is not enough communication between requesters and agencies over aging FOIA requests.

- **Withholding information under the FOIA is a subjective process and the Audit revealed a rise in secrecy from 2003 to 2005.** In several cases the same requests were released in 2003 and again in 2005 with different excisions. Where the same records were released during both surveys, they often contained more information in their 2003 form. The 2005 responses brought not just different excisions, but also more extensive withholding claims. This is the case with records released by the National Archives, Air Force Materiel Command, the Securities and Exchange Commission, and the FBI. These differences highlight both the inherent subjectivity in the review and redaction process, and suggest a greater tendency to withholding information from the public in 2005 than in 2003.

- **Agencies lose FOIA requests.** Eleven out of 64, or 17.2 percent of initial requests sent by the National Security Archive for the 2005 Audit were reported by agencies as never received. The Archive sent these requests via fax or e-mail and always used the FOIA contact information provided by the agency on their website. In spite of confirming that the Archive had the correct contact information and had followed agency instructions regarding submitting a FOIA request, a remarkably high percentage of agencies – 17.2 showed no record of ever receiving the initial request.

- **Despite the passage of eleven months, several agencies failed to respond to the Archive's request for copies of their ten oldest pending FOIA requests.** Furthermore, several of these agencies are the same agencies that failed to process the same Archive FOIA request in 2003. These include the Department of State, the U.S. Coast Guard, and the Department of Labor. Agencies that were able to respond in 2003, but failed to fulfill the Archive's 2005 request in spite of the passage of a comparable timeframe, include the Agency for International Development, U.S. Central Command, Health and Human Services, and the Office of Personnel Management. The Archive has not been able to determine whether these agencies are incapable of identifying their ten oldest requests or if these agencies are so under-resourced that they cannot even come close to meeting the FOIA's time limits.

National Security Archive © 2005

In the two years since the Archive's 2003 report, there have been several hearings in Congress about FOIA and various proposals for FOIA reform. Most recently, on December 14, 2005 President George W. Bush issued Executive Order 13392, "Improving Agency Disclosure of Information." In the Executive Order, the President ordered agencies to implement citizen-centered FOIA operations and sought to ensure senior official oversight of FOIA processing by ordering the appointment of a Chief FOIA Officer at the Assistant Secretary or equivalent level. The Executive Order has been greeted with a mixed reaction by the public, in part because the Administration's only other broad guidance on FOIA was Attorney General Ashcroft's October 2001 Memorandum encouraging greater use of FOIA exemptions and reduction in discretionary releases. Because the Executive Order strongly suggests that agencies will not be given additional resources to solve the problems they have been unable to solve over the FOIAs 40-year history, it is hard to imagine that dramatic changes will result. Moreover, because the Executive Order keeps the entire process of identifying problems and setting milestones for improvement within the agencies, it is hard to imagine the resulting goals will be very ambitious. As Senator John Cornyn (R-TX) stated, the Executive Order should not be seen as anything more than a "first step."

The Archive's Audit reveals problems far more systemic and extensive than the customer service concerns that E.O. 13392 addresses. Although it certainly is important to have the President reaffirm the government's commitment to transparency and responsiveness to Freedom of Information Act requests, a more fundamental change to FOIA administration may be needed than what is provided in the Executive Order. Based on these FOIA Audits the National Security Archive makes five general recommendations regarding FOIA processing.

FOIA Backlog Audit Findings and Recommendations

The Archive's Audit supports the need for additional steps forward to ensure that agencies comply with their obligations to the American public. Without real consequences, agencies have been allowed to let requests languish for over a decade, maintain faulty FOIA tracking systems, and at times simply be unresponsive and unhelpful to legitimate requests for information. The Archive's primary recommendations include:

Recommendation 1: Government agencies should consider FOIA processing as central to their mission and as a duty to the American democracy. FOIA program functioning should be considered a factor in personnel performance reviews in order to compel government agencies to recognize the FOIA's importance to the functioning of the agency and the U.S. government.

Background: There is a Need for High-Level Endorsement of the FOIA and Recognition of FOIA Programs in Personnel Performance Reviews – Currently, too many agencies consider the FOIA a distraction from their missions and underfund or even marginalize the work of their FOIA personnel. The Executive Order begins to address this issue by making top agency officials responsible for FOIA performance. However, those senior agency officials need to recognize the importance of the Freedom of Information Act and endorse comprehensive and efficient FOIA processing by their agencies. Adopting Senators Cornyn and Leahy's amendment to the FOIA proposed in the drafted February 2005 Open the Government Act, which "requires the Office of Personnel Management to examine how FOIA can be better implemented at the agency level, including an assessment of whether FOIA

National Security Archive © 2005

performance should be considered as a factor in personnel performance reviews, whether a job classification series specific to FOIA and the Privacy Act should be considered, and whether FOIA awareness training should be provided to federal employees," would emphasize the importance of the FOIA within agencies.

Recommendation 2: The new Agency Chief FOIA Officer should implement a comprehensive FOIA tracking system and insist that agency FOIA personnel be vigilant about tracking and systematically processing all FOIA requests.

Background: The Quality of Handling, Tracking and Monitoring FOIA Requests Varies Immensely – Over 17% of agencies included in this Audit reported they never received the original April 2005 FOIA request, although the Archive had confirmed that the request was sent to the right e-mail address or fax number, and contained the correct information necessary for processing. This indicates that as many as one in six FOIA requests is never properly received and processed by agencies. Additionally, some requests were processed in two days, while others remain pending over 200 days later. This discrepancy in response times illustrates how disparate the quality of FOIA service can be for requesters.

Recommendation 3: Congress should require agencies to report average processing times and provide a date range from the oldest pending request to youngest, in addition to median processing statistics in order to provide a more representative picture of agency backlogs for Congress and the public.

Background: The Annual FOIA Reports Mask the Seriousness of the FOIA Backlogs – Because the annual reports only require agencies to provide the median age of their pending requests, their oldest requests are masked by numerous newly-received requests. The Archive found that the ten oldest FOIA requests were often far older than would be imagined from the reported agency statistic for "Median Days To Process." Furthermore, FOIA officers are trained to process as many requests as possible as fast as possible. Complex requests, which may contain valuable information, can be pushed aside for years.

Recommendation 4: The current FOIA monitoring systems set up by Congress and most agencies emphasize quantity over quality. FOIA offices are not rewarded or recognized for processing time-intensive requests. Agencies should be recognized for processing complex requests, not rewarded for putting difficult requests aside indefinitely. Congress should assign penalties for extraordinary processing delays.

Background: Agencies Are Rewarded for Quantity, Not Quality – FOIA officers are trained to process as many requests as possible, as quickly as possible. Although the Archive supports multi-track processing in which simple requests can be processed ahead of complex ones, agencies have been allowed to exploit

National Security Archive © 2005

the system and can indefinitely delay processing certain complex requests for five, ten or more than fifteen years.

Recommendation 5: Spending on Freedom of Information Act programs at federal agencies should be directly tied to budgets for public affairs offices and spending on public relations campaigns. Agencies spend significantly more money marketing their own messages than they invest in processing public requests for information regarding the activities of the agency. Congress needs to mandate that a sizable percentage of the public affairs budget (30-40%) be spent on FOIA programs. It is clear from this Audit that current public demand for information is exceeding processing capacity.

Background: Most Agency FOIA Programs Lack the Resources to Response in a Timely Manner to Requests – It is clear that many agency FOIA programs are not adequately funded. The data collected in this Audit illustrates how these agencies are unable to process their oldest pending requests, in some cases even after nearly two decades has passed. The public need for information from these agencies exceeds their processing capabilities. On the other hand, government Public Affairs Offices and public relations campaigns are well-funded and fully supported by the agency to publicly disseminate official agency information.

Exact government expenditures on public affairs activities are unavailable because agencies do not traditionally calculate the total costs of these programs in annual budgets.[1] In 2005, the Congressional Research Service roughly estimated the government's annual spending on advertising, "a subset of public relations and communications," at over $1 billion. A recent study conducted by the United States Government Accountability Office (GAO) found that seven federal agencies[2] collectively spent more than $1.6 billion on contracts with public relations firms, advertising agencies and other media entities over two and a half years between 2003 and 2005.[3] This figure only estimates what a few agencies have spend on outside media contracts and does not include internal agency expenditures on public affairs and media activities. On the other hand, the entire federal government spends between $300-400 million annually processing Freedom of Information Act requests.[4] The total government expenditure on the FOIA for the past two and a half years is less than what seven agencies spent on contracts to public relations firms distributing official government information and improving agency images.

[1] Kevin P. Kosar, "Public Relations and Propaganda: Restrictions on Executive Agency Activities," Congressional Research Service, RL32750 (Updated March 21, 2005)
[2] GAO surveyed the Departments of Commerce, Defense, Health and Human Services, Homeland Security, Interior, Treasury, and Veteran's Affairs.
[3] "Media Contracts – Activities and Financial Obligations for Seven Federal Departments," United States Government Accountability Office, GAO-06-305 (January 2006)
[4] See "Summary of Annual FOIA Reports for Fiscal Year 2003," U.S. Department of Justice Office of Information and Privacy (July 29, 2004). Available at http://www.usdoj.gov/oip/foiapost/2004foiapost22.htm and "Summary of Annual FOIA Reports for Fiscal Year 2002," U.S. Department of Justice Office of Information and Privacy (September 3, 2003). Available at http://www.usdoj.gov/oip/foiapost/2003foiapost31.htm

National Security Archive © 2005

Mr. SHAYS. Dr. Nelson.

STATEMENT OF ANNA K. NELSON

Dr. NELSON. I think I represent those kind of independent historians, academic historians who don't have the resources of the National Security Archives and rather depend upon them to come up, because all we have is what we can find and what we do research about and we do not ever go to court because we don't have those funds. We really are very dependent upon the system.

I was very interested in reading the conclusion of the GAO report, the first sentence. It begins with a statement that the lack of clear policies, effective training and oversight can lead to either over- or under-protection of sensitive but not classified information. As I read it, I thought, this is a statement that could apply to problems associated with classified information. Certainly, the recent removal, this reclassification that we have been talking about, is illustrative of this point.

Because of these questions, I am afraid I have to return you, Mr. Chairman, to the issue of reclassification because I am a historian, a historian of American foreign relations. I would like to bring up just two or three, maybe four, points.

The first point I would like to make is that those people who protect national security documents invariably overreact to current events, even though the records they protect are 25, 30, maybe 50 years old. That is the case of Wen Ho Lee, whom Mr. Kucinich mentioned and others have mentioned. When he was accused of passing information in 1998 and 1999, did an extensive investigation that Mr. Blanton just mentioned occurred under the Lott Act. It took an enormous amount of time. It meant no other documents were being released. And you have to bear in mind that these documents were once carefully examined by Energy officials before being sent to open shelves in the National Archives.

I know that the impression was left that other agencies let these documents go, but for those of us who wait for information with equities while they go to three or four different agencies, including the CIA and the Department of Energy, I am rather suspicious of that. I think that in every instance, Energy people did see these documents, but to them before the Wen Ho Lee case, they did not present a security leak.

The same thing happened after the September 11th events. We started this reexamination that has been the topic here of all those thousands of pages of cold war era documents. They hold information about a Soviet Union no longer in existence, countries in the Soviet orbit that are now in NATO, policies long abandoned. But the media began to talk about a great many issues and the reexamination was, in fact, a result of current concerns. What this is doing, of course, is reading history backward.

There is a vast difference between leaks, between the release of yesterday's confidential discussions, and 25 or 30-year-old memorandums, and this kind of confusion that persists persists to the detriment of the public and the Nation's history.

Second, I would like to point out that there is a lack of consistency. This goes with the fact that there aren't clear policies. This lack of consistency comes because every single President can

amend the Executive order on security classification, and for the most part, they do. In this instance, President Bush only put in amendments to the Clinton administration, but several of those amendments did change the thrust of the Executive order.

The agency guidelines also vary, and again, sometimes because current events intercede. One of the examples that has been pointed out, I think by you, Mr. Chairman, was the issue of that famous document where the Chinese came into the Korean War but the President was told, indeed, the Chinese were not out there. Of course, General MacArthur told him that. But the CIA had published two documents in a volume in 1994, a volume called "The CIA Under Harry Truman," which contains that very information, and many of us have been using it in the classroom ever since.

Sometime between 1999 and 2006, the agency reclassified these documents and the reason for this, of course, is a mystery. Why? Is it necessary for purposes of national security to close a 1951 document because of current policy issues with North Korea? Is it necessary to close it because the CIA doesn't want to admit old intelligence failures given the new ones that have cropped up? In fact, the document may have been reclassified simply because those examining the documents did not know of the previous release, which is even worse.

But the questions I have asked, those questions I have asked above, indicate a third problem with seemingly irrational declassification. They breed notions of cover-up and conspiracy. They further erode confidence in government information.

Fourth, those of us who use national security records at the National Archives know that whereas the government distinguishes between confidential, "Secret," and "Top Secret," the declassifiers generally do not. They certainly treat all records that were originally classified secret and top secret the same, and they often include those marked "Confidential" among those withdrawn with "Secret" and "Top Secret." We have all seen that. An unanswered question in the GAO report relates to this problem. Tom mentioned it. How long will the "Sensitive But Unclassified" records be sensitive and unclassified? The "Official Use Only" records, are they ultimately going to be placed on the same footing as classified records?

Without a clear answer, the Federal Government will be establishing a new category of records headed for 20 or 30 years' stay in the security vaults at a great cost to the American taxpayer. The records under these categories should be clearly marked for opening within a short period of time. They should be given a very short residence within the security rolls.

As Tom mentioned, from 1994 to 1998, I was one of five members of the Kennedy Assassination Records Review Board. We all had "Top Secret" clearances and examined classified records in their original form. Records we reviewed were over 30 years old. In the course of these 4 years, we released countless documents that had been closed by the CIA, much to their concern, including documents that discussed intelligence methods. We protected some names, if people were dead, and we agreed to protect certain symbols and technical information. However, we sent thousands of pages of CIA, FBI, and even NSA records to the open shelves of

the National Archives. To my knowledge, no foreign government protested, no one was killed, and the intelligence agencies are still intact. Old records, with few clear exceptions, do not threaten our national security.

Thank you, Mr. Chairman.

Mr. SHAYS. Thank you very much, Dr. Nelson.

[The prepared statement of Dr. Nelson follows:]

TESTIMONY OF ANNA K. NELSON

MARCH 14, 2006

Subcommittee on National Security, Emerging Threats and International Relations

Committee on Government Reform

The conclusion of the GAO report, *Managing Sensitive Information,* begins with the statement that the lack of clear policies, effective training, and oversight can lead to either over or under protection of sensitive but not classified information. This statement could also apply to problems associated with classified information. Certainly the recent removal, in effect re-classification, of documents that had long been open to the public indicates that those working with the documents had no effective training, just as the agencies who employed them did not have clear policies or useful oversight, given the fact that they had previously approved the publication of several of those re-classified records. Because of the questions surrounding this re-classification effort and because I am a historian of American foreign relations, I would like to turn our attention for a few minutes to the problem of classified national security records.

The first point I would like to make is that those protecting national security documents tend to over react to current events, even though the records they protect are 25, 30 or even 50 years old. Thus the case of Wen Ho Lee, who in 1998 and 1999 was accused of passing information to the Chinese, brought an extensive investigation by the Department of Energy of all previously opened historical nuclear energy documents in the National Archives. It took an enormous amount of money and time to go through the 200 million pages that already resided in the National Archives, especially since only 21,514 documents were withdrawn, a percentage almost too low to register. Bear in mind that all of these records had been carefully examined by Energy officials before being sent to open shelves in the National Archives. Before the Wen Ho Lee affair they did not present a security risk.

Similarly, the increasing number of terrorist attacks in the late 1990s as well as the events of 9/11 have led to a re-examination of thousands of pages of documents from the Cold War era. These documents hold information about a Soviet Union no longer in existence, countries in the Soviet orbit that are now in NATO, and policies long abandoned. Before the events highlighted by the media outlets and political leaders, some of these documents were

available in printed collections of government agencies. The re-examination was a clear result of current concerns, not those noted in the documents. There is a vast difference between leaks, release of yesterday's confidential discussions and twenty-five or thirty year old memoranda. Unfortunately, confusion persists to the detriment of our nation's history.

Second, I would like to point out that in the case of classified records the lack of clear policies is largely the result of a lack of consistency. Not only do president's change or amend the rules through new Executive Orders, agency guidelines also vary when current events intercede. In 1994, the CIA did not worry about the release of an embarrassing document that clearly indicated an intelligence failure. At that time, the CIA published a series of documents in a volume entitled, *The CIA under Harry Truman*. One document dated October 13,1950 assured the president that the Chinese would not send troops to Korea, but as we know, the Chinese did just that six days later. Sometime between 1999 and 2006, the agency reclassified two documents that had basically the same information. The reason for this change is a mystery. Is it now necessary, for purposes of national security, to close this 1951 document because of current policy issues with

North Korea, a potential member of the nuclear club? Or is it necessary to close it because the CIA doesn't want to admit old intelligence failures given the new ones that have cropped up?

In fact, the document may have been reclassified simply because those re-examining the documents did not know of the previous release. But the questions I've asked above indicate a third problem with seemingly irrational declassification decisions; they breed notions of cover-up and conspiracy.

Fourth, those of us who use national security records in the National Archives know that whereas the government distinguishes between Confidential, Secret and Top Secret, the declassifiers generally do not. They certainly treat all records that were originally classified Secret and Top Secret the same, and often include those marked Confidential among those withdrawn. An unanswered question in the GAO report relates to this problem. Will the 'Sensitive but Unclassified Records" and those For Official Use Only" be ultimately placed on the same footing as classified records. When is it no longer necessary to protect these records. Without a clear answer, the federal government will be establishing a new category of records headed for a twenty or thirty year stay in the security

vaults at great cost to the American taxpayer. The records under these categories should be clearly marked for opening within a short time period and given a short residence within the security vaults.

From 1994-1998, I was a member of the Kennedy Assassination Records Review Board. We received top secret clearances and examined classified records in their original form. The records we reviewed were over thirty years old. In the course of those four years, we released countless documents that had been closed by the CIA, including those that discussed intelligence methods. We protected names and agreed to protect certain symbols and technical information. However, we sent thousands of pages of CIA, FBI and even NSA records to the open shelves of the National Archives. To my knowledge, no foreign government protested, no one was killed, and the intelligence agencies are still intact. Old records, with a few clear exceptions, do not threaten our national security.

Mr. SHAYS. Mr. Aid.

STATEMENT OF MATTHEW M. AID

Mr. AID. Thank you, Mr. Chairman. I will be brief. I realize we are getting on in the day——

Mr. SHAYS. Don't say you will be brief. No one who has ever said they will be brief has done so. [Laughter.]

When people say they will be brief, it is that they want to be brief, but they won't be. I attended Rosa Parks' funeral, and I am sorry, I am very sensitive about this, it lasted 7 hours. There were 50 speakers and every one of them said they would be brief. [Laughter.]

So do you want to amend your comments?

Mr. AID. Strike it from the record, please. [Laughter.]

Mr. SHAYS. OK. It is not in the record. Welcome, and it is nice to have your testimony. You have the floor.

Mr. AID. Thank you, Mr. Chairman. We Americans are willing to make sacrifices, sometimes at the cost of our civil liberties, to help ensure that nothing like the tragic events of September 11th ever happens again. Even this middle-aged intelligence historian of dubious repute was willing to make some sacrifices because that is what I have sometimes preached in my writings on intelligence issues.

But then a few months ago, as you are now aware, I discovered that elements of the Department of Defense and the U.S. intelligence community were engaged in a secret historical document reclassification program at the National Archives that had its origins back in 1999, and now I find myself in the position where I can't help but wonder what the U.S. Government officials designated to protect us have been doing since September 11th with the American taxpayers' money.

The question foremost in my mind is, has the reclassification by the Pentagon and the CIA of these 55,000 pages of historical documents, all of which are 25 years old or older, made America any safer in the post-September 11th era, and my answer is I tend to doubt it. Could the millions of dollars and tens of thousands of man hours expended to date on this classified program have been better spent elsewhere, especially at a time when many deserving programs in the United States are being cut in order to fund the ongoing conflicts in Iraq and Afghanistan? Again, I firmly believe that the answer is yes.

Were the fiscal and manpower resources that should have been dedicated to declassification, as mandated by Executive Order 12958, hijacked and used instead to reclassify 50-year-old documents that a small minority of U.S. Government security officials didn't want in the public realm, or is this document reclassification program nothing more than a gravy train for out-of-work security personnel, as one Pentagon official has described it to me?

Finally, if we agree that this document reclassification program was a waste of time and taxpayers' money, how do we ensure that it never happens again? I fear that if this program and others like it are allowed to continue unchecked, we will end up revisiting this issue over and over again for the foreseeable future, for who is to say next month or next year which document some agency of the

U.S. Government may choose to take exception to and demand its withdrawal from the public shelves?

I found that the wolves have even started feeding on themselves. I discovered this Friday afternoon that in 2004, the CIA security screeners began withdrawing a significant number of historical documents from their agency's own paper records that were originally declassified by the CIA in 1997 and deposited at the National Archives, and it again appears that they were withdrawn because they contain criticism of how the agency was being run, written by senior CIA officials. Apparently, the CIA security officials who withdrew the documents in 2004 took grave exception to what their colleagues in 1997 had chosen to release to the public.

If this is all true, my question is, where will it all end? Thank you, Mr. Chairman.

Mr. SHAYS. I thank all three of you.

[The prepared statement of Mr. Aid follows:]

PREPARED STATEMENT OF MATTHEW M. AID BEFORE THE HOUSE COMMITTEE ON GOVERNMENT REFORM, SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS AND INTERNATIONAL RELATIONS

Mr. Chairman, I appreciate the opportunity to appear before you today to testify about the recently discovered U.S. government historical document reclassification effort, which has been taking place at the U.S. National Archives since at least 1999, as well as offer some observations based on personal experience concerning the disturbing trend towards greater secrecy within the U.S. government.

THE HISTORICAL DOCUMENTS RECLASSIFICATION PROGRAM

Beginning in June 1999, and continuing unabated for almost seven years, a number of U.S. government agencies, including the Central Intelligence Agency (CIA), the Defense Intelligence Agency (DIA), and the U.S. Air Force, which reportedly acts as the executive agent for the U.S. Department of Defense, have been secretly engaged in a wide-ranging historical document reclassification program at the National Archives and Records Administration (NARA) research facility at College Park, Maryland, as well as at the Presidential Libraries that are also operated by NARA.[1]

Since the reclassification program began, more than 9,500 formerly declassified documents totaling more than 55,500 pages have been withdrawn from the public shelves at College Park and reclassified because, according to the U.S. government agencies, they all had been improperly and/or inadvertently released to the public.[2] Many of the reclassified documents

---

[1] A more detailed examination of the background and history of the multi-agency historical document reclassification program, including examples of documents that have been reclassified, can be found in Matthew M. Aid, ed., Declassification in Reverse: The U.S. Intelligence Community's Secret Historical Document Reclassification Program, posted on February 21, 2006, located at http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB179/

[2] It should be noted, however, that we do not yet have comparable figures for how many documents have been withdrawn from the public shelves at the Presidential Libraries run by NARA.

have either been published in full as part of the State Department's Foreign Relations of the United States series or in the microfiche supplements to these publications, or are available on the CIA Records Search Tool (CREST) computer database of declassified documents at NARA. The government security personnel have also reclassified documents that had been previously sanitized to remove sensitive classified information or had been declassified pursuant to Freedom of Information Act (FOIA) requests by researchers.

Everything about the Pentagon and the CIA's historical document reclassification effort is a secret. To the best of my knowledge, the reclassification program has never been authorized by Congress, nor has any funding ever been appropriated specifically for this program by any congressional committee. Contrast this was the Department of Energy's parallel historical document security review program, which was duly authorized by Congress pursuant to the 1998 Kyl-Lott Amendment (Section 3161 of the National Defense Authorization Act for Fiscal Year 1999, entitled "Protection Against Inadvertent Release of Restricted Data and Formerly Restricted Data"), which was signed into law on October 17, 1998.

I am led to believe that the cloak of secrecy surrounding this reclassification program stems from the essential fact that it does not enjoy Congressional approval, and that the agencies involved have tried to "catch a free ride" on the coattails of the congressionally-approved DOE document review program. This raises serious questions as to the legality of the multi-agency reclassification program, as well as the closely related question of where the agencies involved came up with the millions of dollars required to fund this classified multi-year program.

The very purpose and intent of the multi-agency historical document reclassification program is also classified. There is a classified interagency Memorandum of Understanding (MOU) which: (a) lays out the underlying nature and purpose of the historical document reclassification program, and (b) governs the conduct of the reclassification effort at the National Archives. We understand that NARA is a party and signatory to this classified MOU. The National Security Archive has requested the declassification of this document pursuant to the Freedom of Information Act (FOIA). A copy of this document will be made available to this committee upon completion of the declassification review.

During its lifetime, the multi-agency document reclassification program adopted all of the attributes of a clandestine intelligence community program. Significant efforts were made to keep the program a secret and disguise its activities. According to newspaper reports, over $1.0 million was spent to build a secure office suite for the government security screeners on the fourth floor of the National Archives research facility at College Park, Maryland. How much additional funding was required for the hiring and training of the security screening personnel (most of whom were civilian contractors hired specifically for this program), the purchase of computer equipment and other indirect costs are not known.

The reclassification program even had its own "cover" arrangements. All of the withdrawal sheets placed in the NARA records boxes by the multi-agency security screeners

identified the organization withdrawing the document in question as the Inprocessing and Declassification Branch of the National Archives, and thus relieving the agencies of having to identify who was really reclassifying the documents. Following the tragic events of September 11, 2001, the multi-agency document reclassification program was disguised as part of NARA's "documents of concern" program, with all records boxes designated for security review containing on its exterior a bright yellow label stating: "Records Require Screening According to IG 1600-3." This refers to a NARA directive entitled Interim Guidance 1600-3, "Access to Archival Materials in the Context of Concern About Terrorism," which provided guidance to NARA staff concerning the protection of "Records of Concern" in the Archive's document collections. The latest cover used by the multi-agency security team is that the review is being conducted pursuant to the terms of Executive Order 12958, whose intent, as the Committee is fully aware, was to mandate declassification of historical records rather than serving as legal justification for a government-wide reclassification effort.

But the most serious aspect of the Pentagon and CIA's efforts to disguise the nature and extent of their activities was their success in keeping key aspects about of the program a secret from the Inter-Agency Security Oversight Office (ISOO). Every single document that was pulled from the public shelves at College Park and reclassified was determined to be "inadvertently released," that is to say, that the documents had never been properly declassified in the first place and had been released erroneously. This meant that the agencies conducting the reclassification effort did not have to follow the strict guidelines laid down by E.O. 12958, which requires a formal written reclassification notification to ISOO by the agency head making the decision. The Pentagon and CIA security screeners went around the strictures contained in E.O. 12958 by declaring every document they reclassified as having never been properly declassified in the first place, and therefore they never filed a single reclassification notification with ISOO during the 6+ years of the program! This behavior raises further serious questions in my mind about the legality of the reclassification decisions made by the agencies since the first documents were pulled from the public shelves in 1999.

The multi-agency reclassification teams have been using what can only be described as an "expanded and enhanced" interpretation of the exemptions contained in Executive Order 12958 in order to justify the reclassification decisions that they have made. Virtually all of the historical documents that have been reclassified to date are at least 25 years old or older, and as such, meet the test for immediate declassification pursuant to Executive Order 12958, as amended. Furthermore, not one of the reclassified documents contains any information which could conceivably fall under any one of the exemptions to E.O. 12958. For example, in removing virtually all of the previously declassified documents from the State Department intelligence files at NARA relating to an abortive 1956 balloon reconnaissance program over the Soviet Union called **Genetrix**, the Defense Intelligence Agency (DIA) claimed that the removed documents (including many newspaper reports concerning the program) had been removed pursuant to exemption 25X6, i.e. that they might: "Reveal information, including foreign government information, that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic

activities of the United States." Needless to say, the public embarrassment to the administration of President Dwight D. Eisenhower caused by the very public failure of this reconnaissance program took place thirty years ago, and there is little if any conceivable possibility that the now reclassified State Department documents could cause the U.S. government any further grief beyond the damage already suffered.

And finally, the government security screeners have sought to make it more difficult for researchers to get the reclassified documents opened up in the future through the Freedom of Information Act (FOIA). As little information about the removed document is contained on the withdrawal sheet, usually omitting such information as the originator of the document or the nature of the document. Moreover, all of the document withdrawal sheets placed in the records boxes since 2001 deliberately do not disclose the identity of the government agency reclassifying the document, or the legal rationale for the document's removal.

DROWNING IN A SEA OF SECRECY

Is the above-described multi-agency document reclassification program just the tip of the iceberg? Sadly, I fear that the answer is almost certainly "Yes."

It now seems clear that the multi-agency historical document reclassification program is symptomatic of a larger and more pervasive ailment afflicting the U.S. government. The ailment, put simply, is that declassification has slowly but surely been dying in America since the late 1990s, with the process having accelerated noticeably since 2001. It is no secret that the leaders of the charge against greater openness in government, and the closely related issue of declassification of government records, have been the Department of Defense and the U.S. intelligence community.

The open opposition within the CIA's Clandestine Service to greater transparency and openness in government is reflected in an unclassified article published in 2001 in the CIA's in-house journal Studies in Intelligence, wherein the author, N. Richard Kinsman, a veteran Clandestine Service officer, argued that declassified historical documents that had appeared in the State Department's respected Foreign Relations of the United States (FRUS) series of publication was damaging the CIA's ongoing clandestine operations overseas, and specifically criticized officials in the State Department, the National Security Council, and the Justice Department who in a number of instances had approved the declassification and release of intelligence documents over CIA objections.[3]

Moreover, one could make a very persuasive argument that one of the reasons the U.S. government's declassification effort has ground to a halt is because available manpower and

---

[3] N. Richard Kinsman, "Openness and the Future of the Clandestine Service," Studies in Intelligence, Fall/Winter 2001, No. 10. This unclassified document can be accessed at http://www.cia.gov/csi/kent_csi/docs/v44i5a07p.htm.

budgetary resources appear to have been redirected to the historical document reclassification effort since 2001. The longtime Washington Post reporter and noted intelligence historian Michael Dobbs wrote just a few days ago that: "The routine declassification of government records has ground to a virtual standstill over the past few years because of the diversion of resources to reexamining previously released documents."[4]

---

[4] Michael Dobbs, "Still Secret After All These Years," Washington Post, March 12, 2006, p. B2.

The underlying evidence supporting this contention is compelling. The number of documents declassified by the U.S. government have declined from 126.8 million pages in 1999 to only 28.4 million pages in 2004 (the last date for which official statistics are available), a decline of 88% in just five years. The amount of money spent by the U.S. government on declassification also declined precipitously, dropping from $233.1 million in 1999 to a mere $43.3 million in 2004, a decline of 91.5% in just five years.[5]

The decline of declassification has been most marked at the Central Intelligence Agency (CIA). CIA spokesmen correctly point out that since 1997, the Agency has declassified and released to the public more than 28 million pages of formerly classified documents, with approximately 9.25 million pages of documents accessioned since 2000 to the CIA's CREST database of declassified documents housed in the Library at the National Archives' College Park facility. Unmentioned is the fact that the number of documents that have been added to the CREST database has declined from 2,082,776 pages in 2000 to 693,358 pages in 2005, a decline of 66.8% in relative terms.[6] Moreover, the documents that have been released to the CREST database by the CIA since 2001 contain many more redactions than had been the case prior to 9/11, so much so that a large number of recently released documents in CREST are essentially worthless from a historical perspective.

The CIA has also since at least 2004 been quietly removing whole sets of previously declassified documents from the CREST database for reasons the Agency refuses to disclose. In the past, CIA officials have publicly stated that: "If a CIA document was mistakenly declassified by the CIA, the Agency will stand by that decision." This is, in fact, not exactly true. Between 1997 and 1999, the CIA released approximately 100 pages of formerly classified documents from three of its archival records groups (the CIA refers to its record groups as "Jobs") and placed them along with other declassified CIA records on the CREST computer database. After the author and a number of other researchers printed out materials from these three specific record groups, in 2003 and/or 2004 the CIA hastily withdrew these three Jobs from the CREST database, leaving no mark that they had ever been there. Repeated attempts by the author to get the CIA Declassification Branch to "re-declassify" these three CIA records groups through the

---

5 OpenTheGovernment.org, Secrecy Report Card: An Update, April 5, 2005, located at www.openthegovernment.org/otg/OTG_RC_update.pdf

6 Data from National Archives and Records Administration.

Freedom of Information Act (FOIA) have to date been unsuccessful.[7]

[7] The now missing three CIA records Jobs are: 78S03377A, 78S00977R, and 78S00763R.

And finally, in recent years CIA security officials have removed documents from non-governmental historical repositories because they contained "inadvertently released" classified information. In February 2005, a team of five government security personnel, including three CIA officials, removed at least a dozen documents from the papers of the late Senator Henry M. "Scoop" Jackson that were held at the University of Washington's Allen Library. The documents had allegedly been "inadvertently released" when Senator Jackson papers were deposited at the library ten years earlier.[8]

THE SENSITIVE BUT UNCLASSIFIED CONUNDRUM

Finally, I would like to offer some comments concerning the U.S. government's attempts to keep so-called "Sensitive but Unclassified" (SBU) information out of the hands of the public.

First, from personal experience it would seem that much of the unclassified material that the U.S. government, especially the Pentagon, is currently trying to protect by cloaking them with the SBU marking is, for the most part, insignificant and harmless from a security standpoint. For example, the Pentagon has gone to great lengths to deny FOIA requests from members of the public for documents such as organization charts, staff directories, and telephone books. The Pentagon and the intelligence community argue that hostile foreign intelligence organizations mine these publications for information that could potentially damage U.S. national security.

It should be noted that at the height of the Cold War with the Soviet Union, all of these documents remained freely available to the public (and Soviet intelligence) with no discernible harm to national security. And while the Pentagon now routinely denies FOIA requests for these types of information, the Defense Department and virtually every other department and agency of the U.S. government currently make this material available to a number of commercial publishers, who in turn make the information available to the public through a variety of unclassified publications, albeit at considerable cost.[9]

---

[8] Lara Bain, "CIA Seizes Sen. Jackson Papers," Everett Daily Herald, February 15, 2005.

[9] See for example the detailed organizational and personnel information for virtually every U.S. government agency that are contained in publications such as the Federal Executive Directory put out by the Carroll Publishing Co. in Washington, D.C., or the Federal

Second, the Defense Department and the military services have arbitrarily removed from public circulation unclassified information which could not cause any conceivable harm to U.S. national security. For example, in 2003 the U.S. Army's Center for Army Lessons Learned (CALL) at Fort Leavenworth, Kansas withdrew from public access all of its unclassified Lessons Learned reports concerning the conduct of operations in Afghanistan and Iraq after a series of critical newspaper reports were published using these materials.[10]

Third, the efforts of the Pentagon and the rest of the U.S. national security establishment to keep SBU information from the public, no matter how diligent, are bucking up against the inexorable tide of information proliferation that is now publicly available on the internet and other electronic media. Today, one can easily find on the internet reams of sensitive information concerning subjects ranging from nuclear, chemical and biological weapons design information, layouts of sensitive U.S. government military and intelligence facilities, "cookbooks" on how to make plastique high explosives, etc. The committee will no doubt understand if I do not provide any further details concerning where these types of information may be found.

Fourth, and finally, I believe that the imposition of a cloak of secrecy over such a broad range of formerly unclassified materials is ultimately wasteful, and can only serve to impede the conduct of day-to-day business inside the U.S. government. For example, the removal of unclassified documents and related indices from public access at the Nuclear Regulatory Commission (NRC) and the Federal Communications Commission in 2004 has only resulted in further slowing down the regulatory activities of these agencies by barring essential information from the companies and individuals who need the information in order to perform their business functions.

Thank you.

Yellow Book, published by Leadership Directories, Inc.

[10] Fred Kaplan, "The Army Buries Its Mistakes," Slate, October 31, 2003, http://www.slate.com/id/2090585/

Mr. SHAYS. You were actually very brief.

Mr. AID. Thank you.

Mr. SHAYS. I won't be able to say that no one who says that is ever brief, so I resent that deeply. [Laughter.]

I am going to have counsel start off.

Mr. HALLORAN. Thank you, Mr. Chairman.

Mr. Aid, what made you go back and look? I mean, my understanding was you were looking for documents, looking in places where documents you had previously accessed and found them not there. What made you go back for a second peek?

Mr. AID. You should understand, sir, that I am not a professional historian in the sense that, unlike Dr. Nelson and Mr. Blanton, I am a 20-year businessman who dabbles in history as a passion. I find that as I get older, I make more mistakes which requires that I go back and back and back to the same records to see things which, if I was 20 years younger, I would have spotted the first time around.

One of the problems with being an intelligence historian is that there is no basis, there is no foundation upon which I, as a historian, can revert back to, because I write about the National Security Agency. Outside of one or two books and a smattering of articles, there is nothing for me to refer back to. So I find that what I am writing is a jigsaw puzzle. I have to go back to the records constantly, because the first time I went through them 10 years ago or 20 years ago, I guarantee you I didn't understand the import of what I was looking at at the time. That is why I went back in the fall of this year to reexamine some of those same State Department records which I looked at back in 1996.

Mr. HALLORAN. In the course of your research, and this goes for all of you, in the course of your research in the Archives, had you run across withdrawn items before, a reference to somebody had pulled this for some classification reason?

Mr. AID. If you live and work at the National Archives, you live with withdrawal slips, many of which date back to when the documents were first released to the public. The first instance I ran into suggesting that something untoward was taking place in the post-September 11th era, meaning recent withdrawals, came in 2004, I believe it is, when I noticed that a number of records that I had already printed out from the CIA's data base of declassified documents had disappeared from the computer data base.

Now, the problem with digital records is there is no place where you can put a withdrawal slip and say, oh, sorry, the CIA has decided that these records were inadvertently released and deserved to be classified. Being a native New Yorker, I went and complained loudly and longly and here I am 3 years later and I still haven't gotten the records, much less the CIA willing to admit that the records once existed.

Dr. NELSON. We all have run into withdrawal slips. We run into them all the time. The most records that have been reviewed have been the Nixon papers, Kissinger and Nixon, and I had one occasion when I had at least six or eight boxes on a cart from the National Archives and not a single document, nothing but withdrawal sheets.

There is also a change in the character of those sheets. They used to be much more explicit. "So-and-so" sent a memo on a certain date. No. Now they don't say that, for the most part. I understand the Archives is going to try to go back to that, because the view was we wouldn't ask for FOIA if we didn't know. But, in fact, we ask for more FOIA because we don't know. I mean, it may be a date we don't want, but we will ask for it because we don't know.

Mr. HALLORAN. While I have you, I can't resist the opportunity to ask if you would help inform our consensus on the extent of over-classification. Having reviewed the Kennedy assassination documents, how much never should have been classified at all of what you saw?

Dr. NELSON. Well, we had a board of five people and I was the only one who had ever used FOIA. They were eminent historians and an archivist and a very good lawyer, who is now a Federal judge. But here you had five civilians in a very unusual situation of being able to declassify and we all agreed each time. We never disagreed over what should be hidden because most of it did not make sense at all. It was just absurd. Occasionally, we would black out three little letters at the top of a piece of paper——

Mr. HALLORAN. But as to the initial decision to classify, initially, back when——

Dr. NELSON. They should never have been classified.

Mr. HALLORAN. At all?

Dr. NELSON. But——

Mr. HALLORAN. Eighty percent of what you saw? Fifty percent? I mean——

Dr. NELSON. Oh, I would say 80 percent of what we saw, and I think the important thing is that they are now open. I might add that I understand that the reclassifiers did go to that collection and ask to look at it and they were told that collection was there under congressional statute, which is what created the board, and they would not let them in.

Mr. HALLORAN. Mr. Blanton, are you familiar with the argument that was made with regard to this reclassification operation that there were certain notifications or processes not followed because this wasn't a reclassification, this was, in effect, an un-declassification? We have to follow that. Is that your understanding of what was happening there?

Mr. BLANTON. That, frankly, and I guess we should abolish the use of the word "frankly" in congressional hearings as well as the "I will be brief," right? [Laughter.]

Isn't that the most overused single word probably in all testimony?

Mr. SHAYS. But at least it is more accurate.

Mr. BLANTON. It is an excuse the agencies are giving to get around a requirement that is somewhat onerous, and deliberately so, in the Executive order, because to reclassify something, you actually have to go get Bill Leonard's and the Information Security Oversight Office's approval. It gets checked out. There are big countervailing forces, checks and balances. There is none if what you can say, oh, this was an inadvertent release and so it is not really declassified, even if, as in the case of the balloon document, it is published in a book in 1,000 libraries and on the World Wide

Web and you can search for it and find it and read it to your kids so they will be in unauthorized possession of classified information.

It is an excuse. It is a semantic game. Unfortunately, they have some good lawyers and they like to play those semantic games and they are trying to get around ISOO's oversight. I think that is really the bottom line.

Mr. HALLORAN. On the SBU side, Mr. Leonard in his testimony made an argument, as did some others, as did you, on the need to try to standardize these SBU formats and regulations. Give us a sense from your studies today how difficult that would be. How wide a range is there? I mean, some have no regulations. Some have very detailed ones. How difficult in terms of individual agency equities and even statutory lanes they travel in would it be to craft—or are there enough common elements that it would not be overwhelmingly difficult to standardize SBU processes and rules?

Mr. BLANTON. I suspect that there are some common elements that are just plain common sense. Why can't the sensitive unclassified area have the same prohibitions that the classified area has on covering up criminality, malfeasance, embarrassment? That is just common sense. I would bet that a statute that the Congress came up with would be hard to argue against that, although people would drag their feet.

There are some common elements like that. The ideas of duration—that was one of the big reforms in the 1990's in the classification system, the idea that at the point of classification, you have to put a sunset on the thing or it is going to live forever. There will be new mountains of FOUO and OUO documents down the road.

So I think there are a number of common elements. I think Bill Leonard has recommended some of them. We have put a few in our specific study where we think these are common sense matters that shouldn't be objectionable because they already apply in the classification world.

Now, I have to caution you, they will not solve the problem. Common sense is not going to solve the problem. We have massive overclassification in the classification world even with all these common sense checks and balances and a full-time audit agency and Federal judges that look at it and OMB that is reporting the cost figures and so forth, and ISCAP [ph.], which is a very useful appeals panel, that kind of challenge structure, an interagency challenge structure that pushes back against some of these kind of classifications. You need all those things, but you probably need something more.

Mr. HALLORAN. Thank you.

Mr. SHAYS. If you had been in my position, what would you have asked the witnesses that preceded you? Let me start with you, Mr. Aid. Who would you have asked, and what would you have asked?

Mr. AID. Where to begin. Actually, I thought, Mr. Chairman, you and the other members of the subcommittee did a very good job of probing the most important aspects of the reclassification program, which is why is this thing a secret?

One of the questions I would have asked is you had the representatives of the Department of Energy and the Department of Defense sitting right where I am today. Why is it that the Department of Energy can issue an annual report giving full details about

its document reclassification efforts, the number of documents that it has removed, the types of information that it has found, and basically give you, the Members of Congress who fund the Department of Energy, and us, the members of the public, some reassurance that what they are doing is reasonable and competent and that they actually are protecting U.S. national security?

What disturbs me about this unnamed component of the Department of Defense Memorandum of Understanding and the separate CIA effort is that it is all done in secrecy. It is all done in the dead of night. There is no accountability. The fact is that——

Mr. SHAYS. So what would you have asked them?

Mr. AID. I would have asked them, why was it done in secrecy? Why, if the program is legitimate, as they claim, I mean, if they say that the Executive order allows agencies to withdraw material because they own the classification on the paper, then why do you have to keep it a secret? I mean, at its most basic level, there is something—I guess in the legal profession you would call it the smell test. Does the way the agencies, the way they behave, does it rise to the level of sounding fishy, or does it seem perfectly rational, even in the post-September 11th world we live in?

Mr. SHAYS. What would you have asked, Dr. Nelson?

Dr. NELSON. Well, I think I would have turned my attention perhaps to the Archivist. I think that it is clear he was not there when this started. He has only been there about a year. But I think that one of the things I would have asked him is what the Archives can do about getting a little more authority and about standing up to certain agencies, and also perhaps reaching out to Congress to help them do that.

Mr. SHAYS. That would have been a great question, I agree. Do you think that they need more authority, or do you believe they have inherent authority they are not exercising?

Dr. NELSON. Well, I think that in the case of general Federal records, they may not be using all they have, but I think in security classified, I think "Sensitive But Unclassified" and "For Official Use" and that sort of thing, I think they probably need more authority because they don't have very much power and they are not trusted, and yet they are the most trustworthy people in the world——

Mr. SHAYS. Not trusted by whom?

Dr. NELSON. Not trusted by the agencies, and yet they are so trustworthy that when the agencies asked the archivists who work in the Archives not to talk about this reclassification business, they didn't. Otherwise, we would have known about it much earlier.

Mr. AID. Right. I can confirm that. This is actually one of the few agencies I have run into in my experience that actually knows how to keep a secret.

Dr. NELSON. They have to.

Mr. BLANTON. They have a lot of them.

Dr. NELSON. They have a lot of secrets, you know. They have all kinds of Watergate secrets. They have all kinds of Clinton——

Mr. SHAYS. I see the smile on your face like—I was thinking, Mr. Aid, that I was going to ask you, is it kind of like mining for gold? When you go in there, you are looking for something that is—you said this is your avocation instead of your vocation and you said

you loved history. I am a history major in college, and your face lights up with the joy of it, and I am seeing you, Dr. Nelson, all of a sudden describe there is Watergate and there is this and it is almost like, my gosh, is this like the best-kept secret? I mean, should we all be going in to look at these documents? [Laughter.]

Dr. NELSON. Well, we can't look at any of those documents because they are still in the vault, but yes, I think for those of us who do this kind of work and feel it is worthwhile and many of us take it into the classrooms——

Mr. SHAYS. Right.

Dr. NELSON. And it sinks down to the public through textbooks ultimately. I think we do think that it is important, but we also obviously——

Mr. SHAYS. So when you look at a document that is particularly significant, maybe changes people's view of what happened in the past, then that is an opportunity for you to publicize it and share it with others and——

Dr. NELSON. It is very rare that one document, of course, will do it, and that is why historians spend so much time at the National Archives and in Presidential libraries to do American history. But, in fact, I think you are right in that we do see documents that do change our views. I will give you an example. People write memoirs. Government officials write memoirs. It is very interesting to see the documents when they come out. The memoirs are wrong. We have perhaps been teaching out of those memoirs, or the American people have believed certain things out of the memoirs. When you get right down to it, the memoirs might be a lie. There might be lies within them because the documents——

Mr. SHAYS. And you determine that by the information you have seen at the Archives?

Dr. NELSON. In the documents.

Mr. SHAYS. Yes. Mr. Blanton, what would you have asked?

Mr. BLANTON. I would just say one caveat. The documents lie, too.

Dr. NELSON. Oh, yes.

Mr. BLANTON. They only have one real virtue, which is they are frozen in time——

Dr. NELSON. That is right.

Mr. BLANTON [continuing]. Unlike memory and memoirs and so forth, and therefore——

Mr. SHAYS. Give me an example of——

Mr. BLANTON [continuing]. I think it is a cross-check.

Dr. NELSON. Only the transcripts of telephone conversations really don't lie.

Mr. BLANTON. Well, I mean, you are missing that tone, but I would say the two questions—[laughter]—the two questions, Mr. Chairman, the two questions I would have asked, I think one is a question to Mr. Leonard and Mr. Weinstein, which is if the agencies don't join in and don't agree in their National Declassification Initiative, what are they going to do now? They might need you to come to their rescue. This is this idea——

Mr. SHAYS. Give me an example of what you mean.

Mr. BLANTON. What they are trying to do——

Mr. SHAYS. When you say "agencies," give me these agencies you would be describing.

Mr. BLANTON. They called a summit of the intelligence agencies. They named a couple of them and they didn't name the other ones. They didn't name the Department of Defense component that has the secret memoranda that we are all after.

Mr. SHAYS. Right.

Mr. BLANTON. But they called a summit of these folks last week, and what was interesting, the release the National Archives put out after the summit had a wonderful clarion call for cleaning up this program in the top half of the document, including a call for a National Declassification Initiative, which would, like the Nazi War Crimes Interagency Working Group, like the Kennedy Assassination Records Board, like what was done for Congress on the Iran-Contra investigation, put the agencies all at the table, all at the National Archives with the Information Security Oversight Office looking over their shoulder, holding their feet to the fire, making a real classification effort happen without this daisy chain of referrals and I get it next.

Well, they brought the people to the summit. They issued this clarion call. But I noticed that the clarion call only really had Mr. Leonard and Mr. Weinstein's name on it and that the agencies were below the fold, in newspaper parlance, you would say, after the call for a declassification initiative. Then you see, and the agencies all agreed there was a problem and agreed to work with us to help solve it. But they are not signing on. So what do you do next if they don't agree?

On SBU, the sensitive unclassified, I think the question I would have asked to Mr. Rogalski of the Department of Defense, you have, what did he say, 2.5 million people who can slap "For Official Use Only" onto records? What is stopping him from cutting that number? I mean, I think the Department of Defense only has 2,000-and-something people who are authorized as original classifiers in the classification system. Would that help or would that not?

Mr. SHAYS. I would have loved to have asked that question. I would love to know his answer.

Mr. BLANTON. I don't know. I encourage you to send him a letter. [Laughter.]

Mr. SHAYS. That would have been a great question.

Mr. BLANTON. It will take him about 6 months to answer my letter. He will do it quicker to you.

Mr. SHAYS. What would you like to put on the record that is not on the record right now?

Dr. NELSON. I would like to put on the record something about equities.

Mr. SHAYS. Move the mic a little closer, Dr. Nelson.

Dr. NELSON. I would like to put something on the record about equities. Equities are the devil behind the words that everyone else is talking about, because the reason these intelligence agencies, the Department of Defense and such, have gone in is because they are protecting what they call their equities. In fact, most of the records that were closed were State Department records and State was not there. Equity is the devil of all of us who look for information.

I have a request that has been there in the National Archives for at least a year and a half, maybe two, and I was just told that it had been sent out to three agencies and they hadn't heard from it. Equities are the problem, and therefore, I agree with Tom Blanton. You have to have some kind of an initiative to bring these agencies together so that everything on the subject is declassified without going through this whole business. It is the worst part of the system. It allows them to come back and reclassify and it keeps the rest of us waiting years for old, old documents.

Mr. SHAYS. Anyone else? Any other comment from either of you?

I am grateful that you all are doing what you are doing. You are doing very important work. What I also like is you came to enjoy it and you have a sense of humor, which I also appreciate. I guess you have to have a sense of humor in this business, don't we.

Mr. BLANTON. Amen.

Mr. SHAYS. So thank you all very much, and with that, we will adjourn this hearing.

[Whereupon, at 4:55 p.m., the subcommittee was adjourned.]

[The prepared statement of Hon. Todd Russell Platts and additional information submitted for the hearing record follows:]

COMMITTEE ON GOVERNMENT REFORM

OVERSIGHT HEARING:

Subcommittee on National Security, Emerging Threats, and International Relations

Drowning in a Sea of Faux Secrets: Policies on Handling of Classified and Sensitive Information

Tuesday, March 14, 2006, 2:00 PM

STATEMENT OF REPRESENTATIVE TODD RUSSELL PLATTS

Thank you, Chairman Shays, for holding this important hearing today regarding the Federal government's policies on the handling of classified and sensitive information. As Chairman of the Government Reform Subcommittee of Management, Finance, and Accountability, which has some jurisdiction on government information policy, I share your interest in this important topic.

In 1995, then-President Bill Clinton signed an Executive Order directing the National Archives to declassify en masse all documents more than 25 years old, with exemptions for certain sensitive documents that might disclose national security or other currently relevant classified information. In response to the order, the National Archives has declassified nearly 1.4 billion pages of previously classified documents.

Recently, we have learned that beginning in 1999, the CIA along with other agencies have reclassified and removed from the shelves of the National Archives more than 9,500 documents (55,000 pages) for national security reasons. Many of these documents have been photocopied by researchers, written about in scholarly publications, distributed to libraries around the country, and in some cases, even posted on federal agency web sites. These documents all went through a labor-intensive process and a strict review prior to being declassified.

Earlier this month, the National Archives imposed a moratorium on reclassification of previously declassified documents and hosted a summit with agency officials to discuss this reclassification effort. I applaud the Archivist for this approach and the interested agencies for their participation.

This is a vitally important issue. In a free society we must maintain a balance between the need to protect national security information, while at the same time ensuring public access to key historical documents. Thank you again Chairman Shays for holding this important hearing today.

OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

INTELLIGENCE

APR 10 2006

The Honorable Christopher Shays
Chairman
Subcommittee on National Security,
Emerging Threats, and International Relations
Committee on Government Reform
United States House of Representatives
Washington, DC 20515-6143

Dear Mr. Chairman:

Thank you for the opportunity to testify before your subcommittee on National Security, Emerging Threats, and International Relations. I am enclosing my responses to questions asked during the hearing on March 14, 2006, entitled "Drowning in a Sea of Faux Secrets: Policies on Handling of Classified and Sensitive Information," as well as additional information requested on the decrease in original classification activity by the Department of Defense. I would like to correct one statement in my oral testimony. In lines 893-895 of the hearing testimony where I said that the Department of Defense had reduced original classification decisions approximately 33 percent, it should read 29 percent.

I request that this correspondence be made a part of the record. If there are any further questions, please do not hesitate to contact me or have a member of your staff contact Ms. Chris Bromwell at (703) 697-1988.

Sincerely,

Robert W. Rogalski ACTING
Deputy Under Secretary of Defense
(Counterintelligence and Security)

Enclosures:
As stated

cc: The Honorable Dennis Kucinich
Ranking Member

Questions for the Record

House Committee on Government Reform
Subcommittee on National Security, Emerging Threats,
and International Relations
Hearing on: Policies on Handling of Classified and Sensitive Information
March 14, 2006

Question: In a March 15, 2006, letter to Acting Deputy Under Secretary of Defense Rogalski, the Subcommittee requested a classified and unclassified copy of the memorandum of agreement (MOA) between the National Archives and Records Administration (NARA) and a Department of Defense agency. In addition, the Subcommittee requested a classified briefing regarding the purpose and content of the MOA.

Answer: A copy of the classified MOA was provided to Chairman Shays on March 24, 2006, by the Office of the Assistant Secretary of Defense for Legislative Affairs. The briefing on the MOA is currently scheduled for April 11. A redacted version of the MOA will be provided to the Subcommittee no later than April 11,2006.

Question: In lines 1589-1592 of the hearing transcript, Acting Deputy Under Secretary of Defense Rogalski said he would take a question posed by Representative Maloney on a specific DCAA audit as a QFR.

Answer: As of September 27, 2005, DCAA has provided the House Committee on Government Reform over 100 complete audit reports (with nothing sanitized) related to Iraq Reconstruction contracts. Included in these audit reports were audits issued on Halliburton – Kellogg, Brown and Root's (KBR) LOGCAP contract and Restore Iraqi Oil contract. DCAA worked with the responsible contracting officials to obtain the necessary release determinations. All of these audit reports were provided to Mr. John Brosnan, Counsel for the Committee on Government Reform. The sanitized version referred to by Representative Maloney was jointly sanitized by Army Corps of Engineer and Halliburton lawyers before release to the United Nations (UN) to ensure that information related to the Trade Act and competition was not disclosed. Normally, when DoD denies or sanitizes documents, the DoD response indicates to whom the recipient may appeal the decision. That indication was inadvertently left out of the response to the UN.

The FOIA appeal process is set forth in the Freedom of Information Act, and DoD policy for the processing of FOIA appeals is contained within DoD 5400.7-R, "DoD Freedom of Information Act Program." Upon receiving an initial response, FOIA requesters have 60 calendar days from the date of the initial denial letter to make a FOIA appeal. Requesters may appeal any determination that they consider to be adverse in nature, to include fee status designations, denials of expedited processing, as well as withholding of information using the established FOIA exemptions. Requesters may also appeal a functional denial of their request if the government agency has not responded within the statutory 20 working day time limit. Once an appeal is received, the government agency has another statutory 20 working days to review the denial and come to an appellate determination. FOIA appeal determinations are made by designated appellate authorities, who, within the DoD, are designated senior officials who were not part of the initial FOIA process to ensure that requesters receive an independent review of the their appeals. Letters to requesters tell them to whom to send the appeal.

Question: In lines 2002-2006 of the hearing transcript, Acting Deputy Under Secretary of Defense Rogalski said he would take a question posed by Chairman Shays and Lawrence Halloran (counsel to the Subcommittee) on the basis of DoD's objections to a GAO recommendation as a QFR.

Answer: The problems that DoD would face if FOIA exemptions were designated on an FOUO document are more functional and practical in nature than they are legal. Freedom of Information Act (FOIA) exemptions are not invoked to deny release until the information in question has been thoroughly reviewed in response to a specific request under the FOIA. Review for applicability of FOIA exemptions is initiated only when a FOIA request has been received. If the information in question has been determined to be responsive to a FOIA request, applicable FOIA exemptions may be used to withhold material. The applicability of FOIA exemptions may change over time, and because of this, it would be almost impossible to determine at the time a document is created whether an exemption would apply to protect the information in the future. To designate a FOIA exemption for FOUO information that has not been requested and reviewed under the provisions of the FOIA risks an inaccurate designation of a FOIA exemption, and would potentially limit releases to the public because DoD personnel may be hesitant to challenge the initial determination of applicable FOIA exemptions. From the practical standpoint, it would require a huge expenditure of resources to train thousands of personnel in the applicability of FOIA exemptions and FOIA law. Additionally, a front-line FOIA review to determine applicable exemptions, in addition to being less than effective for the reasons outlined above, would further delay the work products created by the DoD. We queried the Department of Justice (DOJ) on this issue and were told that they do not put FOIA exemptions on documents when they are created. DOJ has never recommended coupling together FOUO and FOIA exemptions.

Question: In lines 893-895, Acting Deputy Under Secretary of Defense Rogalski gave a percentage of reduced original classification decisions since fiscal year 2004. In a March 23, 2006, letter, the Subcommittee requested an explanation and further details of the statement found on lines 893-895 and requested by number or percent the reduction of original classification decisions for FY 2004, 2005, and 2006 (to date).

Answer: Please see attached spreadsheet.

Comparison of DoD Original Classification Decisions
FY 04 FY 05

Original Classification Decisions				
	FY04	FY05	Δ (#)	Δ (%)
Top Secret	7,000	6,983	-17	-.24
Secret	183,412	129,630	-53,782	-29.32
Confidential	7,942	3,342	-4,600	-57.92
Total	198,354	139,955	**-58,399**	**-29.44**
Derivative Classification Decisions				
	FY04	FY05	Δ (#)	Δ (%)
Top Secret	721,404	454,683	-266,721	-36.97
Secret	2,368,361	2,370,740	+2,379	+.10
Confidential	1,230,381	596,370	-634,011	-51.53
Total	4,320,146	3,421,793	**-898,353**	**-20.79**
Total Original & Derivative Decisions	**4,518,500**	**3,561,748**	**-956,752**	**-21.17**

○