# CLASSIFICATION OF NATIONAL SECURITY INFORMATION

## HEARING

BEFORE THE

## SUBCOMMITTEE ON INTELLIGENCE COMMUNITY MANAGEMENT

OF THE

## PERMANENT SELECT COMMITTEE ON INTELLIGENCE

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

---

Hearing held in Washington, DC, July 12, 2007

Printed for the use of the Committee

---

U.S. GOVERNMENT PRINTING OFFICE

38–190 WASHINGTON : 2007

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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

PERMANENT SELECT COMMITTEE ON INTELLIGENCE

SILVESTRE REYES, Texas, *Chairman*

ALCEE L. HASTINGS, Florida
LEONARD L. BOSWELL, Iowa
ROBERT E. (BUD) CRAMER, Alabama
ANNA G. ESHOO, California
RUSH D. HOLT, New Jersey
C.A. DUTCH RUPPERSBERGER, Maryland
JOHN F. TIERNEY, Massachusetts
MIKE THOMPSON, California
JANICE D. SCHAKOWSKY, Illinois
JAMES R. LANGEVIN, Rhode Island
PATRICK J. MURPHY, Pennsylvania

PETER HOEKSTRA, Michigan
TERRY EVERETT, Alabama
ELTON GALLEGLY, California
HEATHER WILSON, New Mexico
MAC THORNBERRY, Texas
JOHN M. MCHUGH, New York
TODD TIAHRT, Kansas
MIKE ROGERS, Michigan
DARRELL E. ISSA, California

NANCY PELOSI, California, Speaker, *Ex Officio Member*
JOHN A. BOEHNER, Ohio, Minority Leader, *Ex Officio Member*
MICHAEL DELANEY, *Staff Director*

# CLASSIFICATION OF NATIONAL SECURITY INFORMATION

**THURSDAY, JULY 12, 2007**

HOUSE OF REPRESENTATIVES,
PERMANENT SELECT COMMITTEE ON INTELLIGENCE,
SUBCOMMITTEE ON INTELLIGENCE COMMUNITY MANAGEMENT,
*Washington, DC.*

The subcommittee met, pursuant to call, at 1:03 p.m., in room 2216, Rayburn House Office Building, the Hon. Anna G. Eshoo (chairwoman of the subcommittee) presiding.

Present: Representatives Eshoo, Holt, and Issa.

Chairwoman ESHOO. Good afternoon, everyone. My name is Anna Eshoo, and I have the privilege of chairing this small but we think important subcommittee on the management of the intelligence community. So I want to welcome everyone here today; and our distinguished witnesses that are here, they bring so much to the table; and we are very grateful to them for being willing to come and be instructive to us.

I would like to begin by noting how rare it is for the Intelligence Committee and its subcommittees to hold an open hearing. So this is special. I hope that we do more of this. I think it is so important for the American people to have a sense of a committee that is so important in the life of our country and the protection of the citizens.

So while most of our work absolutely has to be done in closed session to protect national security, I know we are going to strive to have more open hearings again so that the American people can see us working.

The subject of today's hearing I think is a rather timely one, but it is something that the members on both sides of the aisle of the subcommittee have an interest in, and that is the classification of national security information.

Actually, when I first came onto the Intelligence Committee, the then chairman, our former House colleague, Porter Goss, had a real interest in this subject matter; and he spoke on it and raised the issue many, many times.

One of the lessons of the attacks of September 11th was that our government did not effectively share information about the terrorists who were plotting the attacks against us. We all know that now. Information sharing was and in some ways remains a major weakness of our Nation's national security apparatus. Overclassification, improper classification and the ability to share information across agencies, the excessive compartmenting of information,

these practices all contribute to a culture that says, "I can't share with you. It is my information, not yours." That hurts our country.

Our Intelligence Community was established during the Cold War when compartmenting of information was deemed necessary to stop the Soviet espionage activity. We no longer face the Soviet bear. We have a newer, more limber challenge. We face a networked adversary that uses information to its strategic advantage and exposes the seams in our system to attack us. So we need to close those seams by reducing the barriers to information sharing; and although we must always protect our sources and methods, we have to balance this with the need to share.

The 9/11 Commission, I think that people in this room are especially aware or keen on the point of their recommendation that the government must develop incentives for sharing to restore better balance between security and shared knowledge. Even today, information may be so highly compartmented that Members and senior policymakers may not have access to it.

For example, the most recent Iraq National Intelligence Estimate, the Iraq NIE, was compartmentalized so that policymakers without those clearances were unable to read it, including many congressional staff. I have to tell you that comes as somewhat of a surprise and certainly worries me.

Today's hearing is going to focus on several issues: First, the consequences of and the proposals to reduce overclassification, and I think that we have given you some examples of overclassification; examine changes to the executive order governing classification over the past decade and the government's compliance with it. There is the executive order. Then there is also compliance to make sure that it works. And, three, the potential changes to the executive order.

The system for safeguarding classified national security information is governed by Executive Order 12958. That number didn't have too much meaning to me until there was a debate that erupted just a handful of weeks ago, and now the number really represents something to me.

Over the years, the executive order has been modified, shifting the balance between secrecy and openness. Our professional, superb witnesses today have been acute observers of these changes over the years; and they are, I think, going to be able to enlighten our committee on how the order has evolved.

I think that this is an important hearing, one, because it is public, certainly because of the content, and also because as part of the Director of National Intelligence 100 Day Plan, the White House and the OBM are reviewing the DNI's authorities with regard to the declassification process. So this is very timely.

I wish that the DNI—I am disappointed, I should say, that the DNI declined to provide a witness today. I think that it would have enhanced the hearing, and perhaps in the not-too-distant future he will agree to and we can work with them as well. Because many of the issues that we are going to discuss today have important, obviously, implications for the Intelligence Community. Otherwise, we wouldn't be here. I hope that Mr. Issa will join me in inviting the DNI to respond for the record.

So, with that, I look forward to the testimony, thank each one of the witnesses and the people that are here in the audience today and would like to recognize Mr. Issa for the remarks that he would like to make. I would just like to say that we are California colleagues; and I think that he is a that we have other opportunity.

We have had many briefings by the DNI in classified settings; and I would note that I can remember one time in which the schedule that showed the DNI, the only witness, the timetable from eight until something, followed by a coffee break, followed by the actual renewal, was classified Top Secret. Now I happen to know that in full battle array with an entourage coming through the Crypt is how he entered. So I have no doubt that the level of secrecy was inappropriate on the agenda.

Therefore, I want to join with you not only in listening to the work that we are going to—the presentations we are going to see today but in continuing to get to where information is most widely available to do the most good while protecting national secrets and, of course, people who risk their lives for our country.

I very much enjoy working with you, and I can't think of a more appropriate hearing to have in the light of day. We may even open the drapes here, because, in fact, declassification should not be a classified hearing.

I yield back.

Chairwoman ESHOO. Thank you very much, Mr. Issa.

The witnesses' full written statements are going to be entered into the record. Without objection, so ordered.

I would like to recognize our witnesses now for their opening statements, and I am going to ask you to limit your opening statement to 5 minutes. I have a clock here. In some of the hearing rooms, we have green, yellow and red, but you are not going to be able to see that. So when you have like a minute left, I will just interrupt briefly and say you have a minute left to summarize.

But the full statement, obviously, is in the record; and then, after you speak, we will begin our questioning.

So why don't we start with Ms. Fuchs. Thank you very much for being here.

I would also like to welcome her daughters that are here and sitting in the front row. Zoe and McKenzie are here with their dad today to hear their mother testify. I hope this experience is going to remain with them for the rest of their lives. I never saw my mother testify in front of Congress.

At any rate, Ms. Fuchs, thank you for being here and we look forward to your testimony. So why don't you begin.

**STATEMENT OF MEREDITH FUCHS, GENERAL COUNSEL, NATIONAL SECURITY ARCHIVE**

Ms. FUCHS. Thank you.

Chairwoman Eshoo, Ranking Member Issa and members of the subcommittee, I am pleased to appear before you today. I am general counsel to the National Security Archive, a nongovernmental, nonprofit research institute. I have submitted written testimony, so I will limit my spoken comments today.

Two weeks ago, the Central Intelligence Agency declassified a 702-page file amassed in 1973 about the CIA's illegal activities, the

so-called "family jewels". It was released pursuant to a FOIA request that my organization made 15 years ago. There was plenty of news coverage about the release, and I will not recount what was in the release, but I just wanted to touch on why the CIA should have to expose the skeletons in its closet.

For one thing, the law requires it to be released. The Freedom of Information Act was passed in 1966, and President Lyndon Johnson when he signed it into law declared: A democracy works best when the people have all the information that the security of the Nation will permit.

A central tenet of the FOIA is that in a democracy the people have the right to know what the government is doing, and Congress passed FOIA because the government bureaucracy was reluctant to have anyone scrutinize its work and was resistant to public requests for information.

In this case, the CIA delayed the decision to release the record for 15 years. They should have released it within 20 business days. Why did they delay it? I mean, although I give them credit for releasing the file, they clearly were trying to do what all governments try to do and that is to control the information.

It is possible the CIA made the release at this time to give the appearance of openness and accountability to an American public that, frankly, is suspicious of their activities today, is concerned about renditioning suspects to secret prisons and about illegal intelligence surveillance of U.S. citizens.

In fact, no real negative consequence is going to reach the Agency as a result of this release of 30-year-old scandals. But the release does help the American public in another way. It helps us understand that there is a genuine risk in having an unrestrained intelligence agency. It shows that abuses have occurred in the past and they can occur if we don't have accountability.

Well, the secrecy situation today offers strong indicators that oversight is necessary now. Since 2001, there has been an explosion of secrecy. I have attached to my written testimony some charts illustrating the problem based on data compiled by the Information Security Oversight Office. Classification has multiplied, reaching an all-time high of 15.6 million classification decisions in 2004, nearly double the number that was in 2001. Last year, in 2005, the most recent year reported, it was at a level of 14.2 million classification actions. I understand today we will learn new numbers for 2006.

The cost of the program also has skyrocketed from an estimated $4.7 billion in 2002 to $7.7 billion in 2005.

Given that we are at war, it is not surprising that there are more secrets and more is being spent to protect them. That is all reasonable. But officials throughout the government, including former Secretary of Defense Donald Rumsfeld, have admitted that there is tremendous overclassification. Those unnecessary secrets come at a cost to society. In addition to the suspicion and skepticism it generates in the general public, there is an increased likelihood of leaks when everything is secret. As such, overclassification devalues the entire security classification system.

Further, as the chairwoman mentioned, we learned from all the inquiries into the September 11th attacks that an excess of secrecy

and compartmentalization of information led to poor intelligence analysis and left us vulnerable to attack.

It is not just a matter of interagency information sharing. Excessive secrecy also locks the doors on the public and prevents the public from knowing information that could be used to protect their families, their communities and the security of the Nation.

My research suggestion that unnecessary secrecy thrives when there is no incentives to limit secrecy. It allows politicians and bureaucrats to avoid embarrassment and accountability and to enforce unpopular or unthinkable measures. Information, quite simply, is power.

My organization has long advocated efforts to increase the incentives on the other side of the secrecy equation in order to encourage openness and discourage unnecessary secrecy. I am going to quickly mention some of our suggestions, which are detailed in my written testimony.

Today, all power for creating and holding secrets rests with a small group of executive branch agencies. One solution to the problems that arise as a result of that is to disperse the power, particularly with respect to historic materials where the passage of time and of events has made the information less sensitive.

I describe some proposals in my written testimony for changing the dynamic, including a declassification center, the national declassification initiative that has started at the National Archives, and statutory independent review boards at every agency with classification authority.

Briefly, I would like to touch on the executive order on classification. There are some changes in the executive order that could lead to less unnecessary classification. In particular, the order should emphasize limited classification, limited duration to classification and a presumption against classification. It should strictly limit reclassification and should employ a cost-benefit analysis to any such effort.

It should also remove the veto authority provided to the DCI and now the DNI over decisions of the Interagency Security Classification Appeals Panel. Emphasis should be put on periodic independent audits of classification decisions, procedures for challenging classification decisions, and adequate current classification guides that include an explanation of a specific harm or threat that justifies the classification.

Just one more comment.

It does not help the system when the classification system and its oversight entity are disregarded or ignored, as was the case in the recent reclassification of records last year at the National Archives and also in the case of the Vice President's office refusing to report its classification activity. Scandals like those merit an immediate response from Congress as a check against misconduct and overreaching.

I am hopeful my testimony has been helpful, and I would be happy to respond to any questions. Thank you.

Chairwoman ESHOO. Thank you very much. We appreciate your testimony, and we are going to have questions for you.

[The statement of Ms. Fuchs follows:]

STATEMENT OF MEREDITH FUCHS, GENERAL COUNSEL, NATIONAL SECURITY ARCHIVE

Chairwoman Eshoo, Ranking Member Issa and Members of the Subcommittee on Intelligence Community Management, I am pleased to appear before you to discuss the issue of classification and declassification of national security information.

I am General Counsel to the National Security Archive (the "Archive"), a non-governmental, non-profit research institute. The Archive is one of the most active and successful non-profit users of the Freedom of Information Act (FOIA) and the Mandatory Declassification Review (MDR) system. We have published more than half a million pages of released government records, and our staff and fellows have published more than 40 books on matters of foreign, military, and intelligence policy. In 1999, we won the prestigious George Polk journalism award for "piercing self-serving veils of government secrecy" and, in 2005, an Emmy award for outstanding news research.

## SKELETONS IN THE CLOSETS

Two weeks ago the Central Intelligence Agency (CIA) declassified a 702-page file amassed in 1973 at the order of then-CIA director James Schlesinger about the CIA's illegal activities—the so-called "family jewels." It was released pursuant to a FOIA request filed 15 years ago by my organization. There was plenty of news coverage about the release. I won't take time today to recount the details of illegal wiretapping, domestic surveillance, assassination plots, and human experimentation acknowledged in the file. The CIA deserves credit for actually reviewing and releasing portions of these records as the FOIA obliges it to do; the Agency is not always so diligent in fulfilling its FOIA obligations. Instead I want to focus on a broader issue about why it is important for records about our government's misdeeds and mistakes to be made available to the public.

For one thing, the law requires the release. When Congress passed the FOIA in 1966 and President Lyndon Johnson reluctantly signed it into law, the President declared that: "A democracy works best when the people have all the information that the security of the nation will permit." Under the FOIA, agencies are supposed to respond to a request for documents within 20 business days. Yet it took some bad publicity about FOIA delays up to 20 years, some pressure from Congress in the form of the OPEN Government Act of 2007—which awaits a Senate vote—and a presidential executive order (E.O. 13392) directing agencies to handle backlogs for this request to finally reach the front of the queue. A central tenet of the FOIA is that in a democracy, the people have a right to know what their government is doing. Congress passed FOIA because the government bureaucracy, reluctant to have anyone scrutinizing its work, was resistant to public requests for information. The law is tool for individuals to demand records of agency activities so that those agencies will be more accountable and make better decisions in the future.

The second reason it is important for agencies to release records like the "family jewels" is that in a mature democracy such as ours, opening up to scrutiny vital parts of our country's recent history builds trust in government institutions and reaffirms their legitimacy. For an agency like the CIA, subject to attack concerning activities such as transporting detainees to secret prisons around the world, the release of the "family jewels" seems to be an attempt to draw a clear line between the past and the present. The acknowledgment of wrongdoing is like an act of atonement and suggests the intent to reform bad practices. The message to the public is that the Agency is not unaccountable.

A third reason the release is important is it allows people to understand what has happened in the past and reminds people that abuses can occur if there is no oversight. A functioning democracy needs an informed citizenry armed with the tools and knowledge to play their role in the political system. Finally, the "family jewels" helps us better understand the thinking of many current government officials who first served in government policy positions in the 1970s, including those who were not happy about the congressional reforms enacted in the 1970s and the weakening of executive branch power.

## THE EXPLOSION OF SECRECY

I would like to return to President Johnson's statement when he signed the FOIA. He did not promise complete openness, but only such openness as the security of the nation permits. We all know secrecy is necessary to avoid providing our enemies with means to harm us, to enable us to forcefully negotiate with foreign governments, and to ensure that the sources and methods of intelligence gathering are protected. The protection of these sorts of secrets is primarily governed by Executive

Order 12958, as amended, and a series of provisions in statutes governing the intelligence community.

The available statistics show that there has been a dramatic upsurge in this sort of government secrecy since the September 11 attacks on the United States. Classification has multiplied, reaching an all-time high of 15.6 million classification actions in 2004, nearly double the number in 2001, and was at a level of 14.2 million classification actions in 2005.[1] Moreover, the cost of the program has skyrocketed from an estimated $4.7 billion in 2002 to $7.7 billion in 2005.[2] At the same time, declassification activity shrank from a high of 204.1 million pages declassified in 1997, down to 29.5 million pages declassified in 2005.

Officials from throughout the military and intelligence sectors have admitted that much of this classification is unnecessary. Secretary of Defense Donald Rumsfeld acknowledged the problem in a 2005 Wall Street Journal op-ed: "I have long believed that too much material is classified across the federal government as a general rule . . . ."[3] The extent of over-classification is significant. Under repeated questioning from members of Congress at a hearing concerning over-classification, Deputy Secretary of Defense for Counterintelligence and Security Carol A. Haave, eventually conceded that approximately 50 percent of classification decisions are over-classifications.[4] These opinions echoed that of Porter Goss, then Chair of the House Permanent Select Committee on Intelligence, and later Director of Central Intelligence, who told the 9/11 Commission, "we overclassify very badly. There's a lot of gratuitous classification going on, and there are a variety of reasons for them."[5]

There are many reasons for the increased numbers of secrets and the increase in costs associated with the national security classification program. We are at war and are highly conscious of the need to prevent terrorist attacks. Yet, what about the unnecessary secrets that clog up the security classification system without offering any additional security? Those unnecessary secrets come at a greater price than the money it costs to protect them.

The Director of the Information Security Oversight Office (ISOO), the governmental agency responsible to the President for policy oversight of the government-wide security classification system and the National Industrial Security Program, who is testifying today, has called secrecy a "double edged sword."[6] While classification serves the purpose of keeping information out of the hands of the enemy, it also sometimes keeps it out of the hands of friends or allies who could use it to protect us. Too much secrecy conceals our vulnerabilities until it is too late to correct them. Indeed, all of the inquiries concerning the September 11 attacks on the United States found that better information dissemination would have made us safer. It is not only government agencies who must share information with each other, but agencies must learn to share information with the public. As Eleanor Hill, Staff Director of the Joint House-Senate Intelligence Committee Investigation into September 11 Attacks, explained in a Staff Statement summarizing the testimony and evidence:

> [T]he record suggests that, prior to September 11th, the U.S. intelligence and law enforcement communities were fighting a war against terrorism largely without the benefit of what some would call their most potent weapon in that effort: an alert and committed American public. One needs look no further for proof of the latter point than the heroics of the passengers

---

[1] ISOO, 2004 Report to the President at 3 (2005), http://www.archives.gov/isoo/reports/2004-annual-report.pdf; ISOO, 2005 Report to the President at 2 (2006), http://www.archives.gov/isoo/reports/2005-annual-report.pdf.

[2] ISOO, 2005 Report on Cost Estimates for Security Classification Activities for 2005 at 3 (2006), http://www.archives.gov/isoo/reports/2005-cost-report.pdf; ISOO, 2001 Report to the President at 9 (2002), http://www.archives.gov/isoo/reports/2001-annual-report.pdf.

[3] Donald Rumsfeld, War of the Worlds, Wall St. J., July 18, 2005, at A12.

[4] Subcommittee on National Security, Emerging Threats and International Relations of the House Committee on Gov't Reform Hearing,108th Cong. (2004) (testimony of Carol A. Haave), http://www.fas.org/sgp/congress/2004/082404transcript.pdf; See id., (Testimony of J. William Leonard, Director of ISOO) ("It is my view that the government classifies too much information.").

[5] 9/11 Commission Hearing, (Testimony of then Chair of the House Permanent Select Committee on Intelligence Porter Goss) (2003), http://www.9-11commission.gov/archive/hearing2/9-11Commission_Hearing_2003-05-22.htm#panel—two.

[6] Emerging Threats: Overclassification and Pseudo-classification: Hearing Before the Subcomm. on Nat'l Sec., Emerging Threats, and Int'l Relations of the H. Comm. on Gov't Reform, 109th Cong. (2005) (statement of J. William Leonard, Director, ISOO, Nat'l Archives and Records Admin.), http://reform.house.gov/UploadedFiles/ISOO Leonard testimony final 3-2-05 hearing.pdf.

> on Flight 93 or the quick action of the flight attendant who identified shoe bomber Richard Reid.[7]

There are other costs to keeping the public in the dark. Dissemination of information has always been critical for advancing technological and scientific progress. When considering the option of making the genome databases secret, even though the data could be used to engineer pathogens for use as biological weapons, the National Academy of Sciences concluded:

> [A]ny policy stringent enough to reduce the chance that a malefactor would access data would probably also impede legitimate scientists in using the data and would therefore slow discovery . . . . It is possible that the harm done during a process of negotiating such an agreement—through building walls of mistrust between peoples—would be greater than the benefit gained through the sense of security that such a regime might provide. Finally, such a restrictive regime, the committee believes, could seriously damage the vitality of the life sciences . . . There is some concern that restricting access to this information might lead to a situation in which the mainstream scientific community is unaware of dangers that may threaten us."[8]

Moreover, overclassification and unneeded secrecy also undermine the effort to keep truly sensitive information secret, "[f]or when everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or careless, and to be manipulated by those intent on self-protection or self-promotion."[9]

If secrecy comes with so many costs, why is there so much unnecessary secrecy? Secrecy can be used as a tool by the government in many ways. When claims of national security secrecy are plausible, secrecy often allows the government to enforce policies that otherwise would be unthinkable. Often, the claim of secrecy ends any public inquiry into allegations of misconduct, as well as any governmental liability. We see this today in the context of the warrantless wiretapping program initiated after September 11, 2001. To date there has been minimal success challenging the program despite confirmation of the program and signs of official concern about the illegality of the program.

Perhaps an even stronger motivation is that by controlling information through classification and selective declassification, the government also has the ability to control public opinion and avoid embarrassment. As former Solicitor General of the United States Erwin Griswold, who led the government's fight for secrecy in the Pentagon Papers case, acknowledged:

> It quickly becomes apparent to any person who has considerable experience with classified material that there is massive overclassification and that the principal concern of the classifiers is not with national security, but with governmental embarrassment of one sort or another. There may be some basis for short-term classification while plans are being made, or negotiations are going on, but apart from details of weapons systems, there is very rarely any real risk to current national security from the publication of facts relating to transactions in the past, even the fairly recent past.[10]

## CONTROLLING EXCESSIVE SECRECY

Today, all power for creating and holding secrets rests with a small group of executive branch agencies. While there is no doubt that the individual agency-centered approach allows for agencies to exercise independent judgment, the unilateral nature of the decision-making allows excessive secrecy to permeate individual agencies unchecked. When that happens, all of the worst features of turf consciousness and bureaucratic inertia come into play.

One solution is to disperse the power, particularly with respect to historic materials where the passage of time and events has made it less necessary for one agency to jealously control all information. The Moynihan Commission, for example, rec-

---

[7] Intelligence Community's Response to Past Terrorist Attacks Against the United States from February 1993 to September 2001: Hearing Before the J. H./S. Intelligence Comm., 107th Cong. (2002) (Joint Inquiry Staff Statement, Eleanor Hill, Staff Dir.), http://intelligence.senate.gov/0210hrg/021008/hill.pdf.

[8] See, e.g., Nat'l Acad. of Sciences, Seeking Security: Pathogens, Open Access, and Genome Databases 54–57 (2004), http://www.nap.edu/books/0309093058/html/52.html.

[9] *New York Times Co.*, 403 U.S. at 729 (Stewart, J., concurring).

[10] Erwin N. Griswold, *Secrets Not Worth Keeping: The courts and classified information,* Wash. Post, Feb. 15, 1989, at A25.

ommended setting up a formal Declassification Center based at the National Archives and Records Administration (NARA) and staffed by an interagency group with delegated powers from their agencies.[11] The National Declassification Initiative (NDI) that emerged last year, only after my organization, working with historian Matthew Aid, exposed the unilateral reclassification by agencies of historical materials that had been publicly available for years, goes part of the way to making this idea a reality. The NDI is sponsored by NARA. By harnessing the combined resources and expertise of many different agencies, the NDI could speed access to insightful historical documents for researchers and the general public. However, the NDI's underlying innovation—the establishment of a comprehensive, interdepartmental declassification review capability for the federal government—could prove to be a serious flaw. The concentration of declassification activities in one location presents the risk that official declassification will fall prey to an unhealthy consensus, built upon the worst disclosure fears of individual agencies rather than principles of increased transparency and public access. As NARA itself has noted, "the biggest impediments to the NDI are culture, attitude, and resistance to change" on the part of participating Executive Branch agencies.[12]

One method of countering this tendency towards group think would be to establish a non-partisan, non-governmental board of private citizens to represent the interests of professional researchers, historians, and the general public in the declassification process of the NDI. Such a board could serve as a conduit for public input and oversight. There are models for such a board, including those authorized by Congress in the President John F. Kennedy Assassination Records Collection Act of 1992 and the Nazi War Crimes Disclosure Act. Another model would be the establishment of a statutory independent review board at every agency with classification authority. The State Department's Advisory Committee on Historical Diplomatic Documentation offers an example of how such a board can be successful in pushing out of the system the secrets that do not need keeping.

The NDI and statutory independent review boards are well suited to breaking down the excessive control that agencies have exerted over historical records. Yet, historical records will still clog up the system because they are subject to the same type of review as current records. To illustrate the problem, consider the myth of automatic declassification. As of January 1 of this year, over 1 billion pages of records had been declassified under the provisions of Executive Order 12958, as amended. Yet, none of us can stroll into the National Archives and get to see those records. All the newly declassified records still must be processed by NARA before they will be made available to the public at NARA research facilities. Each of those records essentially has to go through standard FOIA review before it can be released for the public. That is the same review that in some cases has held records for up to 20 years after a FOIA request is made. A historical records review act that would alter the standard for review and withholding of records older than 25 years could end the bottleneck. Like the Nazi War Crimes Disclosure Act and the John F. Kennedy Assassination Records Review Act, which altered the standards for review and withholding of records older than 25 years.

Chairwoman ESHOO. Next, I would like to welcome Steven Aftergood, Director of the Project on Government Secrecy at the Federation of American Scientists.

Welcome. You have 5 minutes for your testimony.

## STATEMENT OF STEVEN AFTERGOOD, DIRECTOR, PROJECT ON GOVERNMENT SECRECY, FEDERATION OF AMERICAN SCIENTISTS

Mr. AFTERGOOD. Thank you, Madam Chairwoman, Ranking Member Issa. Thank you for holding this hearing.

Some people might think that classification is basically a matter of housekeeping of no great significance, but actually, as you know, it is tremendously significant. It defines the boundaries of what the public is permitted to know, what government officials are per-

[11] Report of the Commission on Protecting and Reducing Government Secrecy, S. Doc. No. 105–2 (1997), at Ch. 3.

[12] See http:/www.archives.gov/declassification/challenges.pdf.

mitted to say in public, and it determines how well our deliberative system is able to function.

Judging from your opening remarks, the two of you, it is clear that there is a consensus that the system is not working as it was intended. It is not working as well as it should. What is less clear is what to do about that.

In my written testimony, I have presented a short menu of specific steps that could be taken; and for now I would like to mention just two of them. My hope is that one or more of them might appeal to you and that you and the subcommittee might pursue them further.

The first is the notion of a declassification database. Right now when a document is declassified, it is a lot like a tree that falls in the forest with no one around. No one has any idea that the document has been declassified, much less that it might be available to them.

So, therefore, it seems sensible to establish an agency-by-agency database which gives some indication that a document or a set of documents has been processed for declassification and is available. In fact, such a database was mandated by Executive Order 12958 in 1995. Unfortunately, that provision was modified in 2003, and the requirement to create a government-wide database was eliminated. So was the requirement to make such a database publicly available. So we have, unfortunately, stepped back from what would have been a very useful step to take full advantage of the declassification that we are already doing.

It is interesting to me to note that, of all agencies, it seems to be the CIA that has made the most progress in developing a declassification database. It has created something called CREST, which is the CIA Records Search Tool, which is actually a database of many millions of documents that have been declassified. Not only that, it is publicly available but only in one particular room at the National Archives in College Park.

The CIA has inexplicably, in my mind, refused to make the database available online or even to release its contents to others who would themselves put it online. So I think that might be something worth the subcommittee's attention. If that could be turned into a public resource, that would immediately multiply the utility of current declassification programs.

A quick second proposal or notion, and that is the concept of the tear-line format in creating classified documents. A tear line refers to the idea that when you create a classified record, you physically segregate the content of the document by classification level so that, in principle, you could tear off the unclassified portion and give it to somebody.

This is not a new idea. It has been around for a while. In fact, Congress endorsed the tear-line format proposal in the 2004 Intelligence Reform Bill; and it instructed the administration to prepare guidelines for implementing tear lines so that we could improve information sharing.

Now those guidelines were never issued, and that might be something the subcommittee wants to look into. Why was a direction that you gave two and a half years ago never acted upon? I mean, I can't help but think when you mentioned that the DNI refused

to send a representative, whether the ODNI is somehow showing inadequate respect for Congress and whether that is not something else to look into.

I will leave it there for now. Thank you very much for holding the hearing.

Chairwoman ESHOO. Thank you for your excellent testimony.

[The statement of Mr. Aftergood follows:]

STATEMENT OF STEVEN AFTERGOOD, FEDERATION OF AMERICAN SCIENTISTS

Thank you for the opportunity to address the Subcommittee.

My name is Steven Aftergood and I direct the Project on Government Secrecy at the Federation of American Scientists, which seeks to enhance public access to government information and to limit national security classification to its necessary minimum.

INTRODUCTION

It has been ten years since the congressionally-mandated Commission on Protecting and Reducing Government Secrecy issued its critique of national security classification policy and called for "a new way of thinking about government secrecy."

The Commission, chaired by Sen. Daniel P. Moynihan and co-chaired by former HPSCI chairman Rep. Larry Combest, concluded that:

> The classification system . . . is used too often to deny the public an understanding of the policymaking process, rather than for the necessary protection of intelligence activities and other highly sensitive matters. The classification [system is] no longer trusted by many inside and outside the Government.[1]

The Commission produced a fine report, but its work led to no discernable improvement in policy. In 2003, another HPSCI chairman, Rep. Porter J. Goss, testified before the 9/11 Commission that "we overclassify very badly. There's a lot of gratuitous classification going on . . ."[2]

The adverse consequences of overclassification are clear enough. Unnecessary or inappropriate classification degrades the performance of government agencies, impedes oversight, and fosters public suspicion and contempt. Yet the classification system has proved to be stubbornly resistant to reform or correction.

In this statement, I would like to propose several specific steps that could be taken to improve classification and declassification policy. While these steps would not fully resolve all concerns about the proper exercise of classification authority, each of them has the virtue of being achievable in the near term. And individually or collectively, they would make a real difference.

*1. Establish a declassification database*

If a database of declassified documents could be established and made publicly accessible, then the positive impact of declassification would be multiplied many times over.

Such a database was explicitly required in 1995 by Executive Order 12958, section 3.8, which stated:

> The Archivist in conjunction with the Director of the Information Security Oversight Office and those agencies that originate classified information, shall establish a Government-wide database of information that has been declassified . . . . Except as otherwise authorized and warranted by law, all declassified information contained within the database . . . shall be available to the public.

Unfortunately, this objective was abandoned in the 2003 amendments to Executive Order 12958. The amended order eliminated the requirement to establish a

[1] Report of the Commission on Protecting and Reducing Government Secrecy, 1997, page xxi, available at http://www.fas.org/sgp/library/moynihan/index.html.

[2] Hearing before the National Commission on Terrorist Attacks, May 22, 2003, available at http://www.fas.org/irp/congress/2003__hr/911Com20030522.html.

Government-wide database and also deleted the requirement that declassified information in any existing databases be made available to the public.[3]

Without some form of public database to serve as a universal finding aid, it seems unlikely that most declassified documents will ever be located by the particular readers who would be most interested in them.

Interestingly, it is the Central Intelligence Agency that has made the most progress in this direction. Its CREST database (CREST stands for CIA Records Search Tool) provides a searchable index of millions of declassified Agency records. And it is publicly available—but only in Room 3000 of National Archives II in College Park, MD.

Inexplicably, CIA has refused to make CREST publicly available online or even to release the database to others who would do so at their own expense. Outside of Room 3000 at the Archives at College Park, the CREST database might as well not exist.

I suggest that this Committee ask intelligence community agencies to establish public databases of their declassified documents. I further suggest that the Committee instruct the CIA to permit online access to its existing CREST database.

*2. Adopt a "tear line" format in at least one agency*

One way to combat the effects of overclassification is to require that official records be written in such a way that their contents are physically segregable by classification level and that unclassified information in the document can be readily separated from any classified information. This is commonly known as a "tear line" format, referring to the possibility of "tearing off" a portion of the document, literally or figuratively, so that it can be widely disseminated.

Congress has already endorsed the tear line approach. In the Intelligence Reform and Terrorism Prevention Act of 2004, Congress mandated that:

> the President shall . . . issue guidelines . . . to ensure that information is provided in its most shareable form, such as by using tearlines to separate out data from the sources and methods by which the data are obtained;[4]

Several years later, however, no such guidelines have been issued.

Under the circumstances, it might be productive to undertake a more focused and limited approach. A "pilot project" applied to one government agency or organization could demonstrate the utility and feasibility of tear lines without engendering widespread bureaucratic opposition.

For example, this Committee could ask the National Intelligence Council to adopt the tear line format in all of the National Intelligence Estimates that it prepares in the next twelve months. Since NIEs are intended for distribution outside of the intelligence community, these seem like a logical category of intelligence records with which to begin applying the tear line approach.

Even if an entire document must remain classified for a time and cannot be publicly disclosed, a tear line approach that isolates compartmented information from collateral classified information would still facilitate distribution throughout government, including Congress. It would also expedite the ultimate declassification of the document.

*3. Add classification oversight to the functions of agency Inspectors General*

In order to augment existing oversight of classification and declassification activities performed by the Information Security Oversight Office, agency Inspectors General should be tasked to perform their own periodic reviews of classification and declassification.

Given the general consensus that classification is very expensive, both financially and operationally, agency heads may well concur that increased oversight of classification practices is appropriate and may be expected to endorse increased IG attention to this area.

Inspectors General with cleared staff are already in place at the relevant agencies and could readily undertake such oversight. Indeed, some of them, like the DoD Inspector General, already perform some classification oversight on an ad hoc basis.

This Committee should therefore ask each of the intelligence community inspectors general to add a periodic review of classification and declassification activities to its portfolio of regular auditing functions.

---

[3] See Executive Order 12958, as amended (EO 13292), at section 3.7. The amended order only says vaguely that agencies "shall coordinate the linkage and effective utilization of existing agency databases." All of the additions and deletions that were made in the 2003 amendments to the executive order can be seen in this markup: http://www.fas.org/sgp/bush/eo13292inout.html.

[4] Intelligence Reform and Terrorism Prevention Act of 2004, section 1016(d)(1).

*4. Declassify the annual intelligence budget*

There is no single declassification action that would signal an end to obsolete classification practices as clearly and powerfully as declassification of the total annual intelligence budget.

That was the bipartisan conclusion of the Aspin-Brown-Rudman Commission in 1996.[5] It was also the unanimous recommendation of the 9/11 Commission in 2004.[6] But it has elicited fierce opposition from those who are attached to the status quo.

Paradoxically, the persistent opposition to intelligence budget disclosure has elevated the issue to one of outstanding significance, thereby making its potential declassification even more powerful.

The notion that that annual disclosure of the total intelligence budget could damage national security, a view that the present Administration appears to hold, has been decisively refuted. The budget total was formally declassified in 1997 and 1998 without adverse effect. Nor did release of the budget in those years lead to uncontrolled disclosure of more sensitive information. In other words, the hypothetical "slippery slope" feared by proponents of continued budget secrecy did not materialize.

In fact, intelligence budget classification is a relic of times gone by that has nothing to do with protecting current national security interests.

Declassification of the intelligence budget will help to set an enlightened new standard for classification policy by demonstrating that even the most entrenched secrecy practices are subject to reconsideration and will be rejected when they no longer make sense.

Although this Committee has already completed its markup of the 2008 Intelligence Authorization Act without addressing intelligence budget disclosure, the Senate version of the bill does include a provision for requiring such disclosure (section 107 of S. 1538). Committee members may therefore encounter this provision in a future House-Senate conference.

If so, I would urge you to seize the opportunity to achieve a final resolution of this longstanding controversy, and a new beginning for intelligence classification policy by endorsing declassification of the intelligence budget.

Thank you for considering my views on these important issues.

Chairwoman ESHOO. Last, but not least, Mr. Bill Leonard, who is the Director of the Information Security Oversight Office. Many members of the committee commonly refer to it as the National Archives and Records Administration, NARA.

Welcome. Thank you for your wonderful service to our country. Very distinguished career dating back before you arrived at the National Archives and Records Administration. So welcome. We look forward to your testimony.

## STATEMENT OF J. WILLIAM LEONARD, DIRECTOR, INFORMATION SECURITY OVERSIGHT OFFICE

Mr. LEONARD. A career of probably more years than I want to admit.

Madam Chair, Mr. Issa, I want to thank you very much for holding this hearing on issues relating to the classification of national security information within the Intelligence Community as well as for inviting me to testify today.

In the invitation to testify, you requested I address a number of issues, to include changes to the executive order over the past decade. In March, 2003, the President signed an order further amending Executive Order 12958. The principal purpose of the amendment was to provide agencies an additional 3½ years to address the remaining backlog of unreviewed 25-year-old classified records of permanent historical value prior to the onset of automatic de-

[5] Preparing for the 21st Century: An Appraisal of U.S. Intelligence, available online at http://www.fas.org/irp/offdocs/report.html, Recommendation 14–2, March 1996.

[6] Final Report of the National Commission on Terrorist Attacks Upon the United States, page 416.

classification, a concept I explain in detail in my formal written statement. I also provide in that statement a synopsis of the other changes that time does not permit me to go into at this time.

However, what is most notable about the 2003 amendment is what did not change. The revision left the existing classification and declassification regime largely intact. It had an exceedingly limited impact on the way in which government officials classified or declassified information. For all practical purposes, it institutionalized automatic declassification as an essential element of the classification process.

I also outline in my formal statement the second issue you requested me to address, specifically, an assessment of agency compliance with the order. In fiscal year 2006, my office conducted a total of 15 on-site reviews of executive branch agencies. Of the general program reviews we conducted, we found that few of the agencies visited had adequately implemented the core elements of the classified National Security Information Program. Shortcomings were observed at multiple agencies in their implementing regulations, self-inspection programs, document markings and refresher security education and training.

I should further note, however, that, as a general rule, Intelligence Community agencies tend to have the most sound information security programs within the executive branch.

Last year, last fiscal year, we concentrated much of our compliance reviews on the appropriateness of classification decisions; and, based upon a sample of over 2,000 documents reviewed, we identified many to be questionable.

Which brings me to the third issue you requested me to address, the impacts of overclassification. The ability and authority to classify national security information is a critical tool at the disposal of the government and its leaders to protect our Nation and its citizens. In this time of constant and unique challenges to our national security, it is the duty of all of us engaged in public service to do everything possible to enhance the effectiveness of this tool.

To be effective, the classification process is a tool that must be wielded with precision. In an audit of agency classification activities conducted by my office over a year ago, we discovered that even trained classifiers with ready access to the latest classification and declassification guides and trained in their use got it clearly right only 64 percent of the time in making determinations as to the appropriateness of classification.

This is emblematic of the daily challenges confronting agencies when ensuring that the 3 million plus cleared individuals with at least a theoretical ability to derivatively classify information get it right each and every time. Too much classification unnecessarily obstructs effective information sharing and impedes an informed citizenry, the hallmark of our democratic form of government.

You also requested I address the effectiveness of current declassification efforts. After several deadline extensions, automatic declassification finally became effective on December 31st, 2006, with a few notable authorized delays. While a detailed analysis of the final results is still under way, it appears that all executive branch agencies have succeeded in meeting their initial obligations under the automatic declassifications provisions of the order.

As significant as the initial development of the concept of automatic declassification was, its actual implementation after so many false starts and delays is even more of an accomplishment. It reflects well on the diligence and efforts of the public servants who accomplished this milestone through hard work and perseverance, as well the agencies that committed the requisite resource. However, significant challenges remain; and I have outlined them in my formal written statement.

Finally, you asked that I address the effect of selective classification and declassification in my formal statement. I provide a synopsis of the policy.

Again, thank you for inviting me here today, Madam Chair. I am happy to answer any and all questions.

Chairwoman ESHOO. Thank you very much.

[The statement of Mr. Leonard follows:]

STATEMENT OF J. WILLIAM LEONARD, DIRECTOR, INFORMATION SECURITY OVERSIGHT OFFICE

Chairwoman Eshoo, Mr. Issa, and members of the subcommittee, I wish to thank you for holding this hearing on issues relating to classification of national security information within the Intelligence Community as well as for inviting me to testify today.

BACKGROUND

By section 5.2 of Executive Order 12958, as amended, "Classified National Security Information" (the Order), 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 directed by the Archivist of the United States, who appoints the Director of ISOO, subject to the approval of the President. We also receive policy guidance from the Assistant to the President for National Security Affairs. Under the Order and applicable Presidential guidance, ISOO has substantial responsibilities with respect to the classification, safeguarding, and declassification of information by agencies within the executive branch. Included is the responsibility to develop and promulgate directives implementing the Order. We have done this through ISOO Directive No. 1 (32 CFR Part 2001) (the Directive).

The classification system and its ability to restrict the dissemination of information the unauthorized disclosure of which could 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 confidentiality and plausible deniability as the only way to balance competing and divergent national interests.

It is the Order that sets forth the basic framework and legal authority by which executive branch agencies may classify national security information. Pursuant to his constitutional authority, and through the Order, the President has authorized a limited number of officials to apply classification to certain national security related information. In delegating classification authority the President has established clear parameters for its use and certain burdens that must be satisfied.

Specifically, every act of classifying information must be traceable back to its origin as an explicit decision by a responsible official who has been expressly delegated original classification authority. In addition, the original classification authority must be able to identify or describe the damage to national security that could reasonably be expected if the information was subject to unauthorized disclosure. Furthermore, the information must be owned by, produced by or for, or under the con-

trol of the U. S. Government; and finally, it must fall into one or more of the categories of information specifically provided for in the Order.[1]

The President has also spelled out in the Order some very clear prohibitions and limitations with respect to the use of classification. Specifically, for example, in no case can information be classified in order to conceal violations of law, inefficiency, or administrative error, to restrain competition, to prevent embarrassment to a person, organization, or agency, or to prevent or delay the release of information that does not require protection in the interest of national security.

It is the responsibility of officials delegated original classification authority to establish at the time of their original decision the level of classification (Top Secret, Secret, and Confidential), as well as the duration of classification, which normally will not exceed ten years but in all cases cannot exceed 25 years unless an agency has received specific authorization to extend the period of classification.

CHANGES TO THE ORDER OVER THE PAST DECADE

The current framework has basically been in effect since 1995. One of the most innovative features of the current framework is the concept of automatic declassification. Under prior executive orders governing classification and declassification, information once classified remained so indefinitely and very often did not become available to general public, researchers, or historians without persistent and continuous effort on the part of these individuals. While all agencies had the responsibility to systematically review historical classified records for declassification, and some agencies such as the State Department did so on a regular basis, there was no specified consequence for agencies that did not conduct such reviews. Understandably, in times of budget constraints, reviews for declassification suffered, resulting in a significant backlog or "mountain" of classified historical records, many of which were much older than 25 years of age.

Under automatic declassification, information in records appraised as having permanent historical value is automatically declassified 25 years after classification, unless an agency head has determined that it falls within one of several limited exceptions that permit continued classification, a continuation that either the President or the Interagency Security Classification Appeals Panel (ISCAP) has approved. In effect, automatic declassification reverses the resource burden. Unlike previous systems, in which agencies had to expend resources to declassify older information, under the current system, agencies must expend resources to demonstrate why older historical information needs to remain classified.

In March 2003, the President signed Executive Order 13292 further amending Executive Order 12958. The principal purpose of the amendment was to provide agencies an additional three and a half years to address the remaining backlog of unreviewed 25-year-old classified records of permanent historical value prior to the onset of automatic declassification. This and other changes were recommended by a broad consensus of interagency professionals in classification and declassification. They reflect seven years of experience in implementing E.O. 12958 as well as new priorities resulting from the events of 9/11.

What is most notable about the 2003 amendment is what did not change. The revision left the existing classification/declassification regime largely intact. It had an exceedingly limited impact on the way in which government officials classified or declassified information. For all practical purposes, it institutionalized automatic declassification as an essential element of the classification process.

For classifiers, the most notable change was a simplification of the process and a resulting change in marking requirements. For those involved in the declassification process, in addition to providing more time to complete the review of 25-year old records, the revision gave greater clarity to what records are subject to automatic declassification and under what conditions.

A synopsis of the most significant changes included in the amendment is set forth below:

---

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

—*Deadline for Automatic Declassification Extended.* The 2003 amendment committed agencies to finish reviewing the backlog of classified records more than 25 years old, by the end of 2006. (Sec. 3.3(a))

—*Clarification of Documents Subject to Automatic Declassification.* Before the most recent amendment, the language of the Order was unclear as to what 25-year-old documents that had not been explicitly exempted from release were subject to declassification and under what circumstances. Moreover, even in blocks of retired records spanning a period of years, the language suggested that older documents would become automatically declassified before the larger body of records was subject to review.

A number of changes were made that clarified the question of what documents are automatically declassified at 25 years:

—Records in a file block shall not be automatically declassified until the most recent record is 25 years old (Sec. 3.3(e)(1));

—An additional five years is allowed for difficult to review records such as audio and video tapes (Sec. 3.3(e)(2));

—An additional three years is allowed for the release of records transferred or referred from another agency (Sec. 3.3(e)(3));

—An additional three years is allowed for newly discovered records (Sec. 3.3(e)(4)).

—*Protecting Foreign Government Information.* The 2003 amendment to the Order contained the presumption that the unauthorized disclosure of foreign government information exchanged in confidence will cause damage to the national security (Sec. 1.1(c)). The practical consequence of this addition was limited since the original Order contained such broad discretion in this area that an original classifier had the authority to classify such information all along. More importantly, the amendment made it explicit that for foreign government information to be exempt from automatic declassification, the same standard as other information concerning foreign and diplomatic relations of the United States and a foreign government is to be applied. Specifically, serious and demonstrable "impairment" or "undermining" of these relations or activities must be shown in order for the information to be exempted. (Sec. 3.3(b)(6))

—*Categories of Classifiable Information Clarified.* Additional categories of information, specifically defense against transnational terrorism, infrastructures, and protection services, were explicitly spelled out as included in those that were eligible for classification. "Weapons of mass destruction" was added as a separate category. Arguably, all such information was already covered by the existing Order but the amendment made these points clearer. (Sec. 1.4(e), (g) & (h))

—*Simplifying the Scheme.* E.O. 12958 had been considered unduly complicated to administer because of separate criteria for original classification for up to ten years; for original classification from 10 to 25 years; and for extending classification beyond 25 years. To correct this, the separate set of criteria for withholding information between 10 and 25 years from date of origin was eliminated. While the revised language maintains ten years as the norm for most original classification actions, there is now one set of criteria for classification up to 25 years (Sec. 1.4) and another for continuing classification beyond 25 years (Sec. 3.3(b)).

—*Reclassification of Properly Released Material.* As originally issued, the Order prohibited the reclassification of information after it had been released to the public under proper authority and prohibited it entirely for documents more than 25 years old. The 2003 amendment restored the ability under the predecessor executive order to reclassify such information and dropped the prohibition on 25-year-old information, but only under "the personal authority of the agency head or deputy agency head" and only if the material may be "reasonably recovered." (Sec. 1.7(c) & (d))

—*Continuing Ability to Exempt File Series.* When the order was originally issued in 1995, it required that all record file series that were to be exempted from automatic declassification at 25 years be identified to the President before the Order went into effect. This was changed so that an agency may now notify the President at any time of file series of records that qualify under the specific standards for exemption. (Sec. 3.3(c))

—*Authority of Director of National Intelligence (DNI) Recognized.* While intelligence sources and methods information remain subject to the jurisdiction of Interagency Security Classification Appeals Panel (ISCAP), the amendment recognized the special authority and responsibility of the now DNI to protect such information. As such, this revision authorized the DNI to object to final ISCAP declassification conclusions about such information. Furthermore, a decision by

the DNI to bar release can still be appealed to the President by any member agency of ISCAP. (Sec. 5.3(f))

—*Sharing Classified Information in an Emergency.* One of the issues that arose in the wake of 9/11 was awareness of the limitations imposed by the lack of authority under the Order to pass classified information to individuals not otherwise eligible (e.g. local and state authorities without the necessary clearances) in an emergency. As a result, a section was added specifically authorizing an agency head or designated person to share classified information with individuals not otherwise eligible to receive it and specifying procedures to be followed. (Sec 4.2(b))

AGENCY COMPLIANCE WITH THE ORDER

In fiscal year (FY) 2006, pursuant to sections 5.2(b)(2) and (4) of E.O. 12958, as amended, my office conducted a total of 15 onsite reviews of Executive branch agencies. Most of these reviews evaluated the agencies implementation of the classified national security information program to include such core elements as organization and management, classification and declassification, security education and training, self-inspections, safeguarding practices, classification markings, and security violations procedures.

Of the general program reviews we conducted last fiscal year, we found that few of the agencies visited had adequately implemented the core elements of the classified national security information program. Shortcomings were observed at multiple agencies in their implementing regulations, self-inspection programs, document markings, and refresher security education and training. It is disappointing to note that these same shortcomings were noted in FY 2004 and 2005. I should note that as a general rule, intelligence community agencies tend to have the most sound information security programs within the Executive branch.

At several agencies, the ISOO onsite reviews identified inadequate support from senior management for the information security program. Sections 5.4 (a) and (b) require agency heads and senior management of agencies that originate or handle classified information to demonstrate commitment and consign necessary resources to the effective implementation of the Order.

An area of significant concern was the failure of agencies to update their regulations that implement E.O. 12958, as amended, even though the Order was amended in 2003. Implementing regulations are essential to the program because they are the foundation for agency personnel in terms of obtaining guidance and procedures pertinent to their individual responsibilities under the Order and the Directive.

As found in FYs 2004 and 2005, many agencies have not established comprehensive self-inspection programs. The primary reason for the shortcomings of these agencies' self-inspection programs were inadequate staffing levels necessary to meet their internal oversight responsibilities and insufficient senior agency official emphasis. Self-inspections are an important element of the information security program because they enable the agency to evaluate, as a whole, its implementation of the Order's program and make adjustments and corrective action, as appropriate.

Refresher security education and training, although an annual requirement of the Order, was not being provided at a few of the agencies reviewed. This training is fundamental to the continuous reinforcement of the policies, principles, and procedures that individuals authorized access to classified information are expected to understand and implement.

In FY 2006, we concentrated much of our compliance reviews on the appropriateness of classification decisions. We focused on evaluating if agencies were correctly applying the Order's standards for originally and derivatively classifying information. Unfortunately, the reviews revealed source information often could not be tracked when "multiple sources" was entered on the "derived from" line of the document classification block. Almost all agencies reviewed were not keeping a list of the source documents with the file or record copy as required by the Directive. In addition, we found a high percentage of documents with an unknown basis for classification, as these documents failed to indicate the authority or basis for classification, thereby calling into question the propriety of their classification. To make clear to the holder the basis for classification and to facilitate information sharing and automatic declassification, it is imperative that multiple sources are listed and the basis for classification is identified when designating national security information as being classified.

Another area of concern was the failure of agencies to review and update their security classification guidance at least every five years or sooner as circumstances require. In large part due to lack of timely revision to classification guides, agencies were still using obsolete X1–X8 declassification markings, which were eliminated by

the 2003 amendment to the Order. As a consequence of this erroneous action, the accuracy and appropriateness of subsequent derivative classification determinations based upon such improperly marked documents is placed in jeopardy.

As part of our onsite reviews, we review a sample of documents to ascertain compliance with requirements set forth in the Order and Directive. A review by ISOO of over 2000 documents in FY 2006 revealed the following:

—Nearly 39 percent had errors with regard to declassification instructions;

—Portion markings were inconsistently applied in over 30 percent of the documents; and

—For over 11 percent of the documents, the basis for classification could not be identified.

An essential requirement of the Order is that only an original classification authority (OCA) is authorized to classify information in the first instance. Thus original classifications can only be made by an OCA, and every derivative classification decision must be able to be traced to a source document or classification guide. The consequence of having so many documents for which the basis of their classification could not be determined is that any future classification decisions based upon these same documents will be equally problematic and their true classification status uncertain.

When an agency fails to effectively implement one or more elements of the classified national security program, it weakens its entire program because each of the elements has an essential purpose that is interdependent upon the others. Implementing regulations set the foundation for the program and establish the agency framework to implement the Order. Deficiencies in regulations lead to gaps in the agency's implementation of the program. Classification guides are a critical tool that prescribes the classification of specific information. They identify the elements of information regarding a specific subject that must be classified and establish the level and duration of classification for each element. Outdated classification guides may reproduce numerous invalid derivative classification decisions, thereby undermining the classification system provided by the Order. It is imperative that classification guides are updated to reflect the changes of the Order and otherwise be kept current.

Security education and training briefings inform/remind agency personnel of their duties and responsibilities and on the proper procedures for creating, handling, and destroying classified information. Inadequately trained personnel are more prone to mistakes while working with classified information. Self-inspections enable an agency to evaluate the implementation of its program on a regular basis, identify areas of concern, and take corrective action, as applicable. The absence of a self-inspection program can leave problems unidentified and uncorrected and eventually place national security information at risk. For an effective program, the various program elements must work together.

## IMPACTS OF OVERCLASSIFICATION

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 our most sensitive secrets at needless increased risk.

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

Classification is an important fundamental principle when it comes to national security, but it need not and should not be an automatic first principle. The decision to originally classify information in the first instance or not is ultimately the prerogative of agency original classification authorities. The exercise of agency prerogative to classify certain information, of course, has ripple effects throughout the entire executive branch. For example, it can serve as an impediment to sharing information with another agency, with State or local officials, or with the public, if they need to know the information.

The challenge of overclassification is not new. Over 50 years ago, Congress established the Commission on Government Security (known as the "Wright Commission"). Among its conclusions, which were put forth in 1955, at the height of the Cold War, was the observation that overclassification of information in and of itself represented a danger to national security. This observation was echoed in just about every serious review of the classification systems since to include: the Commission to Review DoD Security Policies and Practices (known as the "Stillwell Commission") created in 1985 in the wake of the Walker espionage case; the Joint Security Commission established during the aftermath of the Ames espionage affair; and the Commission on Protecting and Reducing Government Secrecy (often referred to as the "Moynihan Commission"), which was similarly established by Congress and which issued its report in 1997.

More recently, the National Commission on Terrorist Attacks on the United States (the "9–11 Commission"), and the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (the "WMD Commission") likewise identified overclassification of information as a serious challenge.

As I stated earlier, the ability and authority to classify national security information is a critical tool at the disposal of the Government and its leaders to protect our nation and its citizens. In this time of constant and unique challenges to our national security, it is the duty of all of us engaged in public service to do everything possible to enhance the effectiveness of this tool. To be effective, the classification process is a tool that must be wielded with precision. In an audit of agency classification activity conducted by my office over a year ago, we discovered that even trained classifiers, with ready access to the latest classification and declassification guides, and trained in their use, got it clearly right only 64 percent of the time in making determinations as to the appropriateness of classification. This is emblematic of the daily challenges confronting agencies when ensuring that the 3 million plus cleared individuals with at least theoretical ability to derivatively classify information get it right each and every time.

### EFFECTIVENESS OF CURRENT DECLASSIFICATION EFFORTS

Setting deadlines for agency action in implementing the automatic declassification provisions of the Order is essential in ensuring the continued integrity and effectiveness of the classification system, which cannot be depended upon to protect today's sensitive national security information unless there is an ongoing process to purge it of yesterday's secrets that no longer require protection. The automatic declassification process increases the potential release of formerly classified information to policy-makers and lawmakers as well as the general public and researchers, enhancing their knowledge of the United States' democratic institutions and history, while at the same time ensuring that information which can still cause damage to national security continues to be protected. An agency's failure to fully implement automatic declassification provisions undermines its ability to achieve these complementary objectives.

After several deadline extensions, automatic declassification finally became effective on December 31, 2006, with a few notable authorized delays. While a detailed analysis of the final results is still underway, it appears that all Executive branch agencies have succeeded in meeting their obligations under the automatic declassification provisions of the Order. As significant as the initial development of the concept of automatic declassification was, its actual implementation after so many false starts and delays is even more of an accomplishment. It reflects well on the diligence and efforts of both the public servants who accomplished this milestone through their hard work and perseverance, as well as the agencies that committed the requisite resources. I should note to you today the significant leadership and support within the interagency declassification community displayed by the Central Intelligence Agency since 1995.

Significant challenges remain. For example, the Order allows a delay in automatic declassification for up to three additional years (December 31, 2009, for classified records currently 25 years old or older) that contain information of more than one agency or information the disclosure of which would affect the interests or activities

of other agencies. Similarly, automatic declassification for classified information contained in microforms, motion pictures, audio tapes, video tapes, or comparable media that make a review for possible declassification exemptions more difficult or costly may be delayed from automatic declassification for up to five additional years. Improved processes, education about other agency equities and enhanced agency collaboration are necessary to ensure quality reviews with minimal referrals and adequate documentation regarding actual decisions made are essential.

It should be noted that from the perspective of the public, researchers and historians, there is no "vault-full" of previously classified records that became automatically publicly available on January 1, 2007. However, in many regards, the public has already seen the major benefits of automatic declassification. Automatic declassification has served as the impetus during the recent past (since 1995) for many agencies to devote necessary resources for the establishment of substantial ongoing declassification review programs.

During FY 2006, the Executive branch declassified 37,647,993 pages of permanently valuable historical records, which is a 27 percent increase over what was reported for FY 2005. This large increase was primarily due to the final push to comply with the December 31, 2006 automatic declassification deadline. Since 1995, agencies have reported the declassification of more than 1.33 billion pages of previously classified historical records. Only 257 million pages were declassified under the two previous executive orders governing classified information, a period encompassing almost twice as many years.

Furthermore, the infrastructures established by agencies to accomplish declassification reviews since 1995 will continue indefinitely, thus contributing to the universe of declassified information as a new batch of historical records reaches 25 years of age each and every year. However, we are concerned that some agencies may have regarded the automatic declassification deadline of December 31, 2006 as a one-time push rather than an ongoing requirement.

Finally, declassification does not always equate to public access. Documents that have been declassified must still be reviewed to ascertain whether they contain other information that may not be releasable to the public, e.g. personal information. Also, declassified records must be accessioned and processed by archivists before they can be "put on the public shelves." These activities ensure that the National Archives and Records Administration (NARA) has both physical and intellectual control of the records. While some 460 million declassified pages of federal records have been made publicly accessible since 1996, NARA holds another 400 million pages of declassified federal records that require additional processing before they can be made available. To add to the burden, hundreds of millions of pages, both classified and recently declassified, remain within the custody of their originating agencies and will also require processing upon accession into NARA before they are made available to the public.

EFFECT OF SELECTIVE CLASSIFICATION AND DECLASSIFICATION

As I indicated earlier, the decision to originally classify information in the first instance or not is ultimately the prerogative of agency original classification authorities.

Similarly, the Order clearly states that information shall be declassified as soon as it no longer meets the standards for classification under this order, irrespective of the initial duration decision of the original classification authority. The Order goes on to state (section 3.1 (b)) that it is presumed that information that continues to meet the classification requirements under the Order requires continued protection. However, the Order does recognize that in some exceptional cases the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, the Order assigns the responsibility to make such a decision to the agency head or the senior agency official designated by the agency head under the Order. That official is responsible to determine, as an exercise of discretion, whether the public interest in disclosure outweighs the damage to the national security that might reasonably be expected from disclosure.

Again, I thank you for inviting me here today, Madame Chairwoman, and I would be happy to answer any questions that you or the subcommittee might have at this time.

Chairwoman ESHOO. We have been joined by another distinguished member of the full committee of this subcommittee, Mr. Rush Holt, Congressman Holt from New Jersey. I would invite you to make a statement.

Mr. HOLT. I will wait until we get to the questions. Thank you.

Chairwoman ESHOO. Let me once again thank the witnesses. There was a lot of material in your comments.

Let me start with this question, and that is, has Congress ever revised an executive order, I mean, leaned in legislatively to either bolster what is an executive order or to change it in some way, shape or form?

Mr. LEONARD. I think the most recent efforts in that area date back to the mid-1990s where there was the commission on reducing government and improving government secrecy, commonly known as the Moynihan Commission, where Senator Moynihan took the lead.

The major thrust of that commission and their findings was to give a legislative basis, if you will, to much of the executive order. That is one of the many recommendations of that commission that actually did quite a bit of effective work that really has not seen the light of day.

Chairwoman ESHOO. Maybe all three of you want to lean in on this. What in your view are the costs of overclassification? I mentioned, obviously, a big one. I mean, what we have learned from September 11th 2001. But if you would like to comment on that, fill it out.

I think it is an important thing for us to be made very well aware of because the tendency is and the number of pages declassified recently are really abysmal when you look at Ms. Fuchs' chart. Who would like to take a stab at that?

Ms. FUCHS. Well, I mean, I think the costs of overclassification are myriad and in some respect they may be hard to identify because we don't know what the secrets are that we haven't heard of. But certainly in a situation where things are classified that shouldn't be classified, it leads to disrespect of the system, and I think that is one of the reasons there have been so many incredible leaks to the press in the last couple of years, because so many important things including important policy choices are classified, and that limits dissent. So I think it leads to more leaks.

I also think it makes the public suspicious. This is the United States of America. This is a democracy. We citizens feel proud we live in a country where the Congress and President are supposed to be responsive to our concerns.

That doesn't happen everywhere. In how many other countries could you see their intelligence agency releasing the skeletons in the closet, the "family jewels"? That is something that we need to preserve because that makes our country special. If we allow secrecy to go unchecked, then we are not going to be like that any more.

Chairwoman ESHOO. I think that is one of the most obvious ones. It is a very important one.

Mr. Aftergood or Mr. Leonard, do you want to add anything?

Mr. LEONARD. Clearly, I think most people would recognize that the best policy, the best solutions always come about after a robust and full exchange of ideas and a full exchange of information. Classification in and of itself guarantees that you will never achieve that optimal level because you, by definition, are restricting your input, restricting the deliberation of whatever.

So there are many times where that is a price we have to pay. We have to accept a sub-optimum outcome because we need to deny information to those who would use against information against us. But when we sign up to a sub-optimal outcome needlessly and deny that full and robust change——

Chairwoman ESHOO. What do you think is the most important tool for what you just described?

Mr. LEONARD. To preclude that from happening?

Chairwoman ESHOO. The misuse of it.

Mr. LEONARD. The most important tool is we literally have to change the culture, because right now we have a culture where people rightfully are held accountable both administratively and criminally when they improperly disclose information. But I dare say I have a hard time identifying a situation where anybody has ever been held accountable for improperly restricting information.

The system is out of kilter in that regard. We need to get it right each and every time from both directions, and until we come up with a means by which to hold people accountable for inappropriately hoarding information or inappropriately and needlessly restricting the dissemination of information, we will always have that tilt to, when in doubt, withhold.

Chairwoman ESHOO. Is it your agency that in some ways—maybe this is a stretch to describe it this way. Do you act in some way, shape or form as kind of an IG looking over the shoulder of the executive and making sure that the executive order is carried out? Is there any Checkpoint Charlie besides the House Intelligence Committee, the Senate Intelligence Committee? Really so much of this rests with the executive branch.

Mr. LEONARD. Ultimately, the decision to classify is a judgment and an act of discretion.

Chairwoman ESHOO. The oversight and implementation of many of the things that you have in your written statement.

Mr. LEONARD. That, from my perspective, is what is lacking. Because my office, the role we play is we will look and say, is the decision—is it made in accordance with the standards, which is different than asking the question was it the right decision.

One of the things that I have long advocated is assigning to a rather senior official within agencies that role to be the advocate for challenging classification decisions where we actually inculcate a culture where people can challenge what they perceive to be inappropriate classification decisions and serve as an advocate for ensuring that the proper judgment is brought to these types of decisions.

Chairwoman ESHOO. Kind of hard to do when we talk about having to change the culture in order to make this happen, though. Sometimes the most effective keepers of the culture are the people that are at the top, and then we would want them to review and make sure that they are essentially being the devil's advocate and check on the system. It is difficult, but I appreciate what you are saying.

Mr. Aftergood, did you want to add something?

Mr. AFTERGOOD. I would endorse both what Ms. Fuchs and Mr. Leonard said, and I think it is true that you need to change the culture, but I don't think it is particularly helpful to put it that

way because it is too diffuse of a goal. Instead, I think we ought to focus more on nuts and bolts questions of how do we actually increase the oversight in a meaningful way.

The President's executive order delegated the only real oversight function to Mr. Leonard's organization, which is an office of perhaps 20 or 30 individuals at the National Archives responsible for overseeing a system of perhaps 3 million people holding clearances and tens of thousands of government officials. So, obviously, it is an oversight system that is not designed to fulfill its declared function.

Okay, so what do you do about that? One thing you can do about it, without getting too grandiose or thinking about something too ambitious, is to expand the number of individuals whose job it is to perform oversight.

How do you do that? Well, most intelligence agencies and other government agencies have inspectors general housed in their agencies. In the intelligence agencies, they all hold clearances. Why not ask them as part of their routine functioning once a year, or more often, periodically do an audit of classification and declassification activity.

Now they may find that they are not classifying enough or they are classifying too low. It doesn't matter. Have somebody whose job it is to think about the proper functioning of the classification system. Let them do an independent audit. Because the IGs are already housed in the agencies, they are less likely to engender the opposition that somebody from way outside the agency is automatically going to generate.

Chairwoman ESHOO. Culture is already accustomed to them.

Mr. AFTERGOOD. Some are already doing it on an ad hoc basis.

But if this subcommittee were to ask each of the intelligence agency IGs, saying, look, we want you to once a year do an audit of classification practices, report to us, preferably in unclassified format, do it every year, and then see what happens.

Chairwoman ESHOO. Very helpful. Thank you.

Mr. Issa.

Mr. ISSA. Thank you very much, Madam Chair.

I am going to try to be tough to get some answers here, because I think there is a couple of things I want to get clear answers for the record on, and I think Director Leonard will probably answer most of these.

Director, do the North Koreans, the Cubans, the Iranians, do they declassify and put on the Web anything?

Mr. LEONARD. Not that I know of.

Mr. ISSA. Did the Soviet Union ever do that during its existence?

Mr. LEONARD. Not that I am aware of, no, sir.

Mr. ISSA. Does Russia currently maintain a high level of secrecy, again, vis-à-vis Putin's announcement that he had secretly done a new level of nuclear weapon while we were paying under Nunn-Lugar to clean up his old weapons?

Mr. LEONARD. Probably a fair statement.

Mr. ISSA. So, in fairness to ourselves, from all three of you, please, to the extent that we do this both publicly and internally, we are, for all practical purposes, the only nation doing it, is that correct? We are the only major nation that has major secrets that

makes anything close to this amount public as a matter—I am not trying to pat us on the back. I think we have a lot of room for improvement. But I want to have us all do a reality check, which is the bad guys do not participate in this and we have had no luck at getting them to participate. Is that a fair statement?

Ms. FUCHS. I think it is fair to say that we are doing a much better job than all those countries we would never want to emulate, that is correct.

Mr. ISSA. Let's go a little further. Has France told us——

Chairwoman ESHOO. Did your daughters hear that?

Mr. ISSA. They left. I waited to get tough.

Has France—France is one of the three greatest spies on us: France, China and Israel. Common knowledge.

Mr. AFTERGOOD. The United Kingdom does a lot of declassification.

Mr. ISSA. Has France told us what they did to spy on us, Israel, or has China told us what they did, the three biggest spies against us? I am not an expert on this. Have we found out what they did 25 years ago by their putting it on the Web?

Ms. FUCHS. I think there have been times when other countries have declassified important information. For example, my organization has sought a lot of information about the Cuban missile crisis; and we were involved with organizing a conference held in Cuba at which former Soviet officials, U.S. officials and Cuban officials attended. And thanks to our efforts to unleash information from the U.S. Government, Fidel Castro actually came to the conference with a stack of papers which showed what Cuba knew was going on at the time of the Cuban missile crisis.

So it happens. I certainly agree that we have made much more of an effort than other countries.

Mr. ISSA. That was really setting it up for the major question and that is one from this part of this hearing is probably our first priority. Ms. Fuchs, from your part, it might be not the first.

Today, the biggest concern I think on the dais—and I am asking for input on this—should be the fact that stovepiping exists, that overclassification that prevents the 3 million people who have security clearances at various levels are unable to get the equivalent of CREST in a classified world so that they know what they don't know. Is that commonly agreed to the extent that you each know about it, particularly Director Leonard? I know you would be more aware of just how much stovepiping there is.

Mr. LEONARD. The classification system in and of itself is an impediment to information sharing, especially third agency rules and things along those lines, yes, sir.

Mr. ISSA. So when we deal with Confidential, For Official Use Only, Secret and Top Secret, we are dealing with the peanuts. Realistically, if this committee is to do its best work, wouldn't we first start with Compartmented, where it is not available to other security agencies even when they have a valid need to know because they don't know that it exists? If we are trying to prioritize some of our highest priorities, would that be fair to say?

Mr. LEONARD. Writing intelligence for the consumer, either taking code word information and writing it to the collateral level, to

the confidential secret level, or writing it to the unclassified level for the uncleared state and locals, yes, sir, that is clearly——

Mr. AFTERGOOD. I would just add there is a cluster of problems here that are slightly different, but they are also related. Disclosure to the public is a different issue than information sharing within the government. Nevertheless, some of the solutions overlap.

For example, the tear-line approach where you segregate information by classification level, you separate out the compartmented stuff from the collateral secret stuff from unclassified stuff. If you do that, you can share both widely within the government, you can also perhaps disclose to the public, and it also facilitates declassification at the end of the document's lifetime.

Mr. ISSA. That is exactly what I was getting to. If we can force the community which we have oversight on to adhere to existing requirements that they in fact begin creating what we all know from doing word processing, sort of the bold lines that we see when we do edits so that when you send back a document, they know what you edited, et cetera. We implement that same basic technology to the basic levels of security. Then we should, as an oversight agency, be able to scan a great deal of information at a level before we ever start asking for the little piece that is essentially redacted but in a digital world redacted in a different way.

Mr. AFTERGOOD. If I could make one practical suggestion. Rather than attempting to change the practice throughout the entire community, which, again, may be too ambitious and may generate automatic opposition, I would suggest it might be tactically wise to break the problem up into smaller pieces and to begin—you mentioned in your opening statement the National Intelligence Estimate that was unable to be shared. Why not begin with the National Intelligence Council and tell them, look, in the future, we want all of your NIEs to be prepared in a tear-line format so that at a minimum, even if they are classified, the noncompartmented portions can be shared widely with Congress, cleared staff and so forth.

Mr. ISSA. You just scored a home run for something I think we can implement as a result of this hearing.

Mr. AFTERGOOD. I should add that that may be the staff director's idea, because we were discussing that prior to the hearing.

Chairwoman ESHOO. You can share it.

Mr. ISSA. We have always found those to be solid. I am going to ask you a tough question, and my time is running short.

Chairwoman ESHOO. It is up, but you can have more time.

Mr. ISSA. Thank you. I will be brief, though.

Because if it goes to a level of declassification, Mr. Aftergood, since your bio gives me the in, I will use it. I always love using people's bios. One of your claims to fame was in fact when you sued the government to find out that the intel budget in 1997 was $226.6 billion. Quite an accomplishment to get a number for the first time.

In your estimate, to the public what breakdown of the right to know below that number do you think is appropriate? I take it from each of you. In other words, I will give you some real quick hypotheticals. Should we break it down by overall agency, by re-

gion, by counties? Should we break it down by how much we pay the operative A, B, C? Where do you draw the line?

I ask you that because you did quite a breakthrough, but we also have to know from our standpoint where the community would draw the line, where you would draw the line.

Mr. AFTERGOOD. If your question is, if I were President, how much would I declassify, then I think I don't see a problem with declassification of individual agency budgets, totals, in other words, figures for individual agencies. I am not the President.

Mr. ISSA. I am not a Senator, so I am not even going to be one.

Mr. AFTERGOOD. I accept the fact that all—that there is a bare consensus represented by the 9/11 Commission and others that the total budget for the national intelligence program should be disclosed but nothing beyond that. And I would note that when the budget was declassified by the Director of Central Intelligence in 1997 and 1998, the one number was released and it did not lead to a hemorrhaging of further detailed secrets. In order words, the system was perfectly capable of drawing a line. It would not have been the line that I would draw necessarily, but it was a line that was drawn and was adhered to.

Mr. ISSA. Thank you.

Thank you, Madam Chair.

I might note for the record that every Member of Congress has the ability to go up to the Crypt, not just those on the committee, and see a considerable level of detail of dollars by agencies and so on. That is a right every Member of the House and Senate has, and it also hasn't led to hemorrhaging of the public hearing how much a particular program goes to.

Thank you.

Chairwoman ESHOO. Thank you. Excellent questions.

Mr. Holt.

Mr. HOLT. Thank you, Madam Chair. Thanks for setting up this meeting and thanks for the excellent staff work. It may have consisted of coaching the witnesses. I am not sure.

But I must say, Mr. Aftergood, you have made several very specific and useful suggestions so far; and I hope we will come out of this hearing with some specific applicable suggestions, perhaps legislative controls that should be imposed or recommendations to agencies.

Recognizing that excessive secrecy is actually a danger to democracy as well as a danger to good decision-making, we have to know where to draw the line. Stovepiping clearly interferes with the appropriate sharing of information that is necessary for good decision-making. It is fairly easy to know when you have erred on the side of failing to classify if someone's sources or methods or identity is exposed and harm comes to them, comes to our country, comes to a program, comes to those who would be assisting our country. But it really is hard in the other direction. I mean, is there a rule of thumb to know that can be applied when there is excessive—when there is overclassification?

That would be for all of you, because it is a general question.

Mr. LEONARD. One of my observations over the years is a good indicator of overclassification is the amount of leaks that occur. As many leakers as there are in this town, there are reasons for doing

it. But one of the things that contributes to leaks is a lack of respect for the integrity of the system where people see information that has markings on it that a reasonable person would question. And when you start having people start substituting their own judgment for the judgment of the process, that is usually an indicator that the process is coming up short.

Ms. FUCHS. I guess I would add that there are audits done of how agencies do their classification decisions, and you can see from those audits that there are problems. I think that is a good recommendation for how to limit overclassification.

When the reclassification of historical records on the public shelves at the National Archives was exposed a couple of years ago, the Information Security Oversight Office did conduct an audit and the Archivist of the United States who held a meeting with officials from all of the agencies who had improperly reclassified information and members of the historical community, including my organization. And at the table I asked the question, so what are the consequences to these agencies for having flouted the executive order that was issued and for having reclassified without notifying the Information Security Oversight Office? The people from the agencies looked at me like I was insane.

Mr. HOLT. That was actually my next question. What sanctions do exist? And I think there are none for overclassification, what sanctions might exist.

I didn't let everyone answer my first question, but if you wanted you could roll the answer of the second question in there.

Ms. FUCHS. I just wanted to finish up. I think that, obviously, the vast majority of people who are keeping secrets or marking them secret are doing it to protect the United States and because that is their job. They are not trying to cause harm. But when it is shown that they have done something wrong, there should be some consequences. There certainly should be retraining. I mean, if they are classifying things improperly——

Mr. HOLT. What sanctions or controls exist against an employee or an office that overclassifies? Is there anything?

Mr. LEONARD. The order and the directive recognizes the need for sanctions but does not prescribe any.

But to build on what Ms. Fuchs indicated, there are some best practices out there that some agencies do. For example, the Department of Energy actually requires a demonstration of a minimum level of competence before someone is allowed to classify. The CIA, for example, requires every classified product to have on it the identity of the individual who signed.

Mr. HOLT. That is training in advance, but is there anything after the fact?

Mr. LEONARD. The nice thing, if agencies require certification, if they require a demonstration of competence, if some of them do audits and demonstrate an inability to get it right, there is an easy way to apply sanctions: Take away your certification. You can no longer classify something. You will have to go to your supervisor or whatever to get classification controls until you get recertified or retrained. That is an easy way, not a debilitating sanction, but it gets people's attention, and I think it actually would work.

Mr. HOLT. In practice, are there regulations or legislation that should be imposed for that to occur?

Mr. LEONARD. Agencies have the leeway right now to do that if they choose. NRO, for example, limits who can assign classification. Most do not.

Mr. HOLT. Do you know of examples where someone's ability, prerogative to classify has been stripped because it was found in an IG report or otherwise they were overusing?

Mr. LEONARD. I believe the DOE, for example, when they see evidence that someone who is trained either as a classifier or declassifier isn't getting it right, at the very least——

Mr. HOLT. Do you think there might be a few examples out there?

Mr. LEONARD. Yes, sir. Only a few. But there are some best practices out there.

Mr. HOLT. You had suggested that the IG in each agency do an audit of classification and the use of it. Does any agency's IG, or other, if not the IG, other agency organization do that now?

Mr. AFTERGOOD. I believe so. I think over the years——

Mr. HOLT. As a regular——

Mr. AFTERGOOD. Not as a regular.

Mr. HOLT. That is what you were suggesting.

Mr. AFTERGOOD. Part of their portfolio, yes.

Chairwoman ESHOO. We are getting some important work done and excellent questions asked.

Mr. HOLT. Following along this line now, not just the training but the process and controls for determining who has the ability and trustworthiness to handle classified information, are those controls appropriate? In other words, how you determine the level of clearance a person has?

Mr. LEONARD. That has been a vexing issue for decades.

Mr. HOLT. That is why we are asking you wise people.

Mr. LEONARD. From a policy perspective, it is identical across the board. From a practical perspective, somehow, some way it doesn't come into reality.

One of the challenges is that, whereas everybody will sign up to the same set of standards for giving someone a clearance at the TS or SCI level, for example, individual agencies will say, okay, that is well and good, but, in addition to that, we have to determine whether you are suitable for overseas posting or suitable for this, and they impose additional suitability requirements, which although technically doesn't affect their clearance, from a practical point of view is the same: I am not going to let you access this information system.

Mr. HOLT. As you answer this, let me throw out a thought that I have had for some time which is the difference among the agencies may not be a bad thing if we use that difference to learn what works and what is appropriate.

Mr. HOLT. If we imposed nationwide or communitywide, you know, one particular way, for example, certain kinds of polygraphs, whatever it is, we might lock ourselves into a decades-long mistake.

Mr. LEONARD. Clearly the standard for someone to be assigned in a national clandestine service overseas needs to be different

than someone who is going to sit, you know, at the Department of Education at a computer terminal. The key is to minimize those differences to ensure that if there is an extra requirement, that it is truly fulfilling a unique need and not just another way of coming up with the same answer to the same question.

Chairwoman ESHOO. Okay. I would like to do another round if you have additional questions.

I would like to just jump in here and ask Mr. Leonard. You mentioned that the Moynihan Commission recommended providing the legislative basis for the Executive Order. Do you have views on what elements should be made statutory?

Mr. LEONARD. The ability to restrict dissemination of national security information clearly is an absolute constitutional prerogative of the President pursuant to Article II, and that has been long recognized by the courts.

So I think the basics in terms of what information is identified, how it is identified, to what level; but then over and above that the mechanics of how agencies implement the President's policies from an overall efficiency point of view, from a point of view of how it impacts upon the mission of an agency and its ability to do that in an efficient and effective way, those nuts-and-bolts-type issues, I think, clearly are appropriate.

Chairwoman ESHOO. Which is really the jurisdiction of this committee and why we are having this examination.

Has Congress ever legislated in this area?

Mr. LEONARD. Congress will on occasion, you know—for example, the first thing that occurs to me is something that has just been reconsidered by the Senate Select Committee on Intelligence. There was a statute passed dealing with clearances of individuals within the DOD and prohibiting the granting of clearances to anyone who had a felony record and spent more than a year in jail. That is something that is over and above the President's policy.

So there is an example of legislation involving classified or access to national security information where Congress has weighed in.

Chairwoman ESHOO. It is an example, but not so much what we are discussing here today, but it is an example of what is legislatively enacted.

Mr. AFTERGOOD. Maybe a more pertinent example is the fact that Congress legislated the classification system for atomic energy information, nuclear weapon design information in the Atomic Energy Act in the restricted data and formerly restricted data, which is essentially a parallel system that was enacted into law by Congress. So when the executive branch says this is a Commander in Chief function, the answer is no, not exclusively, and Congress has demonstrated that.

Now, for myself, I think I would caution against this line of—this pursuit, because I remember 10 years ago testifying with Mr. Leonard—he was then at the Department of Defense—before Senator Fred Thompson's Governmental Affairs Committee on something called the Government Secrecy Act of 1997, which was a proposed bill to essentially legislate a classification system. Now 10 years later, there is no Government Secrecy Act of 1997 because it never went anywhere.

And I think, for me, the lesson is that sometimes when you are too ambitious, you end up getting nothing done. And in retrospect I think a lot of that work done then was wasted effort. And I, for myself, I would rather see incremental changes that really are adopted this year and next year and the year after that, and then we will be way, way ahead of the game rather than, you know, trying to legislate a whole classification system.

Ms. FUCHS. There is one area that Congress has legislated that relates to this in the National Security Act. It puts the obligation on the Intelligence Community not to disclose sources and methods, and that is one area whereas the most important area in many ways with respect to classification, and we see it throughout all sorts of secrecy and disclosure decisions.

But it is also something that the Moynihan Commission touched on, and it is an area—there is frankly not much definition in the law about what sources and methods means and what it is intended to protect, and it is an area where—from the perspective of our advocates—where we say the Intelligence Community has been extreme in its protection of entire documents based on the fact that they derive——

Chairwoman ESHOO. How do you know that if it is a secret——

Ms. FUCHS. Frankly, sometimes we see documents that are disclosed at different times with redactions, so you know, in fact, what was redacted. That is one reason. I mean, in addition, you mentioned—Ranking Member Issa mentioned Mr. Aftergood's litigation against the government involving the intelligence budget in which they said the intelligence budget itself is a method.

I wouldn't draw on that case as an example of extreme points of view, but they have also said that the process of briefing the President, the fact that the CIA briefs the President on intelligence matters is a method. Well, frankly, it is the one method that we all know exists. Former DCI Tenet talked about it extensively in his recent book. The current Secretary of Defense talked about it in his book. President Clinton has talked about it extensively. It is no secret, and yet it is a protective method from the perspective of the CIA.

So there is some extremism there and something that I think, given that it is in the National Security Act, is something that Congress could consider looking at.

Chairwoman ESHOO. Thank you very much.

Mr. Issa.

Mr. ISSA. Well, I think the secret is you can sell books if you keep it a secret, and it seems like it is a bipartisan thing to do.

A couple of questions, and I don't expect full answers today, but I think this is going to go beyond this, and I appreciate your responses as you reflect on this.

You said baby steps and—you didn't say baby steps. I took that word out of it. Yours was redacted.

Mr. HOLT. Incremental changes.

Mr. ISSA. Yes. Baby steps is what it changes to. And I think you are right.

I think the history of great bills that didn't happen or even medium-sized bills that never got implemented tells us we need to

find progress in a relatively short period of time, less than one Presidential term at a minimum.

And so would you support, and this is for each of you, a significant change in the bias of classification, meaning sunsetting of initial classifications, so that any classification would, by definition, have to be reclassified, or it would drop a level—these are levels above Top Secret—so that you would never have a 25-year unless it was looked at repeatedly? Basic conceptual change that—and we are not going to discuss every level and how many years it would be authorized, and who would authorize, and what level it would take above this initial classifier to essentially reassess it, but the basic concept that just throwing "Top Secret Codeword blank" does not make it go away for 25 years because nobody knows about it.

And then at a certain level, well below the levels I have described, do you believe that we should implement and fund a national security database that, by definition, is where materials below a certain level within the community would have to be made available, including—and I think the current that is most important today and what I learned today—those portions of communications which, in this tier-sheet-type environment, are, in fact, at that level? So, you know, at least portions of—at least the fact that we met on a Monday morning at 8 o'clock would be there even if it couldn't say that we met with the DNI.

Those are the three questions. I will take briefly any answers or thoughts that you have and the rest for the record, and I would appreciate it.

[The information follows:]

RESPONSE OF STEVEN AFTERGOOD

Rep. Issa's suggestions for a change in the bias of classification, including an automatic sunsetting of initial classifications after a set period of time, and for establishing a national security database to encourage sharing of classified information merit careful consideration.

But I suspect that these proposals are too abstract and incompletely defined to be implemented as described.

President Nixon's Executive Order 11652 included an automatic classification downgrading schedule that resembles Rep. Issa's concept. But it did not achieve its intended purpose. (President Clinton's EO 12958, as amended, has been somewhat more successful with its automatic declassification provisions.)

As for the national security database proposal, various interagency databases involving classified information have reportedly failed to fulfill their potential, because agencies have declined to fully participate in sharing their information.

So something more or different is required.

Rep. Issa's suggestions might indeed prove fruitful if they were applied within a relatively discrete and homogeneous set of records—say, certain types of intelligence analyses—rather than being applied to the universe of all classified records.

As I tried to indicate in my testimony, I believe "experiments" in classification and declassification policy should be encouraged at the pilot project level. Proposals like Rep. Issa's and others would be worth testing in practice to discover what works.

RESPONSE OF MS. FUCHS

Thank you for the opportunity to respond to the open questions. In my view the implementation of automatic declassification for 25 year old records still has the potential to transform the system by pushing aside secrecy fetishes that have been permitted to exist for decades. As the community learns that historic material can be released without harm, there may be a greater willingness to share current information within the intelligence/law enforcement/homeland security communities. Having said that, automatic declassification has not resulted in the disclosure of much information because all the records still have to be reviewed for other sen-

sitivities, such as privacy, and because many agencies have been able to obtain file series exemptions from automatic declassification.

Although I think it would be helpful to have a system that involves regular review to determine whether classification status should be maintained or dropped, as Mr. Issa suggests, it may be impractical. Thus, the fall back of having initial classification decisions be limited in their duration is important. In addition, having a system of downgrading classification levels is useful. It is also critical to prevent initial overclassification. Thus, requirements that records be created in unclassified format or with unclassified versions would alter the mindset that Mr. Issa referred to—the one that looks as classification as a locked closet where secrets will disappear forever. It would force agencies to explain their policies, practices and activities in a way that could be shared and debated. It would also make it possible for the agencies to share information with their State, local, tribal and private sector colleagues unencumbered by concerns about secrecy. If such unclassified records were required and created in every instance, then the national security database suggested by Mr. Issa could serve a useful purpose. Without a requirement that records be created in unclassified form, however, such a database could be ineffective and misleading.

RESPONSE OF J. WILLIAM LEONARD

While the goal of such a recommendation is commendable, on a practical basis it would be difficult to implement. In an information sharing environment, we want to encourage the appropriate sharing of classified information. However, in the current environment, the originator of the information will never know all the places where the original information eventually ends up. Thus, it would be exceedingly difficult and resource intensive to notify holders of the information as to the results of these periodic reviews of the appropriateness of continued classification. The vast majority of classified information can be declassified well before 25 years and this reflects the actions of agencies as well. For example, in FY 2006 agencies made 231,996 original classification decisions of which nearly 61 percent were assigned a duration of ten years or less. However, I believe that too much information is exempted from declassification after 25 years and that a solution is to carve out a more narrow exception than what is currently in effect as to what information can be kept classified beyond 25 years. I do think we should establish a national security database and I believe such a goal is an integral part of the President's direction to establish an information sharing environment which links people, systems, databases, and information of Federal, State, local, and tribal entities and the private sector to facilitate terrorism information sharing, access, and collaboration. Once such a system is established, it potentially could alleviate the impediments to implementing the recommendation for a relatively short sun set date for classification decisions.

Mr. LEONARD. I think the thing on duration is that is something that is long needed, but it is also the hardest nut to crack.

My personal perspective, I think we have a much more simplified scheme. There is the core things we have to protect for a long period of time: identity of human sources, cryptography, those sorts of things. But I think we could come up with a very narrow universe, put those aside, and then come up with a greatly simplified scheme than what we have now, which, quite frankly, I think ultimately is very—is very difficult to administer.

Mr. AFTERGOOD. It is a pity that the ODNI representative is not here, because these are good questions to air with——

Mr. ISSA. They won't go into it either when he is finally there.

Mr. AFTERGOOD. You know, I think there are some rudimentary equivalents of the kind of database you are describing whether it is Intelink or some other version of it.

Mr. ISSA. The good news of it is we have lots of them; the bad news is we don't have one.

Mr. AFTERGOOD. Well, I think some investigation is required to understand the dynamics behind that, why did it unfold the way it did, why are people not putting much of their information in it and so on.

So I think the question is a good one to ask. I think it needs to be fleshed out with some more research into why the system behaves the way that it does. I don't personally know the answer.

Ms. FUCHS. One thing I might suggest in considering those types of suggestions is also speaking with Ambassador MacNamara, who is the program manager of the information-sharing environment which is housed at the ODNI, because he is—one of the things that he is looking at is how to deal with unclassified information that should be shared, but is also getting caught up in similar things, similar types of problems. So I just wanted to add that as a suggestion because they have some very useful ideas.

And I just wanted to respond on the duration of classification. I mean, I think that our perspective is that automatic declassification, which was in Executive Order 12958 and was retained what it was amended, set a very important standard and forced agencies to confront the issue of old information. And so I think that limiting the duration of classification is an important standard.

My understanding is that it is sometimes confusing when there is multiple time periods, and so it may be, I think as Mr. Leonard suggested, that some work needs to be done to figure out how to do that effectively. But it is a very, very effective and useful tool.

Mr. ISSA. My time has expired, but I was speaking to the fact that, for example, Presidential classifications don't expire even when a President does; that we have, in fact, deep dark secrets for very long period of time without needing a new signature, a new initial. And I, for one, assume that the—and I will just give you a little life briefing from my background. I found that if you didn't open up the HR manual in your company and you didn't make chief executives initial it once a year, they didn't know what was in it, and ultimately they didn't make the changes that needed to be made.

And so that is the reason that I personally will be supportive of any effort we can have to get well below 25 years, and that the higher a classification, the more often there needs to be an affirmative act to say this needs to be kept as a secret not just from the public, which I realize is part of today's hearing, but from the interagency process, which is what will protect us from the next 9/11 if we have it and will cause another fiasco if we don't.

Thank you, Madam Chair.

Chairwoman ESHOO. Thank you for your excellent questions and your observations. This is what makes a hearing one of the most important tools for Members of Congress.

I would like to ask Ms. Fuchs a question if I might—and then I am going to go to Mr. Holt, and then I think we are going to wrap up because we have been at this for almost an hour and a half, and it has been a very, very worthwhile hearing, and you have made it so. In your written testimony, Ms. Fuchs, you talked about the fact that the law requires release. And something that jumps out is that under FOIA, the agencies are supposed to respond to a request for documents within 20 business days, and yet it took FOIA delays of up to 20 years to actually bring out the information.

What is it in the system that allows information that should move and be available in 20 days take 20 years?

Ms. FUCHS. Well, there is a lot of excuses that the agency has for why it takes time. Certainly some of it is resources, and certainly it is not a priority to respond. The agencies——

Chairwoman ESHOO. Most people in the country think the government has adequate resources, don't you think?

Ms. FUCHS. Well, the agencies that take the longest time do tend to be the agencies that have the most sensitive information, but that is not always so. Some agencies disregard their information and never respond to the requests. They destroyed them indeed before responding to them.

We have had several letters from the Treasury Department asking us if we could resend FOIA requests that are a decade old because they destroyed them and never responded to them. So some of it is disregard for the public.

But I think that—there is actually a bill pending right now in Congress, it has passed in the House and it is pending in the Congress, that tries to make an effort to put more pressure on agencies to respond, because the only thing that the public can do is to go to court and sue.

Chairwoman ESHOO. Do you think it is an effective piece of legislation to effect the outcome that you described in your written testimony?

Ms. FUCHS. I think the legislation is designed to have more accountability about the delay, and, in fact, by exposing the delay, that is part of the reason the CIA released this. We actually got a call from the CIA before it was released and they said, you know what? All of the publicity you made about our delays and our backlogs has really gotten us to look at them, and they told us they reduced their backlog of 120 old cases down to 60, this being one of the cases. I think exposure of the problem has been very significant.

Chairwoman ESHOO. I think the exposure on both kind of bookends in this.

And I started out by highlighting that because the key agencies in our government did not share information. We know what the upshot of that was. And then the other bookend that we have just talked about. I think for the average person in the country, when they heard the word "declassified," it means let us just spill our secrets. It is much broader than that. It is much broader than that. And that is really not what this hearing is about.

But I restate it because I think that the naive citizen side of me moves to that sensibility when I hear the word "declassified." And its action, as I said, it is far broader. I think it is really important to examine.

I think you have been outstanding witnesses.

Let me ask Mr. Holt if he has more questions.

Mr. HOLT. I do.

Just to follow on Ms. Eshoo's comments about freedom of information. The classification for official use only seems to be used on occasion to shield things from freedom of information release. Do you think, in fact, it has been used that way? Is that an appropriate use of that classification?

Ms. FUCHS. I guess I would say that I do believe that it has been used that way, and it is an inappropriate use of that classification.

I mean, "for official use only" is something that agencies put on their records as a matter of managing their records within the agency. And I think it is perfectly acceptable for them to come up with ways to decide how to disseminate the records in the agency. But when it comes to a FOIA request, they have to look at the contents, not the label, and decide whether or not it should be disclosed to the public.

Mr. HOLT. Regardless of whether it is for official use only or——

Ms. FUCHS. Almost every record they are creating is for official use. It is for the agency's business. When they create things for public use, they put them on their Web site and inform the public and help the public. But the fact it is for official use only is meaningless when it comes to the FOIA.

Mr. HOLT. Earlier you mentioned the Atomic Energy Act.

How well do you think that classification system has worked? What do you think of the idea of Born Secret as a category, and doesn't that lead to some kind of curious retroactive classifications that are, it seems to me, sometimes nonsensical? And you can explain maybe what you mean by retroactive classifications.

Mr. AFTERGOOD. Well, the answer to the question really depends on how broad a framework you want to put it in. The purpose of the atomic energy classification system is essentially to minimize nuclear weapons proliferation. Arguably it has done a fair to middling job of achieving that goal, you know, over the past 60-plus years. It has not been perfect. And in any event, much of the knowledge which it was designed to protect has been independently generated or replicated outside of the confines of the restricted data system.

How well has it worked? You know, there have been different eras where it has been horribly abused. A decade ago we had a big revelation of human radiation experiments conducted under a cloak of atomic energy secrecy. There have been enormous backlogs. There still are many hundreds of millions of pages of restricted-data documents awaiting processing.

You know, I would say it suffers from many of the same pathologies that the regular classification system does, and it requires much of the same oversight that the regular classification system does and hasn't really gotten it.

Mr. HOLT. Any comments about the kind of Born Secret or retroactive classification?

Mr. AFTERGOOD. The term "Born Secret" does not literally appear in the Atomic Energy Act, but it refers to the idea that any information generated, wherever it may be, that is within the confines of the Atomic Energy Act is controlled by it.

Mr. HOLT. The reason I am asking that is to find out whether that concept should apply to sources and methods in the Intelligence Community.

Mr. AFTERGOOD. No. I think it is a dangerous concept that can be easily abused, and it is not a good model.

Mr. HOLT. Either of you? Any comments on this?

Mr. LEONARD. I am—I am a long advocate that classification should be an act of discretion and represent informed judgment. So——

Mr. HOLT. Now, what about declassification? Should that be automatic? Is a 25-year period appropriate? I mean, if the actual declassification should be discretionary, should there be automatic declassification?

Mr. LEONARD. Yes. Again, taking off the table which—again, the human source identity, cryptography, those types of things. The vast amount of information is time-sensitive, and the sensitivity of it is entitled to the passage of time.

Mr. HOLT. And should that time period be discretionary, or should we have a flat decade, two decades?

Mr. LEONARD. The current Executive Order isn't discretionary because it says information will be declassified as soon as it no longer meets the standard of declassification irrespective of whether it is 25 years old or 2 years old. So the pull there and the challenge is to how to find a way to make it effective.

Mr. HOLT. Under Executive Order 12958, it is required that the executive branch keep data, make data available about what is classified and how it is kept and that sort of thing. There have been revisions of this over the years, or at least one revision I know of, and I think there is another revision under consideration.

What is the purpose of that, do you think, or what is—what should be the purpose of that recordkeeping and disclosure to the appropriate agency then to——

Mr. LEONARD. From my perspective, Congressman, it boils down to this: The purpose of the framework is to protect the substance of the information. And clearly the substance of the information is what we need to keep secret.

The way that system works, though, is that traditionally the process that we use to keep it secret has been transparent. We openly publish the rules that we follow. We openly publish the number of times that that process is invoked. We openly publish the number of individuals who are assigned the authority to invoke that.

When you start taking that process and putting that process behind a cloak of secrecy, I really believe we are starting to—it is very unfortunate, because what makes this system work is not the safe, it is not the alarms, it is not the markings on documents. What makes it work is the faith and confidence of the cleared community that is dependent to make it work day in and day out. And what makes it work is the faith and confidence of the American people that the government makes the decisions and applies this process that is being done uniformly, consistent and in accordance with standards.

And if we evolve to a system where the process becomes secret in and of itself, I think that will degrade that confidence and degrade both the cleared communities and the American people's confidence and the integrity of the process.

Mr. HOLT. Now, the disclosure of the information of the processes and about how classified information is kept and so forth, the disclosure of the national archives and records, to whom should that apply?

I know there is a dispute right now, you know, to whom the Executive Order actually does apply, and the Vice President is saying, it does not apply to me. But so we can talk about how this is actu-

ally written and how it has applied. But in order to accomplish what we are trying to accomplish, what you think that it should accomplish, to whom should it apply? Everyone?

Mr. LEONARD. I think—I think from the perspective of maintaining the integrity and the effectiveness of the system, yes, it has to apply to everyone, because quite frankly, when it applies to some and not to others, it degrades the overall integrity, and people start to wonder, well, you know, why does it apply to me but not somewhere else?

Mr. AFTERGOOD. I think the problem is actually even worse than you are suggesting. From my point of view——

Mr. HOLT. I am trying to be diplomatic.

Mr. AFTERGOOD. I think it is fine if the Executive Order says that the Vice President must report his classification activity to Mr. Leonard, as Mr. Leonard believes that it does. I think it would also be fine if the President were to design an order of, I don't want this reporting requirement to apply to the Office of the Vice President and amended the order accordingly.

What is not fine, however, is for the Vice President to simply set aside the literal, the plain-text reading of the Executive Order and to defy it.

What is also not fine is for the Attorney General, who is required by the Executive Order to adjudicate disputes over the interpretation of the Executive Order, to abstain and to be silent.

Mr. HOLT. So you don't think there is ambiguity that needs to be resolved legislatively? You think it is unambiguous?

Mr. AFTERGOOD. Mr. Leonard thinks it is unambiguous, and he is the official who is designated by the President to implement and oversee the Executive Order. He could be wrong. The Attorney General could say he is wrong. But we have got a situation where the Executive Order is, in effect, being ignored, and that is dangerous because it undermines the integrity of the whole system.

I think, you know, if the President were to amend the Executive Order and say the Vice President is not subject—or if the Attorney General were to say, I have determined that the Vice President is not subject, then the integrity of the system would be preserved. Right now it is in danger of being just undermined.

Mr. LEONARD. I think it is important, this point is important, at least with respect to any issues my office may have raised. I have never raised any issues with the issue of the Vice President, the issues that have been raised.

Chairwoman ESHOO. Isn't that issue the other way around?

Mr. LEONARD. The issue has been with respect to the Office of the Vice President, the public servants just like me who——

Mr. HOLT. I was using shorthand.

Mr. LEONARD. But I think it is an important distinction because there is—you know, for example, the President has a National Security Adviser and a National Security Council staff who advises him on national security matters, and that activity has routinely been transparent in its reports and what have you.

And the OVP does an analogue to that. There is a National Security Adviser and people who work along those lines as well, too. So that is one of the challenges of that, in my own mind, is trying to square the two in terms of understanding how they differ.

Mr. HOLT. And the National Security Adviser apparatus in the President's office has been transparent in previous administrations also.

Mr. LEONARD. In previous administrations also.

Mr. HOLT. And the Vice President's analogue has been transparent in previous administrations.

Mr. LEONARD. And up until 2002 in this administration.

Ms. FUCHS. I just wanted to add, speaking as a citizen, I mean, Mr. Aftergood said he thought it would be fine for the President to exclude some offices from these requirements of the Executive Order, but, frankly, I have always understood the Information Security Oversight Office in part trying to make sure that real secrets are properly protected. And so to me, as a policy matter, it seems like it makes a lot more sense to make everyone report and require everyone to be subject to inquiry as to whether they are, in fact, protecting secrets properly.

I am of an advocacy group that wants to know what the government is doing, but we don't want the real secrets to get out either. We want proper protection for things that should be secure and open with respect to things that are not sensitive.

Mr. HOLT. That is a good note for me to end my questioning.

I want to thank you all for some good insights, some things I think we can work with, and I thank the Chair for organizing this.

Chairwoman ESHOO. Thank you, Mr. Holt, who is always thoughtful in his questions and drills down, and then the experts respond in kind.

So I want to thank each one of you. I think this has been a highly worthwhile hearing. I have learned a great deal myself, and I think that, as Mr. Aftergood said, there are clustered—there is a cluster of problems, but there is an overlap in terms of the solutions. And I quote that because I think that is—that you have given us excellent proposals for us to address the different concerns that have been raised during the hearing.

The issue of beginning with an NIE at the NIE Council, the role of the IGs inside the respective agencies. I am a bit more confused now about the Executive Order relative to the executive branch and how the Office of the Vice President has somehow separated themselves from this Executive Order. I am not quite sure who is—how that is reviewed or addressed, but maybe we can leave that to another day.

Mr. HOLT. And, Madam Chair, let me just say, on that subject, I certainly don't agree with the Vice President, Director Leonard. that your agency should be abolished.

Chairwoman ESHOO. Ditto. Very good.

Mr. HOLT. Thank you, Madam Chair. That is for the record.

Chairwoman ESHOO. So you have been most helpful to us. I hope that we can come back and extract more ideas and information from you either in the hearing setting or our staff working with you, and as I use the word "staff," I would like to acknowledge the important role, key roles, that they play really. Without them we could not do the kind of work, quality of work that we hope to produce for the American people both for the Minority side and the Majority side. We are all in this together.

So with that, this hearing is adjourned.

[Whereupon, at 2:40 p.m., the subcommittee was adjourned.]

○