AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. Hrg. 110–431

GOVERNMENT-WIDE INTELLIGENCE COMMUNITY MANAGEMENT REFORMS

HEARING

BEFORE THE

OVERSIGHT OF GOVERNMENT MANAGEMENT, THE FEDERAL WORKFORCE, AND THE DISTRICT OF COLUMBIA SUBCOMMITTEE

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

FEBRUARY 29, 2008

Available via http://www.gpoaccess.gov/congress/index.html

Printed for the use of the Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE

41–454 PDF WASHINGTON : 2008

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

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
THOMAS R. CARPER, Delaware
MARK L. PRYOR, Arkansas
MARY L. LANDRIEU, Louisiana
BARACK OBAMA, Illinois
CLAIRE McCASKILL, Missouri
JON TESTER, Montana

SUSAN M. COLLINS, Maine
TED STEVENS, Alaska
GEORGE V. VOINOVICH, Ohio
NORM COLEMAN, Minnesota
TOM COBURN, Oklahoma
PETE V. DOMENICI, New Mexico
JOHN WARNER, Virginia
JOHN E. SUNUNU, New Hampshire

MICHAEL L. ALEXANDER, *Staff Director*
BRANDON L. MILHORN, *Minority Staff Director and Chief Counsel*
TRINA DRIESSNACK TYRER, *Chief Clerk*

OVERSIGHT OF GOVERNMENT MANAGEMENT, THE FEDERAL WORKFORCE, AND THE DISTRICT OF COLUMBIA SUBCOMMITTEE

DANIEL K. AKAKA, Hawaii, *Chairman*

CARL LEVIN, Michigan
THOMAS R. CARPER, Delaware
MARK L. PRYOR, Arkansas
MARY L. LANDRIEU, Louisiana

GEORGE V. VOINOVICH, Ohio
TED STEVENS, Alaska
TOM COBURN, Oklahoma
JOHN WARNER, Virginia

RICHARD J. KESSLER, *Staff Director*
LISA POWELL, *Chief Investigative Counsel*
JENNIFER A. HEMINGWAY, *Minority Staff Director*
THOMAS BISHOP, *Minority Legislative Aide*
JESSICA NAGASAKO, *Chief Clerk*

CONTENTS

	Page
Opening statements:	
Senator Akaka	1

WITNESSES

FRIDAY, FEBRUARY 29, 2008

Hon. David M. Walker, Comptroller General of the United States, U.S. Government Accountability Office	4
Marvin C. Ott, Professor, National Security Policy, National War College, National Defense University	6
Steven Aftergood, Director, Government Secrecy Project, Federation of American Scientists	8
Frederick M. Kaiser, Specialist in American National Government, Government and Finance Division, Congressional Research Service	9
Ronald A. Marks, Senior Vice President for Government Relations, Oxford Analytica, Inc	11

ALPHABETICAL LIST OF WITNESSES

Aftergood, Steven:	
Testimony	8
Prepared statement	58
Kaiser, Frederick M.:	
Testimony	9
Prepared statement	65
Marks, Ronald A.:	
Testimony	11
Ott, Marvin C.:	
Testimony	6
Prepared statement	54
Walker, Hon. David M.:	
Testimony	4
Prepared statement	29

APPENDIX

CRS Report entitled "Congressional Oversight of Intelligence: Current Structure and Alternatives," February 11, 2008, submitted for the Record by Mr. Kaiser	71
CRS Report entitled "Security Classified and Controlled Information: History, Status, and Emerging Management Issues," February 11, 2008, submitted for the Record by Mr. Kaiser	99
Background	135
Post-Hearing Questions for the Record Submitted to the Hon. Slade Gorton from Senator Daniel K. Akaka, January 9, 2007	143
Post-Hearing Questions for the Record Submitted to the Hon. Lee H. Hamilton from Senator Daniel K. Akaka, January 9, 2007	145
Letter to Senator Akaka from Lee H. Hamilton, dated January 24, 2007	147
Letter from Mr. Walker to Senator Akaka, dated March 11, 2008, in response to a question at the hearing	148
Letter from Mr. Walker to Senator Akaka, dated April 25, 2008, in response to questions at the hearing	149

GOVERNMENT-WIDE INTELLIGENCE COMMUNITY MANAGEMENT REFORMS

FRIDAY, FEBRUARY 29, 2008

U.S. SENATE,
SUBCOMMITTEE ON OVERSIGHT OF GOVERNMENT MANAGEMENT, THE FEDERAL WORKFORCE, AND THE DISTRICT OF COLUMBIA,
OF THE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10:03 a.m., in Room SD–342, Dirksen Senate Office Building, Hon. Daniel K. Akaka, Chairman of the Subcommittee, presiding.

Present: Senator Akaka.

OPENING STATEMENT OF SENATOR AKAKA

Senator AKAKA. I call this hearing of the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia to order.

Today's hearing—Government-wide Intelligence Community Management Reforms—will examine how to improve oversight of the Intelligence Community (IC) as it implements extensive government-wide management reforms.

Intelligence failures before the attacks of September 11, 2001, spurred the largest restructuring of the Intelligence Community since it was established. The Intelligence Reform and Terrorism Prevention Act of 2004 created a new position—the Director of National Intelligence—to serve as the head of the Intelligence Community and principal advisor to the President on intelligence matters related to national security.

The Intelligence Reform Act provides the DNI with centralized authorities significantly more extensive than those formerly held by the Director of Central Intelligence. The Director of National Intelligence oversees and coordinates the intelligence activities of the other members of the IC, which include 16 other components spread throughout much of the Executive Branch.

Acting on these authorities, the DNI has proposed a host of management reforms, including changes in IC personnel policies, acquisitions, information sharing, and business practices. Such management reforms would create serious transformational challenges in any organization. The Intelligence Community, with its new, but still decentralized structure, led by a new director with new authorities, faces a daunting task in carrying out these management reforms. While what the DNI is proposing may be new for the In-

telligence Community, it is not new for the rest of the Federal Government. Many of the issues being confronted and the solutions posed are ones other Federal agencies have managed already.

So it is my strong belief that the Intelligence Community could benefit from the Government Accountability Office's expertise in reviewing organizational transformations and management reforms. My view is shared by others, including Representative Lee Hamilton, who was Vice Chairman of the 9/11 Commission, and Senator Slade Gorton, also a member of the 9/11 Commission. In response to my questions for the record of a January 2007 Senate Homeland Security and Governmental Affair Committee hearing on implementing the 9/11 Commission's recommendations, both stated that GAO should have the same authorities with respect to the Intelligence Community as it does with other Federal Government agencies.[1] I will place these responses as well as a letter from Representative Hamilton addressing the issue into the record.[2]

Senator AKAKA. I am disappointed that despite GAO's government-wide mandate to assist Congress in reviews, audits, and investigations, the DNI and the CIA so far have resisted taking advantage of GAO's assistance in the transformation of their business practices.

The IC's cooperation with GAO is not simply a matter of making Congress' oversight job easier; it is a matter of making the IC's management reforms smoother, more effective, and more efficient. GAO has expertise in virtually all of the bread-and-butter management challenges that the Intelligence Community is confronting.

For example, GAO has done extensive work on how to fix the security clearance process, which is on GAO's high-risk list. Fixing the long delays in the process is an important national security priority. In response to a question for the record from Senator Voinovich from a November 2005 hearing of this Subcommittee on improving the process, GAO stated that it lacked the cooperation needed to ensure progress on this critical issue.

Similarly, GAO has done numerous evaluations of government information sharing, and it has provided valuable recommendations on improving information-sharing processes. Nonetheless, DNI refused to comment on GAO's March 2006 report on government sharing of sensitive but unclassified information because of its narrow view of GAO's authority.

Moreover, GAO has been a key advisor to Congress in its oversight of the development of new personnel systems at the Departments of Defense and Homeland Security. Given the fact that there are no union representatives to highlight employee concerns or implementation problems with the proposed IC personnel reforms, it is essential that Congress have an independent expert to review how such proposals are working.

Congress and the Intelligence Community could benefit from GAO's expertise on all of these topics, as well as from GAO's capac-

---

[1] The post-hearing questions for the Record submitted to the Hon. Slade Gorton and Hon. Lee Hamilton at the January 9, 2007 hearing from Senator Akaka, appear in the Appendix on pages 143 and 145 respectively.

[2] The letter from Lee H. Hamilton to Senator Akaka, dated January 24, 2007 appears in the Appendix on page 147.

ity to do crosscutting, government-wide evaluations in its institutional and political independence.

In September 2006, I introduced the Intelligence Community Audit Act, which I reintroduced in the 110th Congress as S. 82. This bill would reaffirm GAO's existing authority to perform audits and evaluations of Intelligence Community financial transactions, programs, and activities, and to obtain the documents needed to do so. At the same time, the bill contains provisions to enhance the protection of classified information, including restricting GAO work and dissemination of GAO reports related to covert actions and intelligence sources and methods, and affirming that GAO staff would be subject to the same penalties for unauthorized disclosure of classified information as IC employees.

The Intelligence Community is proposing far-reaching transformational policies. It clearly could benefit from independent analysis and sufficient congressional oversight. But the response of the DNI to Congress is, in effect, "Trust us, we know what we are doing." Unfortunately, history provides numerous examples of intelligence failures that became evident only after it was too late to correct them. The stakes are too high to operate just on trust.

Congress must redouble its efforts—that is what we are trying to do—to ensure that U.S. intelligence activities are conducted efficiently, effectively, and with due respect for the civil rights and civil liberties of Americans, and I will work to see that it does.

I look forward to hearing from our witnesses on their perspectives of how Congress can improve oversight of the Intelligence Community, in particular the role of the GAO. I want to thank our witnesses for being here today to discuss this very important issue.

I want to thank David Walker for nearly a decade of service as the Comptroller General as he prepares to transition to become the President and Chief Executive Officer of the newly established Peter G. Peterson Foundation. Mr. Walker, it has been my pleasure to work closely with you over the years, and I cherish those memories. I wish you well in your new endeavor. I hope that your replacement will be someone who is equally capable and equally dedicated in his or her service to GAO and to Congress and especially to the people of these United States.

And so I want to welcome, again, all the witnesses to this Subcommittee hearing. David Walker, Comptroller General of the United States with the Government Accountability Office.

Marvin Ott, who is a professor of national security policy at the National War College of the National Defense University. Professor Ott also worked as a CIA analyst and as Deputy Staff Director of the Senate Select Committee on Intelligence under Senator Murkowski, among numerous other positions.

Steven Aftergood, Director of the Government Secrecy Project at the Federation of American Scientists. Mr. Aftergood has won numerous awards for his work combating secrecy, including the James Madison Award from the American Library Association.

Frederick Kaiser, specialist in American National Government, at the Congressional Research Service. Mr. Kaiser has worked at CRS for more than 30 years and has taught at American University and the University of Maryland as well.

Finally, Ronald Marks, Senior Vice President for Government Relations at Oxford Analytica, Founder and Director of the Open Source Intelligence Forum and Adjunct Professor for Intelligence and National Security at the National Defense University. Mr. Marks formerly served as a senior CIA official and as intelligence counsel to former U.S. Senators Bob Dole and Trent Lott.

As you know, it is the custom of this Subcommittee to swear in all witnesses, and I would ask all of you to stand and raise your right hand. Do you solemnly swear that your testimony you are about to give this Subcommittee is the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. WALKER. I do.

Mr. OTT. I do.

Mr. KAISER. I do.

Mr. AFTERGOOD. I do.

Mr. MARKS. I do.

Senator AKAKA. Thank you. Let the record indicate that our witnesses answered in the affirmative.

I want our witnesses to know that while your oral statements are limited to 5 minutes, your entire statements will be included in the record.

Mr. Walker, please proceed with your statement.

TESTIMONY OF HON. DAVID M. WALKER,[1] COMPTROLLER GENERAL OF THE UNITED STATES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. WALKER. Thank you, Chairman Akaka. Thank you very much for your kind comments in your introductory remarks. Let me note that while I have several other hearings scheduled during the balance of my 2 weeks as Comptroller General, I believe that this will be my last hearing before this Subcommittee, unless something changes. And I just want to let you know that it has been an honor and a pleasure to work with you, with Senator Voinovich and with the other Members of this Subcommittee. And I take great pride in knowing that working together in partnership we made a big difference.

I also want to let you know that while I am changing my position on the battlefield, I am not leaving the fight. And, in fact, as CEO of the Peter G. Peterson Foundation, I will have more flexibility and more discretionary financial resources to bring on the target—namely, the need to address our sustainability challenges and government transformation needs. So I look forward to continue to work with you, although in a different capacity.

With regard to today's hearing, I am pleased to be here in order to be able to address how GAO could assist the Congress and the Intelligence Community in connection with management reform initiatives. As you know, Mr. Chairman, GAO has assisted the Congress for decades in its oversight role, and we have helped a variety of government departments and agencies with very disparate missions to improve their economy, efficiency, effectiveness, ethics, and equity. In addition, GAO's work has also provided very valuable insight as to which type of programs, functions, and ac-

[1] The prepared statement of Mr. Walker appears in the Appendix on page 29.

tivities work and which ones do not, and also foresight as to what some of the current emerging trends and challenges are facing the United States and its position in the world.

There are a number of government-wide management transformation challenges that are on our high-risk list, and you are very familiar with that high-risk list, including such items as human capital transformation, acquisition, contracting, information technology, strategic planning, organizational alignment, personnel security clearances, and information sharing. Many of these issues affect a vast majority of Federal agencies, including the Intelligence Community. And I think it is important that I am here today to talk about management reforms, not sources and methods. That is a different issue. But there are basic management challenges that every Federal entity faces, including the Intelligence Community.

Second, if the ODNI assumes management of government-wide personnel security clearances, then GAO's ability to continue to review personnel security clearances could be impaired unless greater cooperation is forthcoming from the Intelligence Community.

Now, let me stop here to note that I met personally with the Director of National Intelligence on more than one occasion, and he is a very capable individual, and he seems to be very reasoned and very reasonable, and so our relations are improving. And it is not a personal issue here. Frankly, this is an issue that goes back many years based upon access challenges, based upon an opinion from the Justice Department that has been there for a number of decades. So this is not something that is new. It has been longstanding. And my experience with the director has been positive, as well as some of his key staff.

And as I say, we have developed and maintain a relatively positive working relationship, which has improved in recent times. But because of this past legal opinion, and because of positions taken by some key players historically in the Intelligence Community, we generally have done little to no work in the Intelligence Community, because as you know, Mr. Chairman, we already have a huge supply and demand imbalance. We have way more requests for GAO to do work than we have resources to do it. And in the absence of receiving requests to do the work, then we are not going to use our limited discretionary resources to do work in this community when Congress is not asking us to do the work.

Third, with the support of the Congress and your legislation, S. 82, GAO would be well positioned to provide the Intelligence Community, as well as the appropriate congressional committees, with an independent, fact-based view and evaluation of Intelligence Community management reforms. As you noted in your opening statement, GAO has significant expertise with regard to a broad range of management issues. We have knowledge of best practices as well as lessons learned. And we have, during my tenure, tried to lead by example with regard to a lot of these reforms and really increase the amount of time and effort that we are spending on them to help benefit others in a constructive way, not in a confrontational or traditional audit role way.

We support your bill and believe that if it was enacted, GAO would be well positioned to assist the Congress in its oversight

functions and that we, frankly, could help the Intelligence Community, too. Ironically, our number one competition for talent is the Intelligence Community. We win, fortunately, on most college campuses, but they do a good job, too. And the fact is that we are both hiring, in large part, highly educated, committed individuals to do analytical work. That is what we do at GAO, and to a great extent, that is what the Intelligence Community does. So in many ways, our own experience at GAO frankly is very applicable to a lot of the challenges, I think, that the Intelligence Community faces.

You also have certain affirmation or reaffirmation provisions in the bill that should help to ensure that GAO's audit and access authorities are not misconstrued in the future, and should responsibility for personnel security clearances be transferred to the Director of National Intelligence, to make it clear that we should continue to receive access to that type of information in order to discharge our responsibilities to the Congress and the American people.

Thank you, Mr. Chairman.

Senator AKAKA. Thank you very much, Mr. Walker. Mr. Ott.

TESTIMONY OF MARVIN C. OTT,[1] PROFESSOR, NATIONAL SECURITY POLICY, NATIONAL WAR COLLEGE, NATIONAL DEFENSE UNIVERSITY

Mr. OTT. Mr. Chairman, thank you for the opportunity to appear before this Committee on a matter that is of real and concrete importance to U.S. national security. My testimony submitted for the record is brief. My summary comments I will try to make informal and briefer still.

Let me begin with two, I think, fairly obvious propositions, the first of those being that high-quality intelligence is increasingly critical to the national security of the United States. One way to think about that is to look at the nature of the threats we face and to contrast them with those of the Cold War period when the Soviet threat was military. I think it is fair to say that in a world characterized by an al-Qaeda type of threat, diversifying networks of terrorist groups, not to mention proliferation issues, pandemic issues, and other systemic threats—these are issues that naturally fit the intelligence world in many ways much more exactly than they fit the traditional, conventional military world. So, increasingly, the point of the spear, to borrow a much overused metaphor, for U.S. national security really does reside now in the intelligence world.

Second, effective oversight of the intelligence process is, in fact, critical. People at the top of the intelligence business who have been around and are experienced and have judgment on these matters know that effective oversight is critical. It is a force enabler. It is a corrective. It serves as an advocate and a shield. In a whole variety of ways, it is not an adversary to effective intelligence. It, in fact, is an important support.

With regard to this, then, the question of how effectively the Congress—and I am focusing particularly on the Senate—has conducted intelligence oversight is very relevant. Now, here a little background is necessary. Mr. Chairman, you cited the fact that

[1] The prepared statement of Mr. Ott appears in the Appendix on page 54.

Senator John Glenn, introduced a bill in 1987, S. 1458, that sought to do exactly the kind of thing you are talking about today.

And that bill was not accepted, and I think the principal argument at the time—and I had a ringside seat, as it were—was that in the 1980s, when Senator Glenn introduced that bill, the Senate Select Committee on Intelligence had, in fact, become a very effective vehicle for oversight. This was not easy. The match between the open, democratic, public processes of a democratic legislative body, on the one hand, and the secretive, closed, need-to-know world of intelligence—that is an oil-and-water kind of match. And to make that process work, to bring oil and water together, to have effective oversight that is constructive and works in the secret world of intelligence is a very hard thing to do.

I would argue that probably no country in the world has done it except this country, and we did it in the 1980s, and I can go into some detail regarding the process that made it work.

But suffice it to say, when Senator Glenn introduced his bill at that time, the argument was we are doing effective oversight, not only through the oversight committee, but we are establishing a statutory IG at the CIA, and we have reason to believe that is going to be an effective vehicle. So the argument was we have this problem under control. But things have changed since 1987, and I will just tick off the major points and leave it at that at this point.

First of all, the quality and the effectiveness of the oversight process I have just referred to, deteriorated, degraded, and basically disappeared in the 1990s and into the early part of this decade. It is one of the great tragedies of the legislative history of the United States, in my judgment.

Second, the community that is being overseen has grown in complexity, diversity, and in size. For example, the office of the DNI, which did not exist in 1987, has become a major bureaucracy. I have in my testimony that it comprises of 1,600 people. I believe that is, in fact, conservative. It is probably closer to 2,000. Nobody, including Director McConnell, knows what is going on inside all the different components of the current Intelligence Community.

Moreover, there is a statutory IG at the CIA, but nowhere else in the community. Everybody else, pretty much, is under the DOD IG. That DOD IG has got lots of other things to do on the military procurement side, on the defense side. He is a marginal player when it comes to intelligence oversight.

Finally, the diversity and nature of the threats we face—and I alluded to that at the outset—has multiplied.

Bottom line, there is, in my judgment, currently a mismatch, a serious mismatch, between the capabilities to conduct oversight and the vehicles and the instrumentalities for that, on the one hand, and the nature of the Intelligence Community and the nature of the threats, on the other. And GAO is an important potential asset in correcting that mismatch.

Senator AKAKA. Thank you very much, Mr. Ott. Mr. Aftergood.

TESTIMONY OF STEVEN AFTERGOOD,[1] DIRECTOR, GOVERNMENT SECRECY PROJECT, FEDERATION OF AMERICAN SCIENTISTS

Mr. AFTERGOOD. Thank you, Mr. Chairman. Thank you for holding this hearing. Because of the very importance and the sensitivity of the intelligence enterprise, intelligence oversight is a critical function. The public relies on the oversight system to ensure that intelligence activities are conducted in conformance with law, efficiently and effectively. But the task of intelligence oversight has become significantly more difficult in recent years for at least two reasons. One is the enormous growth in the size of the intelligence budget. Ten years ago, the National Intelligence Program was spending on the order of $20 billion a year. Last year, the DNI disclosed the National Intelligence Program budget reached $43.5 billion. So intelligence spending on national intelligence has more than doubled. Intelligence oversight capacity has not doubled. It has not kept pace.

A second complicating factor is the rise in reliance on intelligence contractors. According to an ODNI account that I cite in my written statement, the spending on intelligence contractors has also doubled from 1996 to 2006. There are literally thousands of new contractual relationships between intelligence agencies and commercial entities that the intelligence oversight system is poorly equipped to regulate, oversee, or even verify that they are doing what they are supposed to be doing.

For these reasons alone, I think that the government ought to be summoning all the tools at its disposal to carry out the task of intelligence oversight, and that certainly includes the Government Accountability Office. I do not think the GAO can solve the oversight challenge all by itself. To do that it might take an organization the size of the GAO devoted entirely to the Intelligence Community, and that does not seem to be a realistic option. But certainly GAO can make a tangible contribution as it does in almost every other area of government oversight.

A couple other quick points. When GAO is excluded from intelligence oversight, not only does Congress miss the benefits of their contribution, but carving out the Intelligence Community actually damages GAO's role in other ways. When GAO does a study of government-wide activities, say, on information sharing or on personnel security, it has to, in effect, come with an asterisk saying this work does not include the activity of the intelligence agencies. And there is no reason for that to be the case. Not only are we not taking maximum advantage of GAO, we are actually tying their hands and reducing the utility of their product.

I would also note that the DNI, the CIA, and others in the Intelligence Community have expressed opposition to your legislation, saying that they do not want GAO to get involved. And I would say that while that may be off-putting at first glance, at second glance it is actually a good sign. I would say that if the Intelligence Community did not object to your proposal, that would be perplexing. No one voluntarily seeks out oversight. No one looks for somebody to look over their shoulder to see how they are doing. So if ODNI

[1] The prepared statement of Mr. Aftergood appears in the Appendix on page 58.

said, "Oh, come on, that is fine," then I would wonder what is wrong with this legislation. Why aren't they objecting? The fact that they are objecting says that this legislation embodies meaningful change, and I would just urge you and the Subcommittee and the Senate not to be deterred by any such opposition. If you are persuaded, as I am, that a GAO role in intelligence oversight is a good one, then by all means you should pursue it.

Senator AKAKA. Thank you. Thank you very much, Mr. Aftergood. Mr. Kaiser.

TESTIMONY OF FREDERICK M. KAISER,[1] SPECIALIST IN AMERICAN NATIONAL GOVERNMENT, GOVERNMENT AND FINANCE DIVISION, CONGRESSIONAL RESEARCH SERVICE

Mr. KAISER. Thank you, Mr. Chairman. I thank you and Mr. Voinovich and Members of the Subcommittee for inviting me to participate in this hearing on government-wide Intelligence Community reforms, and with special attention to oversight of intelligence in this evolving field. The Intelligence Community rubric is formally applied to the 16 agencies, as you had mentioned earlier, but there is still another Intelligence Community that might be worth considering. And that is the Homeland Security Intelligence Community (HSIC). It is a much more nebulous and non-statutory organization, but, nonetheless, there is a collective set of intelligence operations and organizations that play a role, especially in your Subcommittee's jurisdiction. Both of these communities require a substantial amount of interagency cooperation and coordination to provide for a sharing of relevant and timely information as well as to engage in multi-agency activities and operations. Ideally, this second or HSIC can overcome the foreign-domestic divide that, according to the 9/11 Commission, hampered effective intelligence gathering, evaluation, and dissemination.

The homeland security Intelligence Community also requires coordination and cooperation with State, local, and tribal organizations, so it has a wider and a different kind of jurisdiction.

Oversight of intelligence, as we already heard and as you well know, has always been a daunting challenge to Congress. And it seems to be increasingly so, because of the increase of classified national security information and new categories of controlled information, such as sensitive but not classified information. And this affects a range of activities here on the Hill that limit congressional oversight. It even means that committees cannot cooperate with one another, that there are barriers put in between sharing information from one member to another because of the restrictions that are placed on receiving and responding to classified information.

National security concerns also affect other oversight capabilities. Importantly, certain offices of Inspector General are affected by this. The heads of six or seven departments and agencies can prohibit or prevent an IG audit or investigation, and those are largely in the Intelligence Community. The reasons for this prohibition, though, have to be communicated to your Subcommittee as well as the authorizing committees. So it does give your Subcommittee a handle on what has developed or why an audit has not occurred

[1] The prepared statement of Mr. Kaiser appears in the Appendix on page 65.

by the Office of Inspector General. That applies to all the entities that I mentioned except for the CIA, which reports directly then to the House and Senate Intelligence Committees.

Oversight of intelligence has been consolidated in these select committees, but they do not hold exclusive oversight jurisdiction. In fact, importantly, the establishing resolution of the House and Senate select committees repeat the same language: "Nothing in this resolution shall be construed as prohibiting or otherwise restricting the authority of any other committee to study and review any intelligence activity to the extent that such activity directly affects a matter otherwise within the jurisdiction of that committee."

Examples of such oversight extend to, again, your Subcommittee in the past. In the mid-1980s, the Permanent Subcommittee on Investigations looked into the Federal Government security clearance program. Later on, Congress commissioned a review of the Intelligence Community workforce that was conducted by the National Academy of Public Administration. And in July 2001, two Subcommittees of your counterpart at the time, the House Committee on Government Reform, now Oversight and Government Reform, reviewed computer security programs across the board. It relied on a GAO survey that had been conducted earlier, and only one agency was a holdout. That was the Central Intelligence Agency. It declined to participate in the hearings or in the earlier GAO survey.

This is an illustration of the difficulties that GAO has had in providing comprehensive oversight of the Intelligence Community. The CIA has taken this position that it is, in effect, off limits. Your bill would go far to remove that characteristic that the CIA has adopted for itself.

I might mention in conclusion here that other entities within the Intelligence Community do not take that same stand. The Department of Defense, which houses the largest number of IC units, for instance, instructs its personnel to "cooperate fully with the GAO and respond constructively to, and take appropriate corrective action on the basis of, GAO reports." And so there is this distinction.

I might mention, too, as Mr. Ott has said, that in 1987 Senator Glenn from this Subcommittee had introduced legislation along the lines of your bill. An earlier proposal goes back to the mid-1970s, when the Comptroller General then, Elmer Staats, first raised this notion formally before a couple of Select Committees on Intelligence in the House and the Senate. Those two committees, the Pike and Church committees, also approached this subject and advanced proposals to increase GAO's independent audit capabilities.

My prepared remarks go into detail on other types of changes that Congress might consider in improving oversight of intelligence.

Senator AKAKA. Thank you very much, Mr. Kaiser, for your statement.

Mr. Marks, I understand that you do not have a prepared statement to deliver, but I would ask you, if you have any remarks you would like to make, you may make them at this time.

TESTIMONY OF RONALD A. MARKS, SENIOR VICE PRESIDENT FOR GOVERNMENT RELATIONS, OXFORD ANALYTICA, INC.

Mr. MARKS. Thank you, Senator. The last one should always be shortest, if at all possible. It is an honor to be here, especially on something I have considered so strongly over the years, dealt with this issue on and off during my years at CIA, probably now 15, almost 20 years. As I was telling my wife this morning, I may not be an intelligence expert, but I live there, so I think I have a pretty good idea of what is going on.

The Intelligence Community always views itself in terms of a culture of secrecy, as it should, but that secrecy also produces a certain amount of belief of uniqueness. And in my days at CIA—and I spent some 16 years there—five of them were in Congressional Affairs, two of them were up here as intelligence counsel to Robert Dole and Trent Lott. And throughout that entire process, anytime someone mentioned GAO, I could hear the management on the seventh floor of the Central Intelligence Agency cringing, believing that they already had sufficient oversight from both the Senate and the House Intelligence Committees.

I did not necessarily want to argue with them at that time, but I knew of the work that GAO did, and it seemed as though it would be a good idea to introduce it. But low-level officers do not make those kinds of recommendations at the time. The problem I see now in particular, now that I am 10 years outside of the process but still acting as an advisor to the community, is that they have grown so large, so complex, so quickly, that really the problems are well beyond them now. Someone mentioned the contractual problems here before. That is unique to many parts of the community in terms of buying outside contractors, not only to do analytical work for them or other types of engineering work, but actually having people on site, particularly the Central Intelligence Agency, where that is rather unique.

Workforce planning. The size of the Intelligence Community has grown hand over fist since 2001, some estimates 40 percent, some estimates 50 percent, but whatever, there is no real plan in place at this point for helping these young people and directing them through their career within the community and hanging onto them. As someone in the private sector, I can tell you from my own experience at this point that unless you lay out a plan for your young people so that they can grow within your organization, you are going to lose them fairly quickly. And this is a group of young people now who are much less patient, perhaps, than I was back in the 1980s.

I am particularly concerned on the issue of security and compartmentation. This has been going on for a long period of time, really since the fall of the Berlin Wall, the end of the Cold War. We are still working in many ways with a system that was dealing with a very large Nation State, our opponent, the U.S.S.R., who believed in compartmentation, who believed in security, keeping control over their people. We live in a different age. The open source information contained around the world on the Internet alone is so many times the size, I do not think anybody knows what that all is. Yet we still have a system inside that does not allow those people who are analysts, those people who are operatives to really use

that system because it is considered a security threat by virtue of even asking the question. They are hamstringing themselves, they are hamstringing our national security, and I think these are a number of issues that the GAO could help them address because, frankly, the oversight committee process, the IG process at this point will always be viewed as somewhat biased, fair or unfair. But GAO has established itself over the years as a neutral outside organization, and I think it can provide the DNI some real insight into what it is that they are doing for these vast processes that are overseeing the community.

On that note, thank you, Senator. I will end my comments.

Senator AKAKA. Thank you. Thank you very much, Mr. Marks, for your comments.

As you know, I have introduced the Intelligence Community Audit Act of 2007, S. 82, which would reaffirm GAO's authority to perform audits and evaluations of financial transactions, programs, and activities of elements of the Intelligence Community. The bill also includes certain provisions to improve protection of the most sensitive intelligence information. For example, specifying that the House or Senate Intelligence Committees or Majority or Minority Leader would have to request any audit or evaluation of intelligence sources and methods or covert actions.

Do these provisions adequately address the DNI's concerns with protecting the most sensitive intelligence information? Or are there other steps that should be taken? Comptroller General Walker.

Mr. WALKER. Thank you, Mr. Chairman. First, I see a clear distinction between management issues and management reforms that apply to virtually every government department and agency, including the Intelligence Community sources and methods. Those are fundamentally different, and obviously the need to try to be able to provide additional restrictions and safeguards dealing with that type of information is clear; it is compelling.

Sometimes there can be a gray area where you are dealing with management type issues that could touch on some of these other issues. I think you have to keep that in mind.

I think that what you have done is to try to separate between typical management type activities and sources and methods. I will, in the interest of full and fair disclosure, note that as a member of the Board of Directors of the International Auditor Generals Organization, as head of strategic planning for that group, one of the things I have put to my colleagues is to what extent do they do audit and evaluation work in the Intelligence Community, and who do they do it for, and who has access to information.

For all the major industrialized nations, they said yes, the counterpart GAO organization does do work, audit and evaluation work, in the Intelligence Community. However, a significant majority of them also said that they typically only do it at the request of their intelligence committees and that the information is typically only provided to their intelligence committees.

I am not saying that is the right answer, but I feel compelled to provide the information just for your consideration.

Senator AKAKA. Mr. Ott.

Mr. OTT. Just very briefly, Mr. Chairman, I guess my quick reaction is the kind of carve-out that you have identified in the legisla-

tion makes perfect sense, and I am also inclined to say there is a bit of a false dispute here in the sense that, as Mr. Aftergood and Mr. Marks in particular correctly identified, there are huge requirement for effective oversight of management, audit, financial, and contractual activities—all these kinds of requirements for effective oversight. GAO will have more than enough to do if they are given authority to go into those areas. I frankly do not see any reason why there should be any particular demand to go into the narrow and highly sort of compartmented area of covert action and sources and methods. That strikes me as the logical place for the intelligence committees to work.

So it would seem to me that this is, as Mr. Walker has said, a pretty natural division of labor, and to some degree a kind of false problem. It seems to me something that can be worked fairly effectively.

Senator AKAKA. Mr. Aftergood.

Mr. AFTERGOOD. I think the distinction in the bill does make sense, but if your question is will it satisfy the objections of the DNI, I am afraid the answer is no, it will not. And the reason for that is because the Intelligence Community uses the term "sources and methods" with great elasticity.

I obtained a document showing the CIA budget for 1963. It was a declassified document showing that the budget was $500 million that year. I asked the CIA, "Well, what was the budget for 1964?" And they said, "Oh, we are not going to tell you that because of intelligence sources and methods."

And so basically it is a catch-all phrase for whatever they do not want to disclose. They do not use it in the same way that you and I might.

I would say, though, that addressing the ODNI's concerns may not be the hardest challenge facing this legislation. Candidly, it seems to me that the most difficult political obstacle may be winning the consent of the intelligence oversight committees. Speaking as an outsider, a member of the public, it appears to me that there are turf considerations on the part of the Subcommittee, and that just as the ODNI wants an exclusive relationship with the intelligence oversight committees, the intelligence oversight committees may want that very same exclusive relationship.

So there is a tactical question about how do you gain the acquiescence and approval of the intelligence oversight committees to what I think is a proposal that would assist them, if only they could be persuaded of that.

Senator AKAKA. Mr. Kaiser.

Mr. KAISER. May I add a caveat to all of this? In mid-2001, the examination by two House Government Reform subcommittees looked into computer security programs. They asked GAO to mount a preliminary review. The CIA declined to participate, largely because the CIA insisted this was a matter of sources and methods and could not comply with the GAO or the Subcommittee's request. The Subcommittee even invited the CIA to testify in executive or secret session. The CIA refused to do so.

In writing a letter to the Subcommittee explaining why they were not participating, the head of the CIA and DCI at the time said that they would give this information to the intelligence com-

mittees, the House Committee on Intelligence, which, as they interpreted, had exclusive oversight jurisdiction for sources and methods. That does not apply to the Senate side, but that was the argument that was being given at the time. And the CIA did point out that they had the concurrence or approval of the intelligence committee chairman.

So there is this notion of divided oversight responsibilities, jurisdiction, and of sources and methods; here it was applied to computer security programs, not information that might come from them.

Senator AKAKA. Mr. Marks.

Mr. MARKS. Yes. I would urge the Subcommittee very carefully to listen to the arguments made out of the Intelligence Community and CIA. The secrecy flag is often raised when they do not want to necessarily have something examined, and I have always been pleasantly surprised at how carefully they read S. Res. 400, which established the Senate Select Committee on Intelligence.

The problem may not come from the DNI office, and the problem may not come from the Director of Central Intelligence. I think both Mr. McConnell and Mr. Hayden are trying to do their best in very difficult jobs. As a friend of mine says, it is not them, it is the iron majors underneath of them. It is those who have grown up in that system at a lower level who are making the recommendations. And those people in many cases still are not convinced that oversight is necessary, again, based on their predilection towards secrecy. And they oftentimes would be willing to hide behind both SSCI and HPSCI, thinking, in fact, that they would get a better deal. And that is why I think you are seeing some of the information that is being sent back.

Senator AKAKA. Thank you. Mr. Walker.

Mr. WALKER. If I can, Mr. Chairman, add a couple of things based on these comments.

First, I have learned in 9½ years as Comptroller General that everybody is for accountability until they are the ones being held accountable. I have also learned that when you have information that is not classified but somebody says it is sensitive, you can substitute the words "probably embarrassing" for "sensitive."

I think we have a situation here where, as has been noted, sources and methods mean different things to different people depending upon the circumstances. And I would argue that is probably one of the reasons why in our counterpart organizations around the world, they have done work and provided that work to the intelligence committees in order to just eliminate that issue. Whether it is management work or whether it is sources and methods work, what is important is that it be done and it be done by somebody who is qualified, who has the confidence of the Congress and the American people, and that it be provided to the appropriate bodies who have the ability to do something with it.

Now, candidly, I believe that the Select Committees on Intelligence are part of the problem. There is no question about that. I also believe that no matter how caring they are, no matter how capable they are, the simple fact is, given the growth in the size, complexity, and criticality of this area, more needs to be done, and frankly, they do not have the expertise in the management areas

that we are talking about here. So, they do not have the resources, and they do not have the expertise, so as a result, we have a gap. That gap needs to be filled. It is in the national interest for it to be filled. And I think there is a way to bridge these issues. I really do believe so.

Senator AKAKA. Are there any further comments? [No response.]

Let me follow up, and on behalf of GAO, looking at this from the other side of the coin, would S. 82 adequately protect GAO's ability to audit and evaluate elements of the Intelligence Community?

Mr. WALKER. First, Mr. Chairman, I think it would, but I think we have to reinforce a couple of things. We believe, with very limited exceptions, that GAO already has extensive audit and evaluation authority over intelligence agencies, including the CIA. We absolutely reject the position taken by the CIA and selected others, and I think some of the legislative history that Dr. Kaiser mentioned helps to serve to reinforce the fact that people are trying to reinvent history here with regard to what the intention of Congress was at the time that the Select Intelligence Committees were created.

There is an iron triangle here between the Intelligence Community and the intelligence committees, and there is a lot of movement back and forth among key staff there between the communities. They are all very qualified and they are all very capable, but they have a limited capacity, obviously, in that regard.

So I think it would, but I want to reinforce the fact that you are careful in some regards in your bill to reaffirm authority that we already believe we have. And I think it is important that nothing be done that could somehow undercut what we believe to already be the case, and that is, we have authority in most of these areas. We just have not had requests, and we have not in some circumstances had cooperation.

Most of the Intelligence Community is not the CIA, and in a lot of the Intelligence Community, we have had and we continue to have cooperation. So I think it is important that we not paint with too broad a brush here. We need to use a laser. There are problems with regard to specific entities, but there is not a problem necessarily with regard to the whole community. And Director McConnell, I believe, is a very capable person who hopefully we can work out something with.

Senator AKAKA. Any other comments? [No response.]

Mr. Walker, the DNI has expressed concerns that GAO review of intelligence agencies could compromise intelligence information. Over the years, GAO has done significant work involving classified information and also has written classified reports. I find it a bit troubling that the Intelligence Community trusts private contractors with a great deal of intelligence information, yet it does not trust GAO to safeguard the same information.

To your knowledge, has classified information provided to GAO ever been leaked?

Mr. WALKER. To my knowledge, never in the history of GAO, which goes back to 1921, has there been any classified information leaked from GAO, and that includes a lot of entities other than the Intelligence Community. I find more than a little bit of hypocrisy in the position of the Intelligence Community on this.

Senator AKAKA. General Walker, do you have any thoughts on the particular challenges of evaluating government activities where classified information is involved?

Mr. WALKER. Well, Mr. Chairman, we have a number of individuals, including myself and many others at different levels of the organization, that have top secret clearances and also have other "tickets" (Sensitive Compartmented Information Clearances and related accesses) that would be necessary to do a whole range of work. What I would envision is that if the Congress did start asking us to do work in this area, we would limit that to a relatively small group of individuals who had the required clearances and we would want to do that as a further safeguard in order to provide additional assurance that nothing would be leaked and that it was more a need to know within GAO.

But I think you have to keep in mind it is not just the need-to-know concept, it is the right to know. The Congress has a right to know as well as a need to know.

Senator AKAKA. Mr. Walker, if GAO increases its work with the Intelligence Community, with the intelligence committee, it will have to rely on employees with security clearances, as you mentioned. Do you currently have enough GAO analysts with high-level clearances, in particular top secret and SCI, to increase GAO's work with the Intelligence Community if that work were no longer restricted?

Mr. WALKER. I believe we do, Mr. Chairman, but obviously it depends upon how many requests we receive. From a practical standpoint, what we are talking about is reallocating existing resources, given the current budget environment, rather than adding resources. I would be happy to provide for the record, if you would like, how many GAO employees we have with top secret clearance and how many we have with special SCI.[1]

Senator AKAKA. I would appreciate that.

Congress created an Inspector General for the Central Intelligence Agency to improve oversight of that agency. Last fall, CIA Director Michael Hayden launched a probe into the CIA Inspector General's work, and earlier this month, Mr. Hayden announced that the CIA was creating an ombudsman to oversee the IG's work.

How concerned should Congress be that the CIA is trying to rein in the IG's independence? Or is this more a matter of enhancing the IG's accountability? Mr. Ott.

Mr. OTT. Mr. Chairman, to answer that question fully would require a very fine grained knowledge of exactly what is going on in the relationship between the DCI and the IG, which I do not pretend to have. I will say—and I noted it in my testimony—that the current CIA IG's office is a beleaguered office. It is continuing to conduct a series of investigations and do its business, but at the same time is dealing with this probe and these pressures and questions being raised by the DCI. And you now have the creation of an ombudsman as a rival office of some sort. And it basically just goes back to the original proposition that the instrumentalities of oversight that are available to deal with this hugely growing, com-

[1] The letter dated March 11, 2008 with the response from Mr. Walker appears in the Appendix on page 148.

plex animal of the Intelligence Community, even those limited instrumentalities like the CIA IG are, in fact, under pressure, beleaguered, and to some degree probably hobbled.

Senator AKAKA. Mr. Aftergood.

Mr. AFTERGOOD. As you were describing the creation of the ombudsman to review the activities of the Inspector General, I was wondering to myself who is going to oversee the ombudsman. But without prejudging the facts of that case, I would say two quick things.

The Office of the Inspector General performs a crucial function. There is a new report out from the Project on Government Oversight this week examining the strengths and weaknesses of the Inspector General system, and it needs to be bolstered. But it is part of the larger issue confronting this Subcommittee and the Congress and addressed in your bill of how to strengthen the oversight function.

If there are currently 50 intelligence staffers in Congress overseeing a budget of around $50 billion, that means that, on average, each staffer is responsible for $1 billion of government activity. And that is just not a reasonable task to expect them to perform adequately.

So we need to strengthen all of the institutions of oversight, including the Inspector General, most certainly including a GAO role in intelligence.

Senator AKAKA. Thank you. Mr. Kaiser.

Mr. KAISER. Yes, if I may add to what has already been said. When the CIA Inspector General was created, it was in the aftermath of the Iran-contra affair. Congress had already tried to bolster the administratively created Inspector General at the CIA but found that it was not receiving adequate reports and information from that office. Consequently, the new office was created in 1989, and, in fact, in a very remarkable situation, because the Intelligence Authorization Act was already before the Senate on the floor. It was brought back into the intelligence committee, and this provision for a new Inspector General, a statutory Inspector General in the CIA, was added to it; and then the bill was re-released and sent to the floor for approval. That tells us how important and how conflictual that particular episode was.

According to a recent press account, the Director of the Central Intelligence Agency said that he was looking at the IG the way he would at any other management entity. But the Inspector General is not the same as any other management entity within an organization. Even at the CIA, it is given certain statutory protections to prevent it being beleaguered and manipulated, if you will.

The Inspector General also may have his investigations or audits prevented by the head of the agency. That applies, as I mentioned, to only six other governmental organizations.

So for the DCIA to say or to insist that the Inspector General may have gone off on too independent of an exercise, the DCIA has authority to prohibit or intervene in some of those investigations.

Senator AKAKA. Mr. Marks.

Mr. MARKS. That has always been a fractious relationship for as long as it has been there between the IG and the CIA, and particularly on the operations side, which, as someone mentioned—I

mean, this was set up shortly after Iran-contra, and the operations people were rubbed raw, as it was.

It has been a difficult position but a necessary one, certainly the last several IGs who have been there—Britt Snider, Fred Hitz, a few others—have taken their share of flack. I am troubled by the ombudsman business because I think that does send the wrong message. But at the same time, I think the IG continues under John Helgerson, who is a long-time CIA official at a very senior level and a very bright, independent man, to continue to do the kinds of postmortems as well as suggested activities that they need to do there. However, again, I agree with the panel. I think that appointing an ombudsman at this point sends the wrong message altogether.

Senator AKAKA. Thank you.

The fiscal year 2008 intelligence authorization bill would create an Inspector General for the Intelligence Community as a whole. I would like to hear your thoughts on how an IC-wide Inspector General could enhance oversight of the Intelligence Community as well as any potential problems you might see with the proposal. Mr. Marks.

Mr. MARKS. Thank you, Senator. Well, on the positive side of it, the DNI office has grown so large now and is dealing with such complex issues that it probably would not—it would certainly be helpful to have an Inspector General there to begin to look at some of the sub-processes going on there. Certainly an Inspector General at that level could also look at some of the interactions between the agencies and the DNI. I do not think it is any secret at this point that many of the agencies in the Intelligence Community have been greeted by the DNI like a third cousin coming from out of town to borrow money. They are unhappy with their presence there. It has, I think, conflicted to some extent with what the 2004 bill was in terms of creating that DNI, and probably having an Inspector General at this point, I think, would certainly help ease that process. It might also help as an interesting liaison to GAO as they begin their processes within the community as well.

Senator AKAKA. Mr. Walker.

Mr. WALKER. Mr. Chairman, I have mixed thoughts about it. First, I think the government has too many IGs. We have about 60 of them. Some of them are presidentially appointed, about half. About half are appointed by the agency head, and can be removed by the agency head. Some have hundreds of people at their disposal, that is, professionals at their disposal. Some have themselves and maybe one or two staff.

So I think one of the things that has to happen in this year, which is the 30th anniversary of the IG Act, is that Congress needs to relook at the IG community in particular and the accountability community as well, which includes GAO, to try to make sure that there is adequate coverage while avoiding duplication of effort, trying to create more critical mass, more flexibility, more synergies, and more accountability.

That being said, as has been said before, the CIA is the only agency within the Intelligence Community that has its sole, dedicated Inspector General. The DOD IG covers a lot of others, but they, frankly, have got a fair amount of work to do there. And so,

I think you have to think about what do you do with regard to other ones that exist. It is one thing to say that you are going to have an Inspector General for the Intelligence Community and that that person is going to report to the Congress and maybe to the DNI, dual reporting, which the residentially appointed Inspectors General do. But then what is that going to do for the CIA Inspector General? And what is the impact going to be on the DOD IG in order to prevent duplication of effort and in order to create better clarity as to who is responsible for what?

So I think it has some conceptual merit, but I think we have to put it in the context of, if you have more capacity here with an IG, what is that going to do on a micro basis to try to make sure you do not have duplication of effort within that community. And, second, I think we need to take a whole look at the IG Act and rationalize the overall structure and its relationship with GAO after 30 years.

Senator AKAKA. Mr. Aftergood.

Mr. AFTERGOOD. I would concur with that and just say that not all IGs are created equal, and that if there is to be an IC-wide IG, it is important that that office reflect the best practices in government and not the least effective. So the key touchstones really are the independence of the office, as written into statute; the resources that it has; and the personnel, the quality of the personnel working in the office. With the right people, the right resources, and the right statute, it can be a tremendous addition. Without them, it can be insignificant or perhaps even counterproductive.

Senator AKAKA. Mr. Ott.

Mr. OTT. Mr. Chairman, maybe just one point in this regard, and I am keying on Mr. Walker's comments. Oversight works and it works effectively when various criteria are met, and one of those criteria is a perception among the overseen, in the Intelligence Community in this case, that the process is efficient, that the lines of authority and responsibility are clear, that you are not duplicating effort, you are not being asked to keep repeating the same thing to different people, reinventing the wheel, dealing with conflictual authorities. You want the process streamlined in every respect, including on the congressional end, in terms of oversight authority. Do you have multiple masters or is there a fairly limited demarcated set of folks that you are responding to?

I just raise that because it is important in gaining the cooperation and support of the community itself, which is vital to making oversight work well.

So I would encourage the Subcommittee, to keep this in mind as you address all these issues. Oversight is a good thing, but oversight just willy-nilly in all sort of guises and incarnations is not necessarily a good thing. It needs to be efficient and streamlined.

Senator AKAKA. Thank you. Well, thank you for those responses.

Mr. Walker, notwithstanding DNI's reluctance to work with GAO, has DNI publicly identified any specific management issues that the community is having a challenging time working through?

Mr. WALKER. There are several issues that I know we have had conversations about. One in particular is human capital reform. Any organization is only as good as its people. That is clearly true in the Intelligence Community because, by definition, you are talk-

ing about intellectual property, intellectual capital, if you will. And so that is an area where they are engaging in a number of reforms, and, frankly, we have had some informal communications with the DNI's office on those issues. And I have seen some hopeful signs that we may actually be requested to do some work in that area because I think most people view the GAO as the clear leader in this area in government. And while we are not perfect, never will be, we are clearly the leader in this area.

There are other areas that I do not know that the DNI has personally been engaged in or spoken publicly about, but that clearly, I think, should be areas of priority consideration in addition to human capital: Acquisition and contracting, information sharing, and potentially security clearances. All these are on our high-risk list. That is the common denominator. And I think, importantly, while a lot of people do not like oversight, I think sometimes people misconstrue GAO's role because we really try to employ a constructive engagement approach. It is in all of our interest for everybody to be successful, and so a lot of what we do is we try to bring best practices, make the entities aware of best practices based on our collective experience, as well as lessons learned, to increase the likelihood that they will actually be successful. And I think that is what sometimes gets missed. GAO did not always have that reputation, but I think we do have that reputation now, and I fully expect that it is likely to be maintained.

Senator AKAKA. Thank you.

As Mr. Aftergood testified, ODNI has estimated that 70 percent of the Intelligence Community budget is spent on commercial contracts. That really is an astonishing statistic. Do any of you have insight into how IC contract management oversight is working, both in terms of the Intelligence Community's oversight of contractors as well as congressional oversight? Mr. Marks.

Mr. MARKS. At the risk of my business, I think one of the challenges for them right now is simply volume. The number of people involved with this process remains somewhat limited, certainly versus the Defense Department, who has had much greater experience over the years in terms of dealing with contractors. And we have seen some of the challenges that have come out of that as well. The creation of the DNI has added another strain on that process. We have certainly—in my own experience, I have certainly been well treated by those people. They have certainly gone out of their way to attempt to help, but they are oftentimes simply overwhelmed by the volume and, frankly, you have many young people in there who they are attempting to train up at this point. So while there are inefficiencies and you sort of hope they are gaining something on that as you are dealing with the tremendous volume of contracts now and the very large size and the billions of dollars of these contracts, the idea of having someone who can look over their shoulder such as the GAO and give them instruction on acquisition and give them instruction on the most effective best-practice ways of dealing with contracts I think would be greatly appreciated.

Senator AKAKA. Mr. Ott.

Mr. OTT. If I can just refer to one case that I note in my testimony, in 2001 the National Security Agency, with considerable fanfare for a secretive agency, announced a program called "Trail-

blazer" that was to have three prime contractors, very large ones, and some 30 industrial partners and a budget that ultimately well exceeded $1 billion. "Trailblazer" went on for a number of years and was designed to provide a transformation of NSA capabilities to cope with the modern information technology world.

Ultimately, it was a debacle, and then-Director Hayden ended up testifying that—it turned out that the new technologies were unmanageable—they were not working. NSA never fully understood what it was getting into. It ended up much like the infamous computer programs at the FBI, and ultimately the plug was pulled and defeat was declared.

The point for our purposes is that in this whole episode, there was no real effective oversight. The kind of capabilities that a GAO might have brought to that process as it was ongoing just simply did not happen.

So there are lots of examples like that, big examples, that argue the point that something else needs to be put in place here.

Senator AKAKA. Mr. Aftergood.

Mr. AFTERGOOD. This is not entirely a new problem. The National Reconnaissance Office, which builds spy satellites, has never actually built the spy satellites. It is always the contractors to the NRO that have built them for the last 40-plus years. But what is new is the explosion in contracting activity with just an enormous growth in spending and in number of contracts and in contracting on core intelligence functions, including analysis and collection. And the existing oversight system, it seems to me, is not well equipped to deal with that. The intelligence agencies answer to Congress, but the intelligence contractors do not. They answer to their customer, which is the intelligence agency who hired them. And so, in effect, the business of intelligence has been taken at least one step away from the oversight of Congress, and in some way, something needs to be done to rectify that. I think GAO provides an obvious if partial solution to that problem.

Senator AKAKA. Mr. Kaiser.

Mr. KAISER. Yes. To add to the complexity of auditing, overseeing, and evaluating the private contract operations is the notion that many of these contracts are bundled. I do not know if that is true in the Intelligence Community as it is elsewhere. But that means there are a number of separate private firms that are operating within, under a certain contract. That means further decentralization and difficulty in actually identifying or pinpointing who is responsible for what part of the contract. If down the line something does go wrong, there is a lot of finger pointing, and it is very difficult then to identify who is actually in charge of the whole operation or even a part of it.

Senator AKAKA. Well, let me ask Mr. Walker, as Mr. Aftergood testified, the intelligence components in the Department of Defense traditionally have not been as resistant as the CIA to cooperating with GAO. I understand that GAO even had an office at the NSA. Your testimony discusses some work related to elements of the Intelligence Community in the DOD. In general, do you still receive good cooperation from DOD components? Or has that changed as the IC has become somewhat more integrated under the DNI in recent years?

Mr. WALKER. We receive much better cooperation and generally good cooperation from the components dealing with the Department of Defense, at least most of them. We still actually do have space at the NSA. We just don't use it. And the reason we don't use it is we are not getting any requests. So I do not want to have people sitting out there twiddling their thumbs.

Senator AKAKA. Thank you.

Mr. Walker, the Intelligence Community at times uses private contractors for outside reviews or auditing of IC programs or activities. You have served extensively in both government and the private sector reviewing and auditing Executive Branch activities and programs. Do you have any thoughts on the limitations or benefits of having private contractors review Intelligence Community activities?

Mr. WALKER. Well, Mr. Chairman, I think another area that is in desperate need of a review by the Congress is what has happened with regard to the proliferation of the use of contractors in government. It has grown dramatically. We are using contractors in many ways that we never did historically. A lot of times, if you go to a meeting at a particular department or agency, you have no idea who a contractor is and who a civil servant is. You really do not know.

I think that there are certain functions and activities that should never be contracted out, and we need to have another discussion about that. But even if you do decide to contract out, I think there are plenty of things that should be contracted out. You need to have an adequate number of civil servants to be able to oversee cost, quality, and performance. And if you do not, you are going to get in trouble. And with the proliferation of service contracts in particular, there is also the additional challenge of not being able to provide enough specificity with regard to what those service contractors should be doing, which, in effect, gives them a quasi-blank check to do a number of things that may not be cost-effective for the American taxpayer.

Senator AKAKA. Professor Ott and Mr. Marks, you both also have worked as Senate staff on intelligence matters. The DNI is preparing to undertake a series of management reforms to its personnel systems: Contracting practices, financial systems, and business practices, among other proposals. What is your view on what type of expertise is needed by congressional staff to assess the Intelligence Community's performance on core management issues? For example, in your experience, how many auditors or accountants would be sufficient to perform the auditing function? Mr. Ott.

Mr. OTT. The kind of review of management practices that you are referring to, I think it is fair to say, have never been adequately overseen by the intelligence committees. You are really talking about a kind of GAO type of expertise, and to my knowledge—and I will not pretend to be completely knowledgeable on the current set of circumstances—the oversight committees have never had that kind of specialized expertise.

I will also say parenthetically, to use the metaphor, in the 1990s, Humpty Dumpty fell off the wall and was shattered into a very large number of pieces, and it will be a very difficult and very long-

term business to try to put all those pieces back together again, if, in fact, it can be done at all.

So just simply reconstituting what the Subcommittee once did is going to be a very difficult enterprise. And then to add to it a capability to oversee these kinds of management practices that the Subcommittee has really never done in the past will be adding additional difficulty on top of difficulty.

You can detect a skepticism in my voice. I will just note finally that in my direct experience the Senate Subcommittee did in the 1980s, when, as I say, it functioned effectively, had an audit staff, and it was called that. It consisted, as I recall of basically three people. Basically what they did was look at very large budget items, primarily overhead systems, and got into questions of weighing various alternative strategies for constructing and satellite systems. And there were some very high-level, very informed engagements between that staff and the Intelligence Community at the time. I would argue one of the high points of legislative history, frankly, was the quality of debate that went on between that small staff—and I was not part of it—and the leadership of the Intelligence Community with regard to how to use billions of dollars for overhead systems. But that was not the sort of thing you are describing. That was not getting down into management practices, personnel, knowledge management, contracting, that sort of thing. That was big-ticket strategies. And that worked because that staff was world class. It was not big. It was very small. But the people on it, and particularly the leadership of it, was absolutely first rate. It was almost a unique thing. And it is very hard to imagine it being reconstituted, at least in the current environment, to do the kind of job you are talking about.

Senator AKAKA. Mr. Marks.

Mr. MARKS. This, Senator, is the kind of red meat that McKinsey and Booz Allen and others make a lot of money out of. But the problem, again, on this is to develop, as Marvin was saying, an internal expertise, people who understand the community, but at the same time understand these problems. And that is a difficult thing to do. We had a fortunate period of time and a relatively smaller community where people could concentrate on larger contracts and do that, and Marvin and I were acquainted with that audit staff, and they did a very good job. I am not so sure you can re-create that now. Certainly given the depth, you can just run the list—and Mr. Walker down at the end of the table has run this long list of management challenges at this point, ranging from workforce planning to information technology to secrecy and compartmentation. And I think, again, whether I am putting too much of a burden on GAO at this point, these are the kinds of people that you need to have who are going to be there on a longer-term basis and can really engage in a long-term dialogue on this, which I do not think you are going to get from a contractor, and you are certainly not going to be able to get from oversight committees that are already overburdened at this point.

Let me also add another personal note, and this was an earlier comment that was made with regards to contractors within the community themselves. I can remember when this contracting business really began in terms of a much larger scale. Obviously,

it was precipitated by 2001 and trying to buy quick expertise. The logic, however, was always one in which you supposedly got—the government got something cheaper in the sense of you are able to buy the expertise, but you did not have to pay for the pension, you did not have to pay for the insurance and all the rest of it, ignoring the profit the companies were making on top and still thinking you were making out in the long term. I think the term "human capital" has been used here before today, and I think one of the things the government has cheated themselves out of and to some extent cheated the taxpayer out of is that they may be saving some dollars, and I think there is still some debate as to how much they are saving, but certainly in terms of having the cadre of individuals who can deal with these kinds of issues within the government, I think we have cheated ourselves very badly. And maybe one or two of the places, one or two of the centers of expertise certainly remains in GAO, and I think it is one place that we can go back to fairly quickly to get some oversight on this.

Senator AKAKA. Thank you.

Mr. Walker, as I noted in my opening remarks, in response to a question for the record from Senator Voinovich from a November 2005 hearing of this Subcommittee, GAO stated that it lacked the cooperation needed to ensure progress on the security clearance process. As you know, DNI may assume more responsibility for security clearances in the future.

Given this situation, what specifically would GAO need from Congress and the Intelligence Community to continue making progress on this particular issue?

Mr. WALKER. Well, I think your bill, Senator, reaffirms certain authorities that GAO believes it already has, and I believe it also specifically may reference—if not in the statutory language, the contemplated, legislative history—the issue of security clearances.

Let me restate. I have had a constructive working relationship with Director McConnell, and I think he is a very reasoned and reasonable person. He has a tough enough job in trying to do his job with regard to the 16 different entities in the Intelligence Community. And they do not all have the same attitude.

The biggest problem that we have had on a recurring basis over many years has been the CIA, and not just with regard to whether and to what extent we would do work there, but in their historical unwillingness to cooperate on government-wide initiatives, even in circumstances where other members of the Intelligence Community did. And so I think we need to be precise about where the problem is and where it is not, and I do think that part of the problem is up here on Capitol Hill. I think the intelligence committees have still not come to the realization yet that no matter what their authorities are, no matter how capable their staff are, this is just an area that they are not going to be able to perform effectively, and GAO is the logical place to go, and it really, frankly, would not make sense to go anywhere else.

Senator AKAKA. Further, Mr. Walker, what do you think might be the result or what do you think might happen if GAO is unable to audit the security clearance process in the future?

Mr. WALKER. Well, it is already high risk. It would become higher risk, I can assure you.

Senator AKAKA. Mr. Walker, the DNI is trying to move forward with a new personnel system to unify the Intelligence Community. This, of course, is a lofty goal as practically each element of the IC has been granted different personnel flexibilities and has implemented the use of these flexibilities in an uneven manner.

To date, have you provided any feedback to ODNI as it designs and prepares to implement the new personnel system? If not, would you speak a little bit more on how you could be helpful to the DNI in this area?

Mr. WALKER. Well, Ron Sanders is the chief human capital officer for the ODNI. I have known Mr. Sanders for a number of years. He is a very capable professional. There have been some informal conversations that have taken place with regard to what they are trying to do. I know that they have reached out to us at GAO to learn from our own experience and to draw upon some best practices.

This is an area where I think we could add a lot of value. We have not received a formal request to look at what they have put together. But this is an example of an area where there has been some informal interaction and knowledge sharing, but it is an area where I think we could add value not just to the Congress but to the DNI.

Senator AKAKA. Professor Ott and Mr. Marks, you both also have served in the Intelligence Community working with the CIA. In your experience, how is our national security affected if there is inadequate oversight of the Intelligence Community? Mr. Ott.

Mr. OTT. All right. I will venture out on thin ice here and make what is inherently maybe a tendentious assertion, but I will make it anyway because I believe it.

When you pose a question like this it calls to mind the events of September 11, 2001, and the whole postmortem that was done on that by the 9/11 Commission and the connecting of the dots and the location of bits and pieces of information in various parts of the security community and the Intelligence Community in particular and the failure to bring those together and all of that—the story that we are all very familiar with.

My argument is that if intelligence oversight by the Congress had been functioning in the 1990s and the years immediately up to 2001 the way it had functioned in the 1980s, I believe that, in fact, September 11, 2001 would have been prevented. And the reason is that an effective oversight system, as existed in the SSCI at the time, would have reacted to the 1993 truck bomb in the World Trade Center—and then the subsequent embassy bombings in East Africa—by saying we are now confronting something new, important, and dangerous. We are going to have to dedicate two or three of our professional staff to work this issue full-time. And if that had been done—and I think it would have been done by a 1980s-era committee. If that had been done, you would then have had people from the committee ranging across the Intelligence Community, kicking the tires, asking questions: What are you doing? What are the programs? What do you know? And it is inherent in the nature of oversight that a staff doing that can bridge the stovepipes that compartmentalize information and can say, well, I was out at

the FBI last week, and they told me this. Have you heard that? Well, no, we have not heard that.

That is the process of correcting disparate, proprietary information which a Senate staff can do in the nature of things, actually very easily, but the community often cannot do. Not only that, you get the problem of orthodox thinking: Terrorists will never use airplanes, civilian airplanes. Who says? Well, we came to that conclusion somewhere a long time ago, and it is now sort of set in stone.

Well, Senate staff is not beholden to or captured by bureaucratic orthodoxies. They might react with skepticism. Well, wait a minute. Why do you think that? I was talking to somebody in the civil aviation world who thinks quite differently about that. This is a service that oversight performs if it is done well, and it helps the bureaucracy itself bridge gaps, get outside of compartments, think outside the box, rethink conventional wisdom, and it is an absolutely—in the kind of world that we face today, I think it is absolutely critical.

Senator AKAKA. Mr. Marks.

Mr. MARKS. I will take a slight variation on the theme, Senator, and I will take 2001 as the example because that is probably the best of the lot, at least for right now—maybe Iraq judgments.

September 11, 2001, was a structural intelligence failure. We had a system that was built to do something else, to take on a very slow-moving, steady, Western-oriented Nation State, the U.S.S.R., very predictable, perhaps harder to penetrate but very predictable—hard to penetrate but very predictable. We had structures in place that separated international and domestic information. We had long-term laws in place that had placed some restrictions on a number of different agencies talking to each other. And Marvin is absolutely right. You also had cultures that had developed over the years that really were not dealing with each other.

What you would hope for out of any oversight—and I can certainly see Marvin's point in terms of both the Senate and the House Intelligence Committees. But what you would hope for in any kind of oversight is the ability to look long term, the ability to look over the horizon in the sense of trying to get a handle on what is the next set of problems here. In a lot of ways, the Intelligence Community stopped somewhere around December 25, 1991, when the Soviet Union fell, and maintained a lot of the same structures throughout. And obviously there were cutbacks, etc., and that is all history now. But there are a number of us out there who really believed that there had to be an outside group that was saying to them, look, the situation has changed. People certainly were smart enough to realize it inside, but oftentimes they cannot move within their own bureaucracy to get things done. A good oversight committee—and again this is all hindsight, but good oversight of one form or another would have sent out the warning at this point. We are dealing in a different world now, the old joke being that the best thing that could happen to us is that al-Qaeda would have an international and a domestic desk, that they would not have connection. But they do. And the idea that these technologies that were developing in the 1990s that really were not taken into account, whether it is the ability to get on the Internet, whether it is the ability to make simply international phone calls and commu-

nicate that way, really weren't taken into account within the community.

So, fundamentally, I think I agree with Dr. Ott on this, but at the same time, I do not know how much of that burden could have been taken on by the intelligence committees, given structure and, frankly, given the day-to-day issues that they have to deal with.

Senator AKAKA. Well, I want to thank all of you again for the time that you spent preparing as well as presenting this valuable information to this Subcommittee. This Subcommittee has been very fortunate. I hear all of you clearly, and your thoughts.

Today's hearing for me has been a highlight on the need to improve oversight of the Intelligence Community, particularly as it prepares to implement a host of government-wide management reforms. It is clear to me that GAO, which has the expertise and capacity to do cross-cutting audits and evaluations of IC activities could provide valuable assistance to this effort. GAO's feedback would help Congress understand whether the Intelligence Community programs that it authorizes and funds are working properly. But, more importantly, GAO could help the IC work better.

We should remember that the goal of oversight is not to point fingers at the Intelligence Community or to make newspaper headlines. Rather, the goal is to help the Intelligence Community function as effectively as possible to keep the American people safe.

With that goal in mind, this Subcommittee will continue its attention to this important issue, and you have provided us with valuable insights and information to help us do that.

The hearing record will be open for 2 weeks for additional comments or questions or statements other Members may have, and with that, this hearing is adjourned.

[Whereupon, at 11:45 a.m., the Subcommittee was adjourned.]

APPENDIX

United States Government Accountability Office

GAO

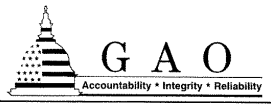
Testimony before the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 10:00 a.m. EST
Friday, February 29, 2008

INTELLIGENCE REFORM

GAO Can Assist the Congress and the Intelligence Community on Management Reform Initiatives

Statement of David M. Walker
Comptroller General of the United States



GAO-08-413T

February 29, 2008

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-08-413T, a testimony before the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Committee on Homeland Security and Governmental Affairs, U.S. Senate

INTELLIGENCE REFORM

GAO Can Assist the Congress and the Intelligence Community on Management Reform Initiatives

Why GAO Did This Study

For decades, GAO has assisted Congress in its oversight role and helped federal departments and agencies with disparate missions to improve the economy, efficiency, and effectiveness of their operations. GAO's work provides important insight on matters such as best practices to be shared and benchmarked and how government and nongovernmental partners can become better aligned to achieve important outcomes for the nation. In addition, GAO provides Congress with foresight by highlighting the long-term implications of today's decisions and identifying key trends and emerging challenges facing our nation before they reach crisis proportions.

For this hearing, GAO was asked to (1) highlight governmentwide issues where it has made a major contribution to oversight and could assist the intelligence and other congressional committees in their oversight of the Intelligence Community, and (2) comment on the potential impact on GAO's access to perform audit work on personnel security clearances if the Office of the Director of National Intelligence (ODNI) were to assume management of this issue from the Office of Management and Budget (OMB). Given historical challenges to GAO's ability to audit the Intelligence Community's programs and activities, this testimony also discusses GAO's views on Senate bill S. 82, known as the Intelligence Community Audit Act of 2007.

To view the full product, click on GAO-08-413T.For more information, contact Davi M. D'Agostino, 202-512-5431 or dagostinod@gao.gov.

What GAO Found

GAO has considerable experience in addressing governmentwide management challenges, including such areas as human capital, acquisition, information technology, strategic planning, organizational alignment, and financial and knowledge management, and has identified many opportunities to improve agencies' economy, efficiency, and effectiveness, and the need for interagency collaboration in addressing 21st century challenges. For example, over the years, GAO has addressed human capital issues, such as acquiring, developing, and retaining talent; strategic workforce planning; building results-oriented cultures; pay for performance; contractors in the workforce; and personnel security clearances, which affect all federal agencies, including the Intelligence Community. Furthermore, GAO identified delays and other impediments in the Department of Defense's (DOD) personnel security clearance program, which also maintains clearances for intelligence agencies within DOD. GAO designated human capital transformation and personnel security clearances as high-risk areas. GAO also recently issued reports addressing Intelligence Community-related management issues, including intelligence, surveillance, and reconnaissance; space acquisitions; and the space acquisition workforce.

If ODNI were to assume management responsibilities over security clearances across the federal government, GAO's ability to continue monitoring this area and provide Congress information for its oversight role could be adversely affected. In 2006, OMB's Deputy Director for Management suggested that OMB's oversight role of the governmentwide security clearance process might be transferred to the ODNI. GAO has established and maintained a relatively positive working relationship with the ODNI, but limitations on GAO's ability to perform meaningful audit and evaluation work persist. While GAO has the legal authority to audit the personnel security clearance area, if the ODNI were to assume management responsibilities over this issue, then it may be prudent to incorporate some legislative provision to reinforce GAO's access to information needed to conduct such audits and reviews.

GAO supports S. 82 and believes that if it is enacted, the agency would be well-positioned to assist Congress in oversight of Intelligence Community management reforms. S. 82 would reaffirm GAO's existing statutory authority to audit and evaluate financial transactions, programs, and activities of elements of the Intelligence Community, and to access records necessary for such audits and evaluations. GAO has clear audit and access authority with respect to elements of the Intelligence Community, subject to a few limited exceptions. However, for many years, the executive branch has not provided GAO the level of cooperation needed to conduct meaningful reviews of elements of the Intelligence Community. This issue has taken on new prominence and is of greater concern in the post-9/11 context, especially since the ODNI's responsibilities extend well beyond traditional intelligence activities. The reaffirmation provisions in the bill should help to ensure that GAO's audit and access authorities are not misconstrued in the future.

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here before you today to address how GAO could assist Congress and the Intelligence Community.[1] You asked that I discuss how GAO's expertise and capacity to perform program reviews of key governmentwide issues, as well as some recent work we have done related to intelligence activities, could be useful in assisting congressional oversight of Intelligence Community management reforms under consideration. Second, as requested, I will comment on the potential impact on GAO's ability to perform audit work on personnel security clearances if the Office of the Director of National Intelligence (ODNI) were to assume management of this issue from the Office of Management and Budget (OMB). Finally, given historical challenges to GAO's ability to audit the Intelligence Community's programs and activities, I would like to discuss GAO's views on Senate bill S. 82, known as the Intelligence Community Audit Act of 2007.[2] My comments today are based primarily on GAO's completed work and on our institutional knowledge, drawn from our prior reviews at the Department of Defense (DOD) and other federal agencies of human capital management, personnel security clearances, and other areas that directly affect the Intelligence Community, as well as on publicly available reports. (See the list of related GAO products at the end of this statement.)

[1] An Intelligence Community member is a federal government agency, service, bureau, or other organization within the executive branch that plays a role in national intelligence. The Intelligence Community consists of the Office of the Director of National Intelligence and 16 different agencies or components: Central Intelligence Agency; Defense Intelligence Agency; Departments of the Army, the Navy, and the Air Force; U.S. Marine Corps; National Geospatial-Intelligence Agency; National Reconnaissance Office; National Security Agency; Department of Energy; Department of Homeland Security; U.S. Coast Guard; Drug Enforcement Administration; Federal Bureau of Investigation; Department of State's Bureau of Intelligence and Research; and Department of the Treasury. The following members of the Intelligence Community are organizationally aligned within the Department of Defense: Defense Intelligence Agency; Departments of the Army, the Navy, and the Air Force; U.S. Marine Corps; National Geospatial-Intelligence Agency; National Reconnaissance Office; and National Security Agency. Additionally, the U.S. Coast Guard is organizationally aligned with the Department of Homeland Security and the Drug Enforcement Administration and the Federal Bureau of Investigation are organizationally aligned with the Department of Justice.

[2] S. 82, *Intelligence Community Audit Act of 2007*, was introduced on January 4, 2007.

Summary

First, GAO has assisted Congress for decades in its oversight role and helped federal departments and agencies with disparate missions to improve the economy, efficiency, and effectiveness of their operations. In addition, GAO's work also provides important insight and foresight to complement the work we have performed for Congress for many years. A number of the governmentwide management challenges we have addressed, such as human capital transformation, acquisition, information technology, strategic planning, organizational alignment, financial and knowledge management, and personnel security clearances, affect most federal agencies, including those within the Intelligence Community. Moreover, we have designated some of these areas as high-risk for the federal government.[3] Human capital transformation and personnel security clearances also have been repeatedly identified as areas of weakness within the Intelligence Community by others, including the Subcommittee on Oversight, House Permanent Select Committee on Intelligence; the Congressional Research Service; and independent commissions.[4] Specifically, strategic human capital transformation and related management reforms; DOD's new pay-for-performance system, known as the National Security Personnel System (NSPS); contractors in the workforce; and personnel security clearances are among the serious challenges going forward. We also have recently completed work on several management issues that are directly related to the Intelligence Community, and we have the capabilities to further support the intelligence and other appropriate congressional committees with their oversight needs. Specifically, we have performed in-depth reviews and issued reports on intelligence, surveillance, and reconnaissance (ISR) systems requirements, operations, and acquisitions; on space acquisitions; and on the space acquisition workforce—issues that are current and

[3] GAO, *High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: January 2007). Agencies within the Intelligence Community also are vulnerable to other high-risk areas, such as contract management, management of interagency contracting, protecting the federal government's information systems and the nation's critical infrastructures, and ensuring the effective protection of technologies critical to U.S. national security interests.

[4] See U.S. Congress, Subcommittee on Oversight, House Permanent Select Committee on Intelligence, *Initial Assessment on the Implementation of The Intelligence Reform and Terrorism Prevention Act of 2004* (Washington, D.C.: July 27, 2006); Congressional Research Service, *Intelligence Issues for Congress*, RL33539 (Washington, D.C.: Updated Dec. 18, 2007); National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (Washington, D.C.: July 22, 2004); and The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States* (Washington, D.C.: Mar. 31, 2005).

critical within the Intelligence Community.[5] For the most part, DOD has agreed with our findings and recommendations. In addition, GAO's highly qualified and experienced staff—including its analysts, auditors, lawyers, and methodologists—and secure facilities position us to perform intensive reviews to assess the transformation and related management reforms under consideration within the Intelligence Community, especially in connection with human capital and acquisition and contracting-related issues.

Second, if the ODNI assumes management of governmentwide personnel security clearances, then GAO's ability to continue to review personnel security clearances could be impaired unless greater cooperation is forthcoming from the Intelligence Community. Although we have established and maintained a relatively positive working relationship with the ODNI, limitations on our ability to perform meaningful audit and evaluation work persist. The ODNI might assume management responsibilities for the security clearance process in the event that either of two potential changes were to occur. First, in 2006, OMB's Deputy Director for Management suggested that the agency's oversight role of the governmentwide security clearance process might be transferred to the ODNI. Alternatively, the ODNI could assume leadership, to some extent, over implementation of a new security clearance process. A team established by the Director of National Intelligence, the Under Secretary of Defense for Intelligence, and OMB's Deputy Director for Management is developing a proposed security clearance process that could be implemented governmentwide. If ODNI were to assume leadership or oversight responsibilities for governmentwide personnel security clearances, then it might be prudent to incorporate some legislative provision to reinforce GAO's access to the information needed to conduct audits and reviews in the personnel security clearance area.

[5] GAO, *Space Based Infrared System High Program and its Alternative*, GAO-07-1088 (Washington, D.C.: Sep. 12, 2007); *DOD is Making Progress in Adopting Best Practices for the Transformational Satellite Communications System and Space Radar but Still Faces Challenges*, GAO-07-1029R (Washington, D.C.: Aug. 2, 2007); *Unmanned Aircraft Systems: Advance Coordination and Increased Visibility Needed to Optimize Capabilities*, GAO-07-836 (Washington, D.C.: July 11, 2007); *Defense Acquisitions: Greater Synergies Possible for DOD's Intelligence, Surveillance, and Reconnaissance Systems*, GAO-07-578 (Washington, D.C.: May 17, 2007); *Intelligence, Surveillance, and Reconnaissance: Preliminary Observations on DOD's Approach to Managing Requirements for New Systems, Existing Assets, and Systems Development*, GAO-07-596T (Washington, D.C.: Apr. 19, 2007); and *Defense Space Activities: Management Actions Are Needed to Better Identify, Track, and Train Air Force Space Personnel*, GAO-06-908 (Washington, D.C.: Sept. 21, 2006).

Third, with the support of Congress and S. 82, GAO would be well-positioned to provide the intelligence and other appropriate congressional committees with an independent, fact-based evaluation of Intelligence Community management reform initiatives. S. 82, if enacted, would amend title 31 of the United States Code to reaffirm GAO's authority to audit and evaluate financial transactions, programs, and activities of the Intelligence Community. The bill also would provide that GAO may conduct an audit or evaluation of intelligence sources and methods or covert actions only upon the request of the intelligence committees or congressional majority or minority leaders. It also would provide that GAO perform such work and use agency documents in space provided by the audited agencies. We support this bill and believe that if it is enacted, GAO would be well-positioned to assist Congress with its oversight functions relating to the Intelligence Community. The reaffirmation provisions in the bill should also help to ensure that GAO's audit and access authorities are not misconstrued in the future.

Background

GAO's Authority to Review Intelligence Community Programs

Generally, we have broad authority to evaluate agency programs and investigate matters related to the receipt, disbursement, and use of public money.[6] To carry out our audit responsibilities, we have a statutory right of access to agency records. Specifically, federal agencies are required to provide us information about their duties, powers, activities, organization, and financial transactions.[7] In concert with our statutory audit and evaluation authority, this provision gives GAO a broad right of access to agency records, including records of the Intelligence Community, subject to a few limited exceptions. GAO's access statute authorizes enforcement of GAO's access rights through a series of steps specified in the statute, including the filing of a civil action to compel production of records in federal district court. However, GAO may not bring an action to enforce its statutory right of access to a record relating to activities that the President designates as foreign intelligence or counterintelligence activities.[8]

[6] 31 U.S.C. §§ 712, 717, 3523, and 3524.

[7] 31 U.S.C. § 716.

[8] 31 U.S.C. § 716(d)(1)(A).

GAO's statutory authorities permit us to evaluate a wide range of activities in the Intelligence Community, including the management and administrative functions that intelligence agencies, such as the Central Intelligence Agency (CIA), have in common with all federal agencies. However, since 1988, the Department of Justice (DOJ) has maintained that Congress intended the intelligence committees to be the exclusive means of oversight, effectively precluding oversight by us. In our 2001 testimony about GAO's access to information on CIA programs and activities, we noted that in 1994 the CIA Director sought to further limit our audit work of intelligence programs, including those at DOD.[9] In 2006, the ODNI agreed with DOJ's 1988 position, stating that the review of intelligence activities is beyond GAO's purview. While we strongly disagree with DOJ and the ODNI's view,[10] we foresee no major change in limits on our access without substantial support from Congress—the requestor of the vast majority of our work. Congressional impetus for change would have to include the support of the intelligence committees, which have generally not requested GAO reviews or evaluations of CIA's or other intelligence agencies' activities for many years. With support, however, we could evaluate some of the basic management functions that we now evaluate throughout other parts of the federal government, such as human capital, acquisition, information technology, strategic planning, organizational alignment, and financial and knowledge management.

Intelligence Reform and Terrorism Prevention Act of 2004

As this Subcommittee is well aware, the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) established the Director of National Intelligence to serve as the head of the Intelligence Community; act as the principal advisor to the President, the National Security Council, and the Homeland Security Council for intelligence matters related to national security; and oversee and direct the implementation of the National Intelligence Program.[11] Since its inception, the ODNI has undertaken a number of initiatives, including the development of both 100- and 500-day plans for integration and collaboration. One of the core

[9] GAO, *Central Intelligence Agency: Observations on GAO Access to Information on CIA Programs and* Activities, GAO-01-975T (Washington, D.C.: July 18, 2001).

[10] DOJ's position and our analysis is set forth in more detail in GAO, *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive But Unclassified Information*, GAO-06-385 (Washington, D.C.: Mar. 17, 2006).

[11] Pub. L. No. 108-458 § 1011 (2004) (codified at 50 U.S.C. § 403).

initiatives of these plans is to modernize the security clearance process across the Intelligence Community and at the national level, where other federal agencies, including DOD, OMB, and Office of Personnel Management (OPM) are also engaged.

Among other things, IRTPA also directed the President to select a single department, agency, or element of the executive branch to be responsible for day-to-day oversight of the government's security clearance process.[12] In June 2005, the President issued an executive order that assigned OMB responsibility for ensuring the effective implementation of a policy that directs agency functions related to determinations of personnel eligibility for access to classified information be uniform, centralized, efficient, effective, timely, and reciprocal.[13] In its new capacity, OMB assigned the responsibility for the day-to-day supervision and monitoring of security clearance investigations, as well as for tracking the results of individual agency-performed adjudications, to OPM. With respect to (1) personnel employed or working under a contract for an element of the Intelligence Community and (2) security clearance investigations and adjudications for Sensitive Compartmented Information, OMB assigned the responsibility for supervision and monitoring of security clearance investigations and tracking adjudications to the ODNI. In May 2006, OMB's Deputy Director for Management stated during a congressional hearing that the agency's oversight role in improving the governmentwide clearance process might eventually be turned over to the ODNI.[14]

[12] Pub. L. No. 108-458 § 3001(b) (2004).

[13] The White House, Executive Order 13381, *Strengthening Processes Relating to Determining Eligibility for Access to Classified National Security Information* (Washington, D.C.: June 27, 2005), as amended.

[14] Senate Committee on Homeland Security and Governmental Affairs, *Progress or More Problems: Assessing the Federal Government's Security Clearance Process*, S. Hrg 109-621 (Washington, D.C.: May 17, 2006).

GAO Experience in Governmentwide Human Capital Issues and Other Management Areas Can Assist Congress and the Intelligence Community on Management Reforms

For decades, we have assisted Congress in its oversight role and helped agencies with disparate missions to improve the economy, effectiveness, and efficiency of their operations and the need for interagency collaboration in addressing 21st century challenges, and we could assist the intelligence and other appropriate congressional committees in their oversight of the Intelligence Community as well. Our work also provides important insight on matters such as best practices to be shared and benchmarked and how government and its nongovernmental partners can become better aligned to achieve important outcomes for the nation. In addition, GAO provides Congress with foresight by highlighting the long-term implications of today's decisions and identifying key trends and emerging challenges facing our nation before they reach crisis proportions. For the purpose of this hearing, I will discuss our extensive experience in addressing governmentwide human capital issues and other management issues that can assist the intelligence and other appropriate congressional committees in their oversight of Intelligence Community transformation and related management reforms.

Human Capital Transformation and Management Are Governmentwide High-Risk Issues also Affecting the Intelligence Community

GAO has identified a number of human capital transformation and management issues over the years, such as acquisition, information technology, strategic planning, organizational alignment, financial and knowledge management, and personnel security clearances, as cross-cutting, governmentwide issues that affect most federal agencies, including those within the Intelligence Community. Human capital transformation and management issues have also been repeatedly identified as areas of weakness within the Intelligence Community by other organizations, including the Subcommittee on Oversight, House Permanent Select Committee on Intelligence; the Congressional Research Service; and independent commissions, such as the 9/11 Commission and Weapons of Mass Destruction Commission.[15] Moreover, the ODNI has acknowledged that Intelligence Community agencies face some of the governmentwide challenges that we have identified, including integration and collaboration within the Intelligence Community workforce and

[15] GAO, *Intelligence Reform: Human Capital Considerations Critical to 9/11 Commission's Proposed Reforms*, GAO-04-1084T (Washington, D.C.: Sept. 14, 2004). Also see *Intelligence Issues For Congress; The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States;* and *Report to the President of the United States.*

inefficiencies and reciprocity of personnel security clearances.[16] Significant issues affecting the Intelligence Community include strategic human capital transformation and reform issues, DOD's new pay-for-performance management system called NSPS, the extent to which agencies rely on, oversee, and manage their contractor workforce, and personnel security clearances. In fact, we have identified some of these programs and operations as high-risk areas due to a range of management challenges.[17]

Strategic Human Capital Transformation and Related Management Reforms across the Government

GAO and others have reported that the Intelligence Community faces a wide range of human capital challenges, including those dealing with recruiting and retaining a high-quality diverse workforce, implementation of a modernized performance management system, knowledge and skill gaps, integration and collaboration, and succession planning. Our extensive work on government transformation distinctly positions us to assist the intelligence and other appropriate congressional committees to oversee the Intelligence Community's efforts to address these human capital challenges as well as to inform congressional decision making on management issues. Our work on governmentwide strategic human capital management is aimed at transforming federal agencies into results-oriented, high-performing organizations. Transformation is necessary because the federal government is facing new and more complex challenges than ever before, and agencies must re-examine what they do and how they do it in order to meet those challenges. Central to this effort are modern, effective, economical, and efficient human capital practices, policies, and procedures integrated with agencies' mission and program goals.

In 2001, we added strategic human capital management to the list of governmentwide high-risk areas because of the long-standing lack of a consistent strategic approach for marshaling, managing, and maintaining the human capital needed to maximize government performance and ensure its accountability. Although the federal government made progress in addressing these issues in the years that followed, we found that more can be done in four key areas: (1) top leadership in agencies must provide

[16] ODNI, *United States Intelligence Community 100 Day Plan for Integration and Collaboration* (Washington, D.C.: Apr. 11, 2007) and Office of the Director of National Intelligence, *The US Intelligence Community's Five Year Strategic Human Capital Plan* (Washington, D.C.: June 22, 2006).

[17] GAO-07-310.

the attention needed to address human capital and related organizational transformation issues; (2) agencies' human capital planning efforts need to be fully integrated with mission and program goals; (3) agencies need to enhance their efforts to acquire, develop, and retain talent; and (4) organizational cultures need to promote high performance and accountability.

NSPS Is a Key Example of GAO's Programmatic Review of Human Capital Transformation Challenges

Based on our experience in addressing agencies' performance management challenges, we are uniquely positioned to help Congress evaluate such issues within the Intelligence Community, including the development and implementation of its pay-for-performance personnel management system.[18] As an example of our experience in this area, I would like to highlight our work on DOD's new civilian personnel management system—the NSPS—which has provided Congress with insight on DOD's proposal, design, and implementation of this system. The National Defense Authorization Act for Fiscal Year 2004[19] provided DOD with authority to establish a new framework of rules, regulations, and processes to govern how the almost 700,000 defense employees are hired, compensated, promoted, and disciplined.[20] Congress provided these authorities in response to DOD's position that the inflexibility of the federal personnel systems was one of the most important constraints to the department's ability to attract, retain, reward, and develop a civilian workforce to meet the national security mission of the 21st century.

Prior to the enactment of the NSPS legislation in 2003, we raised a number of critical issues about the proposed system in a series of testimonies before three congressional committees.[21] Since then, we have provided congressional committees with insight on DOD's process to design its new

[18] Section 308 of H.R. 2082, the bill to authorize appropriations for fiscal year 2008 for the Intelligence Community, would require the Director of National Intelligence to submit to Congress a detailed plan for the compensation-based system of a particular element of the Intelligence Community before it is implemented.

[19] Pub. L. No. 108-136, § 1101 (2003).

[20] The Department of Homeland Security also has received new statutory authority to help manage its workforce more strategically.

[21] GAO, *Defense Transformation: Preliminary Observations on DOD's Proposed Civilian Personnel Reforms*, GAO-03-717T (Washington, D.C.: Apr. 29, 2003); *Defense Transformation: DOD's Proposed Civilian Personnel Systems and Governmentwide Human Capital Reform*, GAO-03-741T (Washington, D.C.: May 1, 2003); and *Human Capital: Building on DOD's Reform Efforts to Foster Governmentwide Improvements*, GAO-03-851T (Washington, D.C.: June 4, 2003).

personnel management system, the extent to which DOD's process reflects key practices for successful transformation, the need for internal controls and transparency of funding, and the most significant challenges facing DOD in implementing NSPS.[22]

Most important, we have noted in testimonies and reports that DOD and other federal agencies must ensure that they have the necessary institutional infrastructure in place before implementing major human capital reform efforts, such as NSPS. This institutional infrastructure includes, at a minimum, a human capital planning process that integrates the agency's human capital policies, strategies, and programs with its program goals, mission, and desired outcomes; the capabilities to effectively develop and implement a new human capital system; and the existence of a modern, effective, and credible performance management system that includes adequate safeguards to ensure a fair, effective, nondiscriminatory, and credible implementation of the new system. While GAO strongly supports human capital reform in the federal government, how it is done, when it is done, and the basis upon which it is done can make all the difference in whether such efforts are successful.

Contractor Workforce in Government Is an Emerging Governmentwide Issue also Acknowledged as a Challenge for the Intelligence Community

An additional major issue of growing concern, both within and outside the Intelligence Community, deals with the type of work that is being performed by contractors, the need to determine the appropriate mix of government and contractor employees to meet mission needs, and the adequacy of oversight and accountability of contractors.[23] These are areas where we also are well-positioned to provide additional support to the intelligence committees. While there are benefits to using contractors to perform services for the government—such as increased flexibility in fulfilling immediate needs—GAO and others have raised concerns about

[22] GAO, *Human Capital: DOD Needs Better Internal Controls and Visibility Over Costs for Implementing Its National Security Personnel System*, GAO-07-851 (Washington, D.C.: July 16, 2007) and *Human Capital: Observations on Final Regulations for DOD's National Security Personnel System*, GAO-06-227T (Washington, D.C.: Nov. 17, 2006).

[23] For example, Section 307 of H.R. 2082, the bill to authorize appropriations for fiscal year 2008 for the Intelligence Community, would require the Director of National Intelligence to submit a report to the congressional intelligence committees describing the personal services activities performed by contractors across the Intelligence Community, the impact of such contractors on the Intelligence Community workforce, plans for conversion of contractor employment into government employment, and the accountability mechanisms that govern the performance of such contractors.

the federal government's increasing reliance on contractor services.[24] A key concern is the risk associated with contractors providing services that closely support inherently governmental functions. Inherently governmental functions require the exercise of discretion in applying government authority and/or in making decisions for the government; as such, they should be performed by government employees, not contractors.[25] In 2007, I testified before the Senate Committee on Homeland Security and Governmental Affairs that the proper role of contractors in providing services to the government was the topic of some debate.[26] I would like to reiterate that, in general, I believe there is a need to focus greater attention on which functions and activities should be contracted out and which should not, to review and reconsider the current independence and conflict-of-interest rules relating to contractors, and to identify the factors that prompt the government to use contractors in circumstances where the proper choice might be the use of civil servants or military personnel. Similarly, it is important that the federal government maintain an accountable and capable workforce, responsible for strategic planning and management of individual programs and contracts.

In a September 2007 report, we identified a number of concerns regarding the risk associated with contractors providing services that closely support inherently governmental functions.[27] For example, an increasing reliance on contractors to perform services for core government activities challenges the capacity of federal officials to supervise and evaluate the performance of these activities. The Federal Acquisition Regulation (FAR) provides agencies examples of inherently governmental functions that should not be performed by contractors.[28] For example, the direction and control of intelligence and counter-intelligence operations are listed as

[24] See, for example, GAO, *Highlights of a GAO Forum: Federal Acquisition Challenges and Opportunities in the 21st Century*, GAO-07-45SP (Washington, D.C.: Oct. 6, 2006) and Acquisition Advisory Panel, *Report of the Acquisition Advisory Panel to the Office of Federal Procurement Policy and the United States Congress* (January 2007).

[25] OMB Circular A-76, Performance of Commercial Activities, May 29, 2003; Federal Acquisition Regulation, Subpart 7.5.

[26] GAO, *Federal Acquisitions and Contracting: Systemic Challenges Need Attention*, GAO-07-1098T (Washington, D.C.: July 17, 2007).

[27] GAO, *Department of Homeland Security: Improved Assessment and Oversight Needed to Manage Risk of Contracting for Selected Services*, GAO-07-990 (Washington, D.C.: Sept. 17, 2007).

[28] FAR § 7.503(c).

inherently governmental functions.[29] Yet in 2006, the Director of National Intelligence reported that the Intelligence Community finds itself in competition with its contractors for employees and is left with no choice but to use contractors for work that may be "borderline inherently governmental."[30] Unless the federal government, including Intelligence Community agencies, pays the needed attention to the types of functions and activities performed by contractors, agencies run the risk of losing accountability and control over mission-related decisions.

Personnel Security Clearances Continue to Experience Delays and Impediments

For more than 3 decades, GAO's reviews of personnel security clearances have identified delays and other impediments in DOD's personnel security clearance program, which maintains about 2.5 million clearances, including clearances for intelligence agencies within DOD. These long-standing problems resulted in our adding the DOD personnel security clearance program to our high-risk list in January 2005. One important outgrowth of this designation has been the level of congressional oversight from this Subcommittee, as well as some progress.[31]

In the past few years, several positive changes have been made to DOD—as well as governmentwide—clearance processes because of increased congressional oversight, recommendations from our work, and new legislative and executive requirements. One of OMB's efforts to improve the security clearance process involved taking a lead in preparing a November 2005 strategic plan to improve personnel security clearance processes governmentwide. In its February 2007 and 2008 annual IRTPA-mandated reports to Congress,[32] OMB noted additional improvements that

[29] FAR § 7.503(c)(8).

[30] *The US Intelligence Community's Five Year Strategic Human Capital Plan.*

[31] GAO, *DOD Personnel Clearances: Delays and Inadequate Documentation Found for Industry Personnel*, GAO-07-842T (Washington, D.C.: May 17, 2007); *DOD Personnel Clearances: New Concerns Slow Processing of Clearances for Industry Personnel*, GAO-06-748T (Washington, D.C.: May 17, 2006); *DOD Personnel Clearances: Government Plan Addresses Some Long-standing Problems with DOD's Program, But Concerns Remain*, GAO-06-233T (Washington, D.C.: Nov. 9, 2005); and *DOD Personnel Clearances: Some Progress Has Been Made but Hurdles Remain to Overcome the Challenges That Led to GAO's High-Risk Designation*, GAO-05-842T (Washington, D.C.: June 28, 2005).

[32] Office of Management and Budget, *Report of the Security Clearance Oversight Group Consistent with Title III of the Intelligence Reform and Terrorism Prevention Act of 2004* (February 2007), and *Report of the Security Clearance Oversight Group Consistent with Title III of the Intelligence Reform and Terrorism Prevention Act of 2004*, (February 2008).

had been made to the security clearance process governmentwide. For example, OMB had issued standards for reciprocity (an agency's acceptance of a clearance issued by another agency), OPM had increased its investigative workforce, and DOD and other agencies had dramatically increased their use of OPM's Electronic Questionnaires for Investigations Processing system to reduce the time required to get a clearance by 2 to 3 weeks. Further, the Director of National Intelligence, the Under Secretary of Defense for Intelligence, and OMB's Deputy Director for Management established a team, the Joint Security Clearance Process Reform Team, to improve the security clearance process. The team is to develop a transformed, modernized, and reciprocal security clearance process that is supposed to be universally applicable to DOD, the Intelligence Community, and other federal agencies. The extent to which this new process will be implemented governmentwide, or whether leadership of the new system will be assigned to the ODNI, however, remains uncertain.

Any attempts to reform the current security clearance process, regardless of which agency or organization undertakes the effort, should include some key factors. Specifically, current and future efforts to reform personnel security clearance processes should consider, among other things, determining whether clearances are required for positions, incorporating more quality control throughout the clearance processes to supplement current emphases on timeliness, establishing metrics for assessing all aspects of clearance processes, and providing Congress with the long-term funding requirements of security clearance reform.

Although we have not worked with the entire Intelligence Community as part of our body of work on security clearances, we have worked with DOD intelligence agencies. For example, in the period from 1998 through 2001, we reviewed National Security Agency clearance investigative reports and Defense Intelligence Agency adjudicative reports. Similarly, our February 2004 report examined information about adjudicative backlogs DOD-wide and the situation in those two intelligence agencies.[33] Importantly, since 1974, we have been examining personnel security clearances mostly on behalf of Congress and some on behalf of this Subcommittee. Through scores of reports and testimonies, we have acquired broad institutional knowledge that gives us a historical view of

[33] GAO, *DOD Personnel Clearances: DOD Needs to Overcome Impediments to Eliminating Backlog and Determining Its Size*, GAO-04-344 (Washington, D.C.: Feb. 9, 2004).

key factors that should be considered in clearance reform efforts. We are well positioned to assist Congress in its oversight of this very important area.

Recent GAO Reviews of Intelligence-Related Programs and Activities

In addition to our work on human capital transformation and personnel security clearance issues, our recent work has also addressed management issues—such as ISR systems, space acquisitions, and the space acquisition workforce—that directly affect the Intelligence Community and illustrate our ability to further support the intelligence and other appropriate congressional committees in their oversight roles. GAO's highly qualified and experienced staff—including its analysts, auditors, lawyers, and methodologists—and secure facilities position us to perform intensive reviews that could be useful in assessing the transformation and related management reforms under consideration within the Intelligence Community, especially in connection with human capital and acquisition and contracting-related issues. GAO personnel who might perform work relating to the Intelligence Community have qualifications, skills, expertise, clearances and accesses, and experience across the federal government, in the national security arena, and across disciplines. For example, GAO methodologists have expertise in designing and executing appropriate methodological approaches that help us develop recommendations to improve government operations. Our attorneys advise GAO's analysts, issue external legal decisions and legal opinions, and prepare testimony, legislation, and reports on subjects reflecting the range of government activity. This legal work, for example, involves subjects such as information technology, international affairs and trade, foreign military sales, health and disability law, and education and labor law. GAO also already has personnel with appropriate clearances and accesses. I would like to highlight a couple of examples of GAO's work to demonstrate our expertise and capacity to perform intensive reviews in intelligence-related matters.

GAO's Work Addressing ISR Requirements, Operations, and Acquisitions Identified Opportunities for Improvement

In the past year, we have testified and issued reports addressing DOD's ISR systems, including unmanned aircraft systems. The term "ISR" encompasses multiple activities related to the planning and operation of sensors and assets that collect, process, and disseminate data in support of current and future military operations. Intelligence data can take many forms, including optical, radar, or infrared images, or electronic signals. In April 2007, we testified that DOD has taken some important first steps to formulate a strategy for improving the integration of future ISR requirements, including the development of an ISR Integration Roadmap and designating ISR as a test case for its joint capability portfolio

management concept. We also testified that opportunities exist for different services to collaborate on the development of similar weapon systems as a means for creating a more efficient and affordable way of providing new capabilities to the warfighter.[34] As part of another review of ISR programs, we found that nearly all of the systems in development we examined had experienced some cost or schedule growth.[35] As part of our work, we selected 20 major airborne ISR programs and obtained information on current or projected operational capabilities, acquisition plans, cost estimates, schedules, and estimated budgets.[36] We analyzed the data to determine whether pairs of similar systems shared common operating concepts, capabilities, physical configurations, or primary contractors. We reviewed acquisition plans for programs in development to determine whether they had established sound business cases or, if not, where the business case was weak. We reviewed cost and schedule estimates to determine whether they had increased and, where possible, identified reasons for the increases. Based on our research and findings, we recommended that DOD develop and implement an integrated enterprise-level investment strategy, as well as report to the congressional defense committees the results of ISR studies underway and identify specific plans and actions it intends to take to achieve greater jointness in ISR programs. DOD generally agreed with our recommendations.

We have also performed in-depth reviews of individual space programs that are shared with the Intelligence Community. For example, in recent years we have examined the Space Radar program, which is expected to be one of the most complex and expensive satellite developments ever. We reported that while the program was adopting best practices in technology development, its schedule estimates may be overly optimistic and its overall affordability for DOD, which was parternering with the Intelligence Community, was questionable.[37] Our concerns were cited by the Senate Select Committee on Intelligence in its discussion of reasons for reducing funding for Space Radar.[38]

[34] GAO-07-596T.

[35] GAO-07-578.

[36] These programs were either in technology or systems development, already fielded but undergoing significant upgrade, or operating in the field but due to be replaced by a system in development and one space-based program in technology development.

[37] GAO-07-1029R.

[38] S. Rep. No. 110-75, at 48 (2007).

GAO's Work on the Space Acquisition Workforce Recommended Management Improvements

Our work on the space acquisition workforce is another example of in-depth programmatic reviews we have been able to perform addressing intelligence-related matters. In a September 2006 report, we identified a variety of management issues dealing with Air Force space personnel.[39] This is a critical issue because the Air Force provides over 90 percent of the space personnel to DOD, including the National Reconnaissance Office (NRO). We found that the Air Force has done needs assessments on certain segments of its space workforce, but it has not done an integrated, zero-based needs assessment of its space acquisition workforce. In the absence of an integrated, zero-based needs assessment of its space acquisition workforce and a career field specialty, the Air Force cannot ensure that it has enough space acquisition personnel or personnel who are technically proficient to meet national security space needs—including those in the Intelligence Community. As a part of this work, we collected and analyzed Air Force personnel data in specific specialty codes related to space acquisition and tracked their career assignments, training, and progression, including those assigned to the NRO. For example, we collected and analyzed data on space acquisition positions and personnel from multiple locations, and conducted discussion groups about topics including education and prior experience with junior and midgrade officers at the Space and Missile Systems Center in California. We made recommendations to DOD to take actions to better manage its limited pool of space acquisition personnel, and DOD generally agreed with our findings and recommendations.

GAO's Access to Perform Audit Work Could be Affected If the ODNI Assumes Management of Personnel Security Clearances

Our ability to continue monitoring security clearance-related problems in DOD as well as other parts of the federal government and to provide Congress with information for its oversight role could be adversely affected if the ODNI assumes management responsibility over this area. First, in 2006, OMB's Deputy Director for Management has suggested that the agency's oversight role of the governmentwide security clearance process might be transferred to the ODNI. Alternatively, the ODNI could assume leadership, to some extent, of a new security clearance process that is intended for governmentwide implementation by a team established by the Director of National Intelligence, the Under Secretary of Defense for Intelligence, and OMB's Deputy Director for Management. While we have the legal authority to audit the personnel security clearance area if its

[39] GAO-06-908.

oversight is moved to the ODNI or if the Joint Security Clearance Process Reform Team's proposed process is implemented governmentwide, we could face difficulties in gaining the cooperation we need to access the information.

Although we have established and maintained a relatively positive working relationship with the ODNI, limitations on our ability to perform meaningful audit and evaluation work persist. Specifically, we routinely request and receive substantive threat briefings and copies of finished intelligence products prepared under the ODNI, and we meet with officials from the ODNI and obtain information about some of their activities. We also receive the ODNI agency comments and security reviews on most of our draft reports, as appropriate. However, since some members of the Intelligence Community have taken the position that the congressional intelligence committees have exclusive oversight authority, we do not audit or evaluate any programs or activities of the ODNI, nor are we able to verify or corroborate factual briefings or information provided. This resistance to providing us access to information has taken on new prominence and is of greater concern in the post-9/11 context, especially since the Director of National Intelligence has been assigned responsibilities addressing issues that extend well beyond traditional intelligence activities. For example, the ODNI and the National Counterterrorism Center refused to provide us security-related cost data for the 2006 Olympic Winter Games in Turin, Italy, although we were provided this type of data in prior reviews of the Olympic Games.

If we continue to experience limitation on the types and amounts of information we can obtain from the Intelligence Community, then GAO may not be able to provide Congress with an independent, fact-based evaluation of the new security clearance process during its development and, later, its implementation. Either of these actions could occur without legislation. If the ODNI were to take leadership or oversight responsibilities for governmentwide personnel security clearances, it might be prudent to incorporate some legislative provision to reinforce GAO's access to the information needed to conduct audits and reviews in the personnel security clearance area.

GAO Comments on the Intelligence Community Audit Act of 2007

Finally, GAO supports S. 82 and we would be well-positioned to provide Congress with an independent, fact-based evaluation of Intelligence Community management reform initiatives with the support of Congress and S. 82. Specifically, S. 82 would, if enacted, reaffirm GAO's authority, under existing statutory provisions, to audit and evaluate financial transactions, programs, and activities of elements of the Intelligence Community, and to access records necessary for such audits and evaluations. GAO has clear audit and access authority with respect to elements of the Intelligence Community,[40] subject to a few limited exceptions. However, since 1988, DOJ and some members of the Intelligence Community have questioned GAO's authority in this area. In addition, for many years, the executive branch has not provided GAO with the level of cooperation needed to conduct meaningful reviews of elements of the Intelligence Community. As previously noted, this issue has taken on new prominence and is of greater concern in the post-9/11 context, especially since the Director of National Intelligence has been assigned responsibilities addressing issues that extend well beyond traditional intelligence activities, such as information sharing. The implications of executive branch resistance to GAO's work in the intelligence area were highlighted when the ODNI refused to comment on GAO's March 2006 report involving the government's information-sharing efforts, maintaining that DOJ had "previously advised" that "the review of intelligence activities is beyond the GAO's purview." We strongly disagree with this view. GAO has broad statutory authorities to audit and evaluate agency financial transactions, programs, and activities, and these authorities apply to reviews of elements of the Intelligence Community.[41]

Importantly, S. 82, in reaffirming GAO's authorities, recognizes that GAO may conduct reviews, requested by relevant committees of jurisdiction, of matters relating to the management and administration of elements of the Intelligence Community in areas such as strategic planning, financial management, information technology, human capital, knowledge management, information sharing, organizational transformation and management reforms, and collaboration practices. In recognition of the heightened level of sensitivity of audits and evaluations relating to intelligence sources and methods or covert actions, this bill would restrict

[40] IRTPA (Pub. L. No. 108-458), which established a Director of National Intelligence, did not alter GAO's authority to audit and evaluate financial transactions, programs, and activities of elements of the Intelligence Community.

[41] DOJ's position and our analysis of it is set forth in more detail in GAO-06-385.

GAO audits and evaluations of intelligence sources and methods or covert actions to those requested by the intelligence committees or congressional majority or minority leaders. In addition, in the context of reviews relating to intelligence sources and methods or covert actions, the bill contains several information security-related provisions. The bill includes, for example, provisions (1) requiring GAO to perform our work and use agency documents in facilities provided by the audited agencies; (2) requiring GAO to establish, after consultation with the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives, procedures to protect such classified and other sensitive information from unauthorized disclosure; and (3) limiting GAO's reporting of results of such audits and evaluations strictly to the original requester, the Director of National Intelligence, and the head of the relevant element of the Intelligence Community. In our view, Congress should consider amending the bill language to include the intelligence committees in these reporting provisions when the congressional leadership is the original requester.

The reaffirmation provisions in the bill should help to ensure that GAO's audit and access authorities are not misconstrued in the future. One particularly helpful provision in this regard is the proposed new section 3523a(e) of title 31, specifying that no "provision of law shall be construed as restricting or limiting the authority of the Comptroller General to audit and evaluate, or obtain access to the records of, elements of the intelligence community absent specific statutory language restricting or limiting such audits, evaluations, or access to records." This provision makes clear that, unless otherwise specified by law, GAO has the right to evaluate and access the records of elements of the Intelligence Community pursuant to its authorities in title 31 of the United States Code.

Chairman Akaka, Senator Voinovich, and Members of the Subcommittee, this concludes my prepared testimony. I would be happy to respond to any questions that you or other Members of the Subcommittee may have at this time.

Contact and Acknowledgments

For further information regarding this testimony, please contact Davi M. D'Agostino, Director, Defense Capabilities and Management, at (202) 512-5431 or dagostinod@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals who made key contributions to this testimony are Mark A. Pross, Assistant Director; Tommy Baril; Cristina T.

Chaplain; Jack E. Edwards; Brenda S. Farrell; Robert N. Goldenkoff; John P. Hutton; Julia C. Matta; Erika A. Prochaska; John Van Schaik; Sarah E. Veale; and Cheryl A. Weissman.

Related GAO Products

General Cross-Cutting Issues

GAO Strategic Plan 2007-2012. GAO-07-1SP. Washington, D.C.: March 2007.

High Risk Series: An Update. GAO-07-310. Washington, D.C.: January 2007.

Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies. GAO-06-15. Washington, D.C.: October 21, 2005.

Defense Management: Key Elements Needed to Successfully Transform DOD Business Operations. GAO-05-629T. Washington, D.C.: April 28, 2005.

DOD's High-Risk Areas: Successful Business Transformation Requires Sound Strategic Planning and Sustained Leadership. GAO-05-520T. Washington, D.C.: April 13, 2005.

High-Risk Series: An Update. GAO-05-207. Washington, D.C.: January 2005.

Results-Oriented Cultures: Implementation Steps to Assist Mergers and Organizational Transformations. GAO-03-669. Washington, D.C.: July 2, 2003.

Human Capital

Human Capital: Federal Workforce Challenges in the 21st Century. GAO-07-556T. Washington, D.C.: March 6, 2007.

Intelligence Reform: Human Capital Considerations Critical to 9/11 Commission's Proposed Reforms. GAO-04-1084T. Washington, D.C.: September 14, 2004.

Aviation Security: Federal Air Marshal Service Is Addressing Challenges of Its Expanded Mission and Workforce but Additional Actions Needed. GAO-04-242. Washington, D.C.: November 19, 2003.

High-Risk Series: Strategic Human Capital Management. GAO-03-120. Washington, D.C.: January 2003.

National Security Personnel System

Human Capital: DOD Needs Better Internal Controls and Visibility over Costs for Implementing Its National Security Personnel System. GAO-07-851. Washington, D.C.: July 16, 2007.

Human Capital: Observations on Final Regulations for DOD's National Security Personnel System. GAO-06-227T. Washington, D.C.: November 17, 2005.

Human Capital: DOD's National Security Personnel System Faces Implementation Challenges. GAO-05-730. Washington, D.C.: July 14, 2005.

Contracting Workforce in Government

Military Operations: Implementation of Existing Guidance and Other Actions Needed to Improve DOD's Oversight and Management of Contractors in Future Operations. GAO-08-436T. Washington, D.C.: January 24, 2008.

Federal-Aid Highways: Increased Reliance on Contractors Can Pose Oversight Challenges for Federal and State Officials. GAO-08-198. Washington, D.C.: January 8, 2008.

Department of Homeland Security: Improved Assessment and Oversight Needed to Manage Risk of Contracting for Selected Services. GAO-07-990. Washington, D.C.: September 17, 2007.

Federal Acquisitions and Contracting: Systemic Challenges Need Attention. GAO-07-1098T. Washington, D.C.: July 17, 2007.

Defense Acquisitions: Improved Management and Oversight Needed to Better Control DOD's Acquisition of Services. GAO-07-832T. Washington, D.C.: May 10, 2007.

Security Clearances

Personnel Clearances: Key Factors to Consider in Efforts to Reform the Security Processes. GAO-08-352T. Washington, D.C.: February 27, 2008.

DOD Personnel Clearances: Improved Annual Reporting Would Enable More Informed Congressional Oversight. GAO-08-350. Washington, D.C.: February 13, 2008.

DOD Personnel Clearances: Delays and Inadequate Documentation Found for Industry Personnel. GAO-07-842T. Washington, D.C.: May 17, 2007.

DOD Personnel Clearances: New Concerns Slow Processing of Clearances for Industry Personnel. GAO-06-748T. Washington, D.C.: May 17, 2006.

DOD Personnel Clearances: Government Plan Addresses Some Long-standing Problems with DOD's Program, But Concerns Remain. GAO-06-233T. Washington, D.C.: November 9, 2005.

DOD Personnel Clearances: Some Progress Has Been Made but Hurdles Remain to Overcome the Challenges That Led to GAO's High-Risk Designation. GAO-05-842T. Washington, D.C.: June 28, 2005.

DOD Personnel Clearances: DOD Needs to Overcome Impediments to Eliminating Backlog and Determining Its Size. GAO-04-344. Washington, D.C.: Feb. 9, 2004.

Statement of Marvin C. Ott, Professor
National Security Policy, National War College,
National Defense University

Mr. Chairman, Members of the Committee: thank you for the opportunity to testify before you concerning the "Intelligence Audit Act of 2007." This legislation and this hearing address a matter of direct, concrete relevance to the national security of the United States.

Let me begin with two propositions: (1) High quality, timely intelligence is absolutely critical to the national security of the United States; (2) Effective oversight is a vital, even irreplaceable, prerequisite for maintaining a community of agencies that can produce such intelligence. The first of these propositions is, I believe, beyond debate. The threats that confront this nation in a post-9/11 world, particularly from international terrorist networks, are often a mismatch for conventional military assets, but they are tailor-made for intelligence agencies. Such agencies were created to combat secretive adversaries and to do so with a variety of clandestine methods. The second proposition requires a bit more explication.

Power, held in secret and used in secret, is inherently subject to abuse. The Church and Pike Committee Hearings in the 1970s exposed the abuses that had occurred as intelligence agencies operated without effective oversight by either the Congress or the Executive. Members of this body will appreciate how difficult legislative oversight of intelligence really is. It juxtaposes the open, public world of a democratic legislature with the secretive, closed world of clandestine intelligence. It requires mixing oil and water and they don't mix easily. Nevertheless, for a number of years – notably the decade of the 1980s – the Senate, in particular, did establish a system of effective oversight. The key ingredients of this success included a Chairman and Vice-Chairman determined that the Senate Select Committee on Intelligence (SSCI) would function in an entirely nonpartisan fashion and a staff composed of nonpartisan professionals – most of them former career intelligence officials. As part of its oversight responsibilities, the Senate Committee initiated legislation establishing a statutory Inspector General (IG), confirmable by the Senate, at the CIA.

It was in this environment in 1987 that Senator Glenn, Chairman of this Committee and a member of the Intelligence Committee introduced S1458 providing for GAO audits of the CIA. That bill ultimately failed to get sufficient support for passage. The principal argument against it at the time was that an effective system of oversight already existed with the House and Senate Intelligence Oversight Committees as well as the CIA IG, which was formally established two years later. Therefore, empowerment of the GAO as an additional vehicle for oversight was unnecessary.

That argument at that time was plausible. But the landscape has changed in three key respects since 1987. First, the quality and effectiveness of Congressional oversight has declined drastically. Second, the size and complexity of the Intelligence Community has grown dramatically and the contracting and procurement practices have begun to mirror normal government practice. Third, the security threats facing this country have become increasingly complex and diverse. Let's briefly examine each in turn.

When Senator David Boren left the Chairmanship of the SSCI in 1991 he and his long-time Vice-Chairman, Senator William Cohen, bequeathed to their successors a remarkably effective, professional system of intelligence oversight. It is probably accurate to say that nothing like it existed in any other country then or subsequently. Tragically, that finely-tuned mechanism was allowed to atrophy in the 1990s. By 2001, Senate oversight of intelligence existed in name only. The once effective relationship that had been built up between the Committee and the Intelligence Community had ceased to exist.

This was not a small matter. In my judgment, if intelligence oversight had been maintained at the same professional level it had reached in the 1980s, there is a real likelihood that the attacks of 9/11 would have been prevented. An effective oversight committee would have had two or three professional staff working the terrorist threat full time following the 1993 truck bombing of the World Trade Center. Such a staff effort might well have ferreted out the isolated pieces of information that would have revealed the 9/11 plot had that information been known more widely within the Community. Senate staff can range across the bureaucratic stovepipes and challenge entrenched orthodoxies in a way that intelligence officials often cannot.

Second, as the Chairman has noted in his statement, the Intelligence Community has grown and proliferated since 9/11. The Office of the Director of National Intelligence (DNI) which did not exist in 2001 now has a staff of 1600. Budgets and personnel have burgeoned across the board. As a result, the task of oversight is now more challenging than it has ever been. Even at its best, the SSCI of the 1980s would be overmatched by the current Intelligence Community without a major augmentation in the staff and capabilities of the Committee. Nothing like that has occurred. That is said with a full acknowledgement that Senator Rockefeller has undertaken a serious effort to reconstitute effective oversight. But when Humpty-Dumpty has fallen and shattered, putting the pieces back together is a difficult and time-consuming business, if it is possible at all.

In truth, the Community has grown so fast that no one really knows what all the different components are doing or how they are performing. To ask DNI McConnell to have mastery of all this is to ask too much. Nor is the Office of the DNI well-equipped to perform audit and other similar functions. That office is engaged in setting overall priorities and managing the analytical process.

The CIA IG remains in place but is currently the subject of an internal inquiry initiated by the Director of Central Intelligence. The IG continues to pursue a number of investigations but is itself, a beleaguered office. Even if these pressures are removed, the IG's jurisdiction remains confined to the CIA. Other major components of the Intelligence Community do not have a statutory IG and most fall under the authority of the IG of the Defense Department. That IG has huge responsibilities related to military programs and is a marginal player when it comes to intelligence programs. For example, in April 2001, the National Security Agency announced with considerable fanfare (for them) the launch of a program dubbed "Trailblazer" intended to "define the architecture, cost, and acquisition approach" to the "transformation" of NSA to "meet the challenge of rapidly evolving, modern communications." Three prime contractors with over thirty industry partners were enlisted. But after an expenditure if $1.2 billion the program has produced nothing like its promised results. Nor was there effective oversight. In sum, there is a striking mismatch between the resources devoted to oversight and the size and complexity of the Intelligence Community itself. The price is paid in terms of diminished security and spectacular cost overruns.

In 1987 agencies like NSA used highly proprietary technologies that they developed themselves or through exclusive arrangements with selected contractors. Now such agencies increasingly rely on commercially available technologies or those used elsewhere in the federal government. As a consequence, Intelligence Community procurement and contracting looks very much like that of other components of the government with the same sort of oversight issues GAO deals with on a daily basis.

Third, it almost goes without saying that the security threats facing the U.S. have diversified and metastasized: terrorist networks, failed states and jihadist movements, potential pandemics, WMD proliferation, missile systems controlled by hostile regimes and so on. In such a challenging environment, effective oversight can be a vital partner and an enabler of Intelligence Community efforts. Done properly and professionally, oversight will assist Community managers in spotting problems, identifying solutions, and mobilizing Congressional support to meet critical intelligence needs. At the same time oversight will play a critical role in preventing and detecting waste, fraud and abuse in what are huge, complex programs with often massive budgets. The very skills that GAO brings to the table in terms of auditing, financial management, information technology, and knowledge management are precisely those in shortest supply in current oversight efforts.

There is one matter that will be of great concern to the Intelligence Community and should be noted. Wise officials in the Community will not object to effective oversight; they will welcome it. They will object to an undue proliferation of Committees exercising oversight as both burdensome and a potential problem in terms of information security. I would encourage the Committee to consider how a GAO role can be crafted while retaining a relatively streamlined oversight system.

In conclusion, the Intelligence Community needs all the help it can get and the American people need the assurance that the capabilities they are funding are being kept under tight control. GAO is equipped to meet these vital requirements.

Statement of Steven Aftergood
Federation of American Scientists

Before the Subcommittee on Oversight of Government Management,
The Federal Workforce, and the District of Columbia
Of the
Committee on Homeland Security and Governmental Affairs
United States Senate

Hearing on
Government-wide Intelligence Community Management Reforms

February 29, 2008

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, a non-governmental policy research and advocacy organization. The Project seeks to promote public oversight and government accountability in intelligence and national security policy.

Summary

At a time when the U.S. intelligence community is expanding in size and complexity, it stands to reason that Congress should utilize all of the tools at its disposal to ensure that intelligence activities are conducted in compliance with the law, and are performed efficiently and effectively. Towards this end, the Government Accountability Office (GAO) could make a distinct and valuable contribution, and it should be called upon to do so.

Intelligence Spending Has Doubled in the Past Ten Years

In the past decade, intelligence spending has doubled. But intelligence oversight capacity has not grown at the same rate. For this reason alone, it is appropriate to activate new oversight tools.

In FY 1997 the aggregate total of all U.S. intelligence spending was $26.6 billion.[1] This figure included the budgets for national, joint military and tactical intelligence.

In FY 2007 the total budget for the national intelligence program alone was $43.5 billion.[2] Together with spending for the military intelligence program, which likely exceeds $10 billion annually, the resulting aggregate figure is more than $50 billion per year.

This is an extraordinary rate of growth. And it has not been matched by a comparable increase in the size of the oversight committee staffs or a corresponding expansion of other oversight mechanisms. In effect, there has been a net decrease in intelligence oversight. Given the great sensitivity and importance of intelligence activities, this is a problematic development that warrants a response.

Intelligence Contracting Has Also Doubled in the Past Ten Years

An additional challenge to intelligence oversight arises from the steady increase in the use of intelligence contractors, which is a development that existing oversight practices may be ill-suited to meet.

An astonishing 70% of the intelligence community budget is now spent on contracts with commercial entities, according to one estimate from the Office of the

---

[1] This figure was declassified by DCI George J. Tenet on October 15, 1997 in response to a Freedom of Information Act lawsuit filed by the Federation of American Scientists.

[2] This figure was disclosed by DNI J. Michael McConnell on October 30, 2007 in compliance with section 601 of the "Implementing Recommendations of the 9/11 Commission Act of 2007," Public Law 110-53.

Director of National Intelligence.[3] This represents a doubling of spending on intelligence contractors from 1996 to 2006, according to the same ODNI account.[4]

Unlike intelligence agencies, intelligence contractors are not directly answerable to the congressional intelligence oversight committees. Contractors have their own commercial motivations and Congress is not their "customer." Congress has yet to adapt to the new landscape of intelligence contracting. Yet oversight of contractor management is an area where the Government Accountability Office has experience and a proven track record.[5]

For that reason, it would be useful to employ the GAO's core auditing function here, so as to ensure that the many billions of intelligence contracting dollars are in fact going where they are intended to go, and are being expended properly and productively. That is more than the intelligence oversight committees can assure the public today.

The Quality of Intelligence Oversight is Strained

Regardless of one's views on particular questions of intelligence policy, there is reason to doubt that current intelligence oversight arrangements are adequate to fulfill their important task. Intelligence oversight lacks the personnel, the full range of expertise, the requisite information, and other resources needed to do the job.

"*In toto*, we are perhaps one dozen or so full-time budget staff supporting the Intelligence Authorization and Appropriations Committees of both the House and the

---

[3] "Procuring the Future": 21st Century IC Acquisition" by Terry Everett, DNI Procurement Executive, 2007, Power Point presentation, at page 10. This document was first reported by Tim Shorrock, "The Corporate Takeover of U.S. Intelligence," Salon.com, June 1, 2007. A copy of the document is available at: http://www.fas.org/irp/dni/everett.ppt .

[4] Ibid., see the second bar chart on page 11.

[5] See, most recently, these GAO products: GAO-08-436T, "Military Operations: Implementation of Existing Guidance and Other Actions Needed to Improve DoD's Oversight and Management of Contractors in Future Operations," January 24, 2008; and GAO-08-294, "Best Practices: Increased Focus on Requirements and Oversight Needed to Improve DoD's Acquisition Environment and Weapon System Quality," February 2008.

Senate reviewing activities conducted by tens of thousands of civilian and military personnel and programs valued in the multiple billions of dollars," wrote Senate Intelligence Committee staffer Mary K. Sturtevant in 1992 in a revealing internal account of the congressional oversight process at that time.[6] Despite some growth in staff since then, the fundamental problem persists.

Consider the startling disparity between the enormous size of the U.S. intelligence apparatus and the modest reach of its oversight system. If there are now roughly 50 intelligence committee staff with budget oversight responsibility for an intelligence budget of around $50 billion, that would mean that each staffer is responsible on average for oversight of a billion dollars worth of intelligence spending. This is not an optimal arrangement.

The comparatively small size of the budget oversight staff inevitably means, as Ms. Sturtevant candidly acknowledged in 1992, that "the great majority of continuing, or 'base,' programs go unscrutinized."[7]

What the GAO Has to Offer

The Government Accountability Office cannot provide an alternative to intelligence committee oversight, but it can provide a useful complement to it.

Committee oversight will always be required to assess new initiatives, review fundamental policy choices, and evaluate points of controversy. But the particular expertise of intelligence committee staff is not required for oversight of many of the more mundane programs that make up the infrastructure of U.S. intelligence, including many of the "base" programs that routinely get overlooked.

---

[6] Mary K. Sturtevant, "Congressional Oversight of Intelligence: One Perspective," American Intelligence Journal, Summer 1992. Available at: http://www.fas.org/irp/eprint/sturtevant.html .

[7] Ibid. It should be noted that due to classification restrictions, intelligence oversight, unlike other areas of congressional oversight, is largely isolated and deprived of support from intensive news coverage, public interest advocacy, and other independent sources.

In addition to its longstanding financial auditing function, the GAO has experience in many disciplines that are of current relevance to management of U.S. intelligence.

One example is personnel security policy and the granting of security clearances. GAO has been conducting oversight and investigations of security clearance policy for several decades and has aided Congress considerably in coming to grips with this perennially challenging area.[8]

Another example is information sharing, a critical post-9/11 agenda item, where GAO has also contributed significant insights on obstacles to information sharing and potential remedies.[9]

These and other areas of GAO expertise can enable GAO to shoulder some of the oversight burden so that the intelligence oversight committees can focus their efforts where they are most needed.[10]

Security Concerns

It has been objected that any increased role for GAO in intelligence oversight could pose an unacceptable threat to the security of intelligence programs. "Pursuant to obligations to protect intelligence sources and methods, the IC [intelligence community] has traditionally declined to participate in GAO inquiries that evaluate intelligence

---

[8] See, most recently, GAO-08-470T, "DoD Personnel Clearances: DoD Faces Multiple Challenges in Its Efforts to Improve Clearance Processes for Industry Personnel," February 13, 2008.

[9] See, for example, GAO-06-383, "Information Sharing: DHS Should Take Steps to Encourage More Widespread Use of Its Program to Protect and Share Critical Infrastructure Information," April 2006.

[10] The resources that GAO could bring to bear on intelligence oversight were discussed further by the Comptroller General in a March 1, 2007 letter to the Senate Intelligence Committee at pp. 7-8. Copy available at: http://www.fas.org/irp/gao/walker030107.pdf .

activities, programs, capabilities, and operations," Director of National Intelligence J. Michael McConnell wrote last year.[11] But this statement is incomplete and misleading.

GAO has long had access to some of the most sensitive and highly compartmented programs in the U.S. government.[12] While it is true that the Central Intelligence Agency has historically opposed GAO oversight, other members of the U.S. intelligence community have successfully demonstrated varying degrees of cooperation with GAO.

"In practice, defense [intelligence] agencies do not adopt the 'hard line' CIA approach but generally seek to cooperate with GAO representatives," according to a 1994 CIA memorandum prepared for the Director of Central Intelligence.[13]

In fact, the same 1994 memorandum explained, "NSA [the National Security Agency] advises that the GAO maintains a team permanently in residence at NSA, resulting in nearly continuous contact between the two organizations. NSA's practice has been to cooperate with GAO audits and investigations to the extent possible in accordance with DOD regulations."[14]

Likewise, long before the existence of the National Reconnaissance Office was declassified and publicly acknowledged (in 1992), GAO produced a classified "Review of DoD's Reconnaissance Intelligence Assets" (in or around 1978).[15]

Thus the feasibility of a role for GAO in intelligence audits and investigations with no adverse security consequences has already been demonstrated in practice.

---

[11] Letter to the Chairman and Vice Chairman of the Senate Intelligence Committee, March 7, 2007. Copy available at: http://www.fas.org/irp/gao/mcconnell030707.pdf .

[12] See, for example, "Auditing Highly Classified Air Force Programs" by Rae Ann Sapp and Robert L. Repasky, The GAO Review, Winter 1987.

[13] "DCI Affirmation of Policy for Dealing with the General Accounting Office (GAO)," by Stanley M. Moskowitz, CIA Director of Public Affairs, 7 July 1994, paragraph 13, copy available at: http://www.fas.org/sgp/gao/ciapolicy.html .

[14] Ibid., paragraph 14.

[15] GAO Code 951357. The GAO document was cited in a declassified NRO memorandum dated 3 February 1978. My thanks to Allen Thomson for this information.

Currently, all Department of Defense components are instructed to "cooperate fully with the GAO" and to provide GAO investigators with classified information after verifying their security clearances.[16]

There is no record of a compromise of classified information resulting from GAO oversight.[17]

Conclusion

Congressional oversight of intelligence, which has never been robust, has not kept pace with the extraordinary growth of U.S. intelligence in the past decade, and has not yet adapted to the fundamental changes associated with the growing reliance on intelligence contractors.

The Government Accountability Office appears to be ready, able and willing to contribute to the crucial function of intelligence oversight. GAO has a proven track record of adding value to the oversight process, combining competence in the performance of audits and investigations with discretion in the handling of classified information.

I believe that Congress should promptly take advantage of this established resource. Doing so will aid congressional oversight and will ultimately benefit the intelligence agencies themselves.

---

[16] DoD Instruction 7650.02, "Government Accountability Office (GAO) Reviews and Reports," November 20, 2006. Available at: http://www.fas.org/irp/doddir/dod/i7650_02.pdf .

[17] In the early 1980s, it was alleged that Soviet spies had infiltrated the GAO. But Senate Intelligence Committee "staff investigated these charges and found no substantiation for them," Committee chairman Sen. Barry Goldwater told the Senate on September 24, 1982. See Frank J. Smist, Jr., Congress Oversees the United States Intelligence Community, Second Edition, (Univ. of Tenn. Press, 1994), page 131; citing *Congressional Record*, September 24, 1982, 512286.

Statement of Frederick M. Kaiser, Specialist in American National Government
Congressional Research Service

Before
The Senate Committee on Homeland Security and Governmental Affairs
Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia
House of Representatives

February 29, 2008
on
"Government-wide Intelligence Community Management Reforms"

Mr. Chairman, Mr. Voinovich, and Members of the Subcommittee:

Thank you for inviting me to participate in this hearing on government-wide Intelligence Community (IC) management reforms, with attention also to congressional oversight of this evolving field.[1] My prepared statement focuses on the current oversight structure, its effectiveness, and areas of inquiry that the panel might wish to pursue.

Introduction

The Intelligence Community (IC) rubric is formally applied to the 16 entities under the umbrella of the Director of National Intelligence (DNI).[2] But another intelligence entity also exists. The group, which may be called the homeland security intelligence community (HSIC), is a separate collective, although it overlaps with the national security IC.[3] Ideally, the HSIC can overcome the "foreign-domestic divide" that, according to the 9/11 Commission, hampered effective intelligence gathering, evaluation, and dissemination.[4] Both intelligence communities require a substantial amount of interagency cooperation and coordination, to provide for a sharing of relevant and timely information as well as to engage in multi-agency activities and operations. The HSIC mission also requires coordination and cooperation between the federal government, on the one hand, and state and local governments, on the other.

Oversight of intelligence is — and has always been — a challenge to Congress, because of the high degree and pervasiveness of secrecy surrounding such operations, activities, and even organizational characteristics. This feature, which appears to be expanding and increasingly institutionalized, constrains congressional oversight in a

---

[1] For more detail and citations, see CRS Reports RL32525, *Congressional Oversight of Intelligence: Current Structure and Alternatives*, by Frederick M. Kaiser; and RL32617, *A Perspective on Congress's Oversight Function*, by Walter J. Oleszek.

[2] U.S. Director of National Intelligence, *An Overview of the United States Intelligence Community* (2007), available at [http://www.DNI.gov/who_what/members_IC.htm]. See also CRS Report RL34231, *Director of National Intelligence Statutory Authorities: Status and Proposals*, by Richard A. Best, Alfred Cumming, and Todd Masse.

[3] This still somewhat "nebulous" community is examined in detail in CRS Report RL33616, *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches*, by Todd Masse, p. 1.

[4] U.S. National Commission on Terrorist Attacks Upon the United States, *Final Report*, pp. 399-428, available at [http://www.goiaccess.gov/911/pdf/fullreport.pdf].

number of ways. It may restrict: communicating directly with the executive; gaining access to classified national security information as well as to a growing amount of sensitive (but not classified) information; sharing information, analysis, and insights among Members, committees, and staff of Congress; and using congressional support agencies. Secrecy may also present obstacles to Congress benefitting from the findings, conclusions, and other contributions of non-governmental organizations, which are limited in their access to government-controlled information.

National security concerns may also affect other oversight capabilities. Importantly, certain offices of inspector general operate under security constraints. The heads of seven departments or agencies (out of the more than 60 with statutory offices of inspector general) — the Departments of Defense, Homeland Security, Justice, and the Treasury; the Central Intelligence Agency (CIA); the Federal Reserve Board; and the U.S. Postal Service — may prevent the inspector general from initiating, carrying out, or completing an audit or investigation. The reasons for exercising this power are to protect national security matters or ongoing criminal investigations. These reasons are to be communicated to the Senate Homeland Security and Governmental Affairs Committee (HSGAC), the House Oversight and Government Reform Committee, and the authorizing committees for the agency for all the agencies except the CIA, whose reports are submitted only to the House and Senate select committees on intelligence.[5]

Current Oversight Structure

Oversight of intelligence has been consolidated in the House and Senate select committees on intelligence since the latter 1970s, when the panels were established.[6] These committees have exclusive jurisdiction and authority over legislation and authorizations for the Central Intelligence Agency and the Director of National Intelligence, and formerly had such over the Director of Central Intelligence, a now abolished office. But the select committees share legislative jurisdiction and authority for the rest of the intelligence community with other committees in their respective chambers.[7] The intelligence committees, moreover, do *not* hold exclusive oversight over the DNI and CIA or any other component of the intelligence community. Current Senate rules, importantly, repeat the original directive in the establishing charter for its Select Committee on Intelligence:

> Nothing in this resolution shall be construed as prohibiting or otherwise restricting the authority of any other committee to study and review any intelligence activity to the extent that such activity directly affects a matter otherwise within the jurisdiction of such committee ....[8]

Examples of such oversight include the Permanent Subcommittee on Investigations, which, in 1985 (the so-called "Year of the Spy"), conducted hearings into the federal

---

[5] 5 U.S.C. Appendix for all but the CIA (P.L. 101-193).

[6] The two select committees have reserved seats for other committees with shared jurisdiction. On the Senate side, these include a majority and minority member from four panels: the Committees on Appropriations, Armed Services, Foreign Relations, and the Judiciary. U.S. Congress, Senate, *Nonstatutory Standing Orders*, no. 94, sec. 2(a). By coincidence, in the 110th Congress, one member of the Committee on Homeland Security and Governmental Affairs (i.e., Senator John Warner) is also a member of the Select Committee on Intelligence.

[7] Ibid., sec. (3)(a)-(b).

[8] Ibid., sec. (3)(c). This provision originated in 1976, when the Senate Select Committee on Intelligence was established by S. Res 400, 94th Cong., 2nd sess.

government's security clearance programs.[9] In the late 1980s, Congress commissioned a review of the intelligence community workforce, conducted by the National Academy of Public Administration (NAPA).[10] Over the years, various Senate and House panels (other than the select committees on intelligence) have looked into aspects, activities, and operations of the intelligence community. In July 2001, for instance, two subcommittees of the House Committee on Government Reform (now Oversight and Government Reform) reviewed computer security programs at nearly all executive departments and agencies. The lone exception was the CIA; it declined to participate in the hearings and in an earlier survey by the General Accounting Office, now the Government Accountability Office (GAO).[11] The CIA's position on cooperation led the chairmen of the two subcommittees to criticize that stand as a threat to effective oversight.[12]

Throughout its history, the CIA has taken the position that it is, in effect, off-limits to the Government Accountability Office, because of special statutory provisions giving the Agency a protected status.[13] GAO has countered that it has the necessary independent authority to review and audit the CIA but that the Office lacks effective enforcement powers to ensure its cooperation.[14] Significantly, other IC components state positions that are in contrast to the CIA's. The Department of Defense (DOD), which houses the largest number of the IC units, for example, instructs its personnel to "cooperate fully with the GAO and respond constructively to, and take appropriate corrective action on the basis of, GAO reports."[15]

Effective Oversight of Intelligence

There are a number of options that Congress and its committees could explore to increase effective oversight of intelligence.[16] Such options of interest to this subcommittee might include:

- Engaging in cooperative ventures with other subcommittees on HSGAC and/or with other committees that have shared or overlapping jurisdiction. This could help to spread the workload among several panels and create a setting where additional viewpoints could arise.

---

[9] U.S. Congress, Senate Permanent Subcommittee on Investigations, *Federal Government Security Clearance Programs*, hearings, 99th Cong., 1st sess. (Washington: GPO, 1985).

[10] *The Intelligence Community Workforce for the 1990s* (Washington: NAPA, 1989).

[11] U.S. Congress, House Subcommittees on Government Efficiency and on National Security, *Is the CIA's Refusal to Cooperate with Congressional Inquiries a Threat to Effective Oversight of the Operations of the Federal Government?*, hearings, 107th Cong., 1st sess. (Washington: GPO, 2001), pp. 1 and 5.

[12] The CIA had initially agreed to cooperate in the GAO survey but later declined. The Agency reportedly attempted, unsuccessfully, as it turned out, to enlist other intelligence agencies to do the same. Finally, the CIA declined to participate in any subcommittee hearings, even though the chairmen had agreed to hold these in executive or secret session. Ibid., pp. 1-8.

[13] For citations to the statutory provisions and related materials, see CRS Report RL32525, *Congressional Oversight of Intelligence*, pp. 21-22.

[14] Ibid.

[15] DoD Instruction 7650.02, November 20, 2006.

[16] For elaboration, see CRS Report RL32525, *Congressional Oversight of Intelligence*, pp. 14-23; and CRS Report RL30240, *Congressional Oversight Manual*, by Frederick M. Kaiser, et al.

- Possibly applying the standards and requirements of the Government Performance and Results Act (P.L. 103-62; 107 Stat. 285) to the CIA, which is currently exempt from it. (CIA reports might be classified and submitted to the House and Senate select committees on intelligence.)

- Establishing a post of Inspector General of the Intelligence Community, with jurisdiction paralleling that of the DNI.[17] This might expand IG capabilities, provide a community-wide perspective, and improve coordination among the inspectors general in each IC component.

- Making requests to relevant inspectors general for studies, audits, investigations, or inspections.[18]

- Reviewing the findings, conclusions, and recommendations of the ombudsman-like offices in the Department of Homeland Security (i.e., the Privacy Officer, Officer for Civil Rights and Civil Liberties, and special duties assigned to the Inspector General).[19] The resulting oversight efforts could help assess DHS's compliance with its statutory obligations, including the protection of civil rights and liberties.

- Contracting with nongovernmental organizations, such as NAPA or the Rand Corporation, to conduct relevant studies.

- Engaging the Government Accountability Office directly in planned oversight endeavors, through advanced requests for specific reviews, briefings, and testimony at hearings.

- Clarifying GAO's authority to audit all components of the Intelligence Community, possibly as proposed in the Intelligence Community Audit Act of 2007 (S. 82 and H.R. 978, 110th Congress).

Possible Areas for Inquiry

---

[17] Currently, an IG in the Office of the DNI exists; but the DNI is granted full discretion to create and construct the office (P.L. 108-458). A proposal to establish a IC-wide inspector general has been advanced in the Intelligence Authorization Act for Fiscal Year 2008 (H.R. 2082, 110th, 2nd sess.), which has been cleared for the White House. For a description of such an office, see U.S. Congress, Senate Select Committee on Intelligence, *Intelligence Authorization Act for Fiscal Year 2008*, S.Rept. 110-75, 110th Cong., 1st sess., pp. 16-19. This new IG, however, would not replace the existing statutory inspectors general in the departments and agencies under the IG Act of 1978, as amended, or in legislation covering the CIA (P.L.101-193).

[18] Under the Inspector General Act of 1978, as amended, IGs have nearly total discretion in determining their priorities and projects, although some have responded to congressional requests for specific audits or investigations. Current legislative proposals (H.R. 928 and S. 2324, 110th Congress) would also aid oversight, by increasing the IGs' independence and coordination among them. See CRS Report RL34176, *Statutory Inspectors General: Legislative Developments and Legal Issues*, by Vanessa K. Burrows and Frederick M. Kaiser.

[19] P.L. 108-458; 118 Stat. 3867-3869.

There are a number of possible areas of inquiry with regard to the management of the intelligence communities — both the national security and homeland security communities — that the Subcommittee could choose to pursue.[20]

The Range of Subjects. The wide range of subjects includes, among others: the collection capabilities of the agencies; the analytical quality of intelligence; cooperation and coordination among the components; effectiveness of new structures; and improvements in sharing information among the IC components themselves and with homeland security agencies. Such subjects may be affected by competing priorities and the different orientations and cultures of the agencies: e.g., intelligence for national security purposes, support for military operations, or anti-terrorism and other homeland security efforts. To varying degrees, the ability to meet these challenges is dependent on the powers and real power of the DNI to bring about the necessary coordination and sharing of responsibilities among the components. Along with this is the role of the DHS Secretary in ensuring that homeland security intelligence needs are met. Another overarching concern could be protection of civil liberties and individual rights, in light of the government's enhanced anti-terrorism powers.

Personnel Matters. Other possible interests center on personnel in the intelligence community.

One is their understanding of foreign cultures and languages, which, in turn, derives from their training, education, and experience.[21] To what degree has this capability increased in the recent past? What impediments exist in recruiting, hiring, and/or training intelligence personnel in this regard?

Another area of inquiry may be the security clearance process. It is a key component for transferring and re-assigning personnel — temporarily or permanently — in the national security and homeland security intelligence communities. The process and its results appear to have improved, with an increased emphasis on reciprocity among the agencies and assigning most of the background investigations to one organization (i.e., the Office of Personnel Management now handles 90% of these).[22] But the full process still faces obstacles, in light of the growing demand for more and higher-level clearances, which then require more frequent reinvestigations. Possible questions include:

- To what degree has the DNI been active in assessing or changing certain requirements (such as polygraph testing for the highest-level and special categories of clearances) or speeding up the process (through increased resources, for instance)?

- Has there been any reconsideration of the current requirement for withholding or delaying clearances for noncitizens? If so, how would this be changed?

---

[20] These areas and others are spelled out in three CRS reports: RL34231, *Director of National Intelligence Statutory Authorities: Status and Proposals*; RL33539, *Intelligence Issues for Congress*, by Richard A. Best; and RL33616, *Homeland Security Intelligence.*

[21] For elaboration on this subject, see CRS Report RL31625, *Foreign Language and International Studies: Federal Aid Under Title VI of the Higher Education Act*, by Jeffrey J. Kuenzi.

[22] See U.S. Office of Management and Budget, Security Clearance Oversight Group, *Report* (February 2008).

- To what degree has reciprocity been achieved between the CIA and FBI, which still conduct their own background investigations, and between either of these and other government agencies?

- Are there proposals to extend reciprocity to the adjudication phase of the security clearance process, at least on a temporary basis for certain individuals or on a pilot basis for agencies?

- Have the clearances at DHS kept pace with the rising demand brought on by new hires as well as existing staff needing or seeking higher levels of clearances?

- How many state and local officials have received clearances from DHS? Have any state or local officials involved in homeland security been denied clearances? If so, what happened to the positions?

Thank you for your attention. I would be pleased to answer any questions that you might have.

Order Code RL32525

CRS Report for Congress

Congressional Oversight of Intelligence: Current Structure and Alternatives

Updated February 11, 2008

Frederick M. Kaiser
Specialist in American National Government
Government and Finance Division

Prepared for Members and
Committees of Congress

Congressional
Research
Service

Congressional Oversight of Intelligence: Current Structure and Alternatives

Summary

Interest in congressional oversight of intelligence has risen again in the 110th Congress, in part because of the House Democratic majority's pledge to enact the remaining recommendations from the U.S. National Commission on Terrorist Attacks Upon the United States, commonly known as the 9/11 Commission. Its 2004 conclusions set the stage for reconsideration of the problems affecting Congress's structure in this area. The commission's unanimous report, covering many issues, concluded that congressional oversight of intelligence was "dysfunctional" and proposed two distinct solutions. These were, (1) creation of a joint committee on intelligence (JCI), modeled after the defunct Joint Committee on Atomic Energy (JCAE), with authority to report legislation to each chamber; or (2) enhanced status and power for the existing select committees on intelligence, by making them standing committees and granting both authorization and appropriations power.

Congress's interest in a joint committee on intelligence dates to 1948 and the early years of the Central Intelligence Agency (CIA) and Director of Central Intelligence (DCI). Similar recommendations have arisen in the meantime, although the lion's share were made before separate Intelligence Committees were established in the House (1977) and Senate (1976). The numerous proposals for a JCI, which would end the two existing intelligence panels, moreover, vary in their specifics and raise competing viewpoints over practical matters and matters of principle.

Although it did not adopt either of the 9/11 Commission proposals, Congress has pursued other initiatives to change its intelligence oversight structure and capabilities in the 110th Congress. This has occurred through the chambers' leadership, existing committees, and a Senate bipartisan working group, leading to that chamber's restructuring its oversight panels plus new working arrangements between the intelligence and appropriations panels. The House altered its arrangements (H.Res. 35), when it created a Select Intelligence Oversight Panel on the Appropriations Committee, a hybrid structure that is perhaps unique in the annals of Congress. The new 13-member panel combines members of the House Permanent Select Committee on Intelligence and the Committee on Appropriations to study and make recommendations to relevant appropriations subcommittees on the annual intelligence community appropriations. Other proposals, some with a long heritage, include clarifying and expanding the independent authority of the Government Accountability Office (GAO) over the intelligence community, particularly the CIA; placing the CIA expressly under the Government Performance and Results Act; increasing the coordinative capabilities and reporting of relevant inspectors general (IGs); and adding a new IG covering the entire intelligence community.

This report first describes the current select committees on intelligence and then the former Joint Committee on Atomic Energy, often cited as a model for a counterpart on intelligence. The study also sets forth proposed characteristics for a joint committee on intelligence, differences among these, and their pros and cons. The report, to be updated as events dictate, also examines other actions and alternatives affecting congressional oversight in the field.

Contents

Introduction 1

House and Senate Select Committees on Intelligence 2
Jurisdiction and Authority 3
Membership and Leadership 3
Secrecy Controls 4

Joint Committee on Atomic Energy as a Model 4

Proposed Joint Committee on Intelligence Characteristics 6
Methods of Establishment 6
Jurisdiction and Authority 7
Membership 7
Terms and Rotation 7
Leadership 8
Secrecy Controls 8
Staffing 9
Budget and Funding 9
Pros and Cons 9
Pros 9
Cons 11

Alternatives to a Joint Committee 14
Changing the Select Committees' Structure and Powers 14
Senate Action 15
House Action 16
Concerns about Restructuring the Intelligence Committees 17
Improving Coordination Between the Two Intelligence Panels 18
Joint Hearings 18
Leadership Meetings 19
Constraints on Coordination 19
Interchanges with Other Panels and Members 19
Goals 20
Techniques 20
Limitations 21
Other Proposals 21
Use of Congressional Support Agencies 21
Applying GPRA Requirements to the CIA 22
Changes Affecting the Inspectors General 22

Observations on Oversight of Intelligence 23
Obstacles to Oversight 23
Secrecy Constraints 23
Appeal of Intelligence Oversight 24
Overcoming the Obstacles 24
Objectives and Goals 24
The Joint Committee Approach and Alternatives 24

Congressional Oversight of Intelligence: Current Structure and Alternatives

Introduction

Congress has long considered various ways to oversee intelligence, an often perplexing and always difficult responsibility because of the secrecy and sensitivity surrounding intelligence findings, conclusions, dissemination, and sources and methods.[1] The first oversight proposal — to create a joint committee on intelligence (JCI) — occurred in 1948.[2] This was just one year after the establishment of the Cental Intelligence Agency (CIA) and the Office of Director of Central Intelligence (DCI), both integral parts of the most far-reaching executive reorganization in United States history.[3] Numerous other initiatives to change Congress's oversight structure have materialized in the meantime, including, most importantly, the creation of parallel select committees on intelligence in both chambers. The House's and Senate's recent actions modifying each body's own structure have diverged from each other[4] as well as from the 9/11 Commission proposals. The commission's report concluded that congressional oversight of intelligence was "dysfunctional" and recommended either a merger of appropriations and authorization powers into each select committee or the creation of a joint committee on intelligence.[5]

---

[1] See, among other sources, CRS Report RL32617, *A Perspective on Congress's Oversight Function*, by Walter J. Oleszek; CRS Report RL33742, *9/11 Commission Recommendations: Implementation Status*, by Richard F. Grimmett, Coordinator; and CRS Report RL33715, *Covert Action: Legislative Background and Possible Policy Questions*, by Alfred Cumming.

[2] H.Con.Res. 186, 80th Cong., 2nd sess., introduced by Rep. Devitt, Apr. 21, 1948.

[3] The monumental National Security Act of 1947 also gave birth to the National Security Council and National Military Establishment, later re-designated as the Department of Defense (61 Stat. 496 et seq.).

[4] The House and Senate have considered proposals in this broad area through their existing committees as well as a bipartisan working group in the Senate, which has recommended enhancing the powers and status of the current Intelligence Committee. Sen. Mitch McConnell, "Senators Reid and McConnell Convene Meeting of Bipartisan Working Group to Reform Congressional Oversight of Intelligence," Press Release, Oct. 4, 2004; Sen. Bill Frist, "Frist, Daschle Appoint Members to Working Group Evaluating 9/11 Commission Proposals," Press Release, Aug. 25, 2004.

[5] U.S. National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report* (Washington: GPO, 2004), p. 420. The commission offered a second option to strengthen oversight: i.e., "a single committee in each house of Congress, combining authorization and appropriating authorities .... (Ibid.)."

This report reviews the basic characteristics of proposed joint committees on intelligence, differences among them, and perceived advantages and disadvantages.[6] It also covers the congressional panels a JCI would replace: namely, the House and Senate select committees on intelligence. Along with this is a brief review of the defunct Joint Committee on Atomic Energy (JCAE) — often cited as an organizational model for a joint intelligence panel, as it has been for the 9/11 Commission.

In addition, the report looks at recent actions, such as the creation of a new (and possibly unique in the history of Congress) intelligence oversight panel on the House Appropriations Committee, consisting of Members from both the parent committee and the Select Committee on Intelligence; the new panel would make recommendations regarding the annual intelligence community appropriations to the Defense Appropriations Subcommittee. This report also covers separate developments in the Senate, including a Memorandum of Agreement (MOA) in 2007, designed to improve coordination and transparency between the Intelligence Committee, which handles authorizations for the intelligence community, and the Appropriations Committee, which handles appropriations for the same. Other ways seen as strengthening oversight in this field would be to (1) clarify and expand the authority of Government Accountability Office (GAO) over the intelligence community, particularly the CIA; (2) remove the Agency's exemption from coverage of the Government Performance and Results Act; and (3) increase coordination and strengthen reporting requirements among the relevant offices of inspector general.

House and Senate Select Committees on Intelligence

A joint committee on intelligence would replace the current House Permanent Select Committee on Intelligence, established in 1977, and the Senate Select Committee on Intelligence, created a year earlier.[7] These units emerged after

---

[6] Additional coverage of JCI recommendations, characteristics, and perceived advantages and disadvantages, which are detailed below, is available in U.S. Congress, House Committee on Rules, Subcommittee on Rules of the House, *House Rule XLVIII*, hearing, 101st Cong., 2nd sess. (Washington: GPO, 1990); Frederick M. Kaiser, "A Proposed Joint Committee on Intelligence: New Wine in an Old Bottle," *Journal of Law and Politics*, vol.5, fall 1988, pp. 127-186; and Independent Task Force, Council on Foreign Relations, *Making Intelligence Smarter: The Future of U.S. Intelligence* (New York: Council on Foreign Relations, 1996), pp. 32-33.

[7] Development of congressional oversight of intelligence is examined in U.S. Congress, Senate Select Committee on Intelligence, *Legislative Oversight of Intelligence Activities*, S.Prt. 103-88, 103rd Cong., 2nd sess. (Washington: GPO, 1994); Frederick M. Kaiser, "Congress and the Intelligence Community," in Roger Davidson, ed., *The Postreform Congress* (New York: St. Martins Press, 1992), pp. 279-300; Loch K. Johnson, "Congressional Supervision of America's Secret Agencies," in Loch K. Johnson and James J. Wirtz, eds., *Strategic Intelligence* (Los Angeles: Roxbury Publishing, 2004), pp. 414-426; and Mark M. Lowenthal, *Intelligence: From Secrets to Policy* (Washington: CQ Press,

(continued...)

extensive, detailed congressional and executive investigations revealed widespread abuses in the intelligence community and concluded that effective congressional oversight was lacking. The panels were set up to consolidate legislative and oversight authority over the entire intelligence community, supplanting the fragmented system at the time, which relied exclusively on disparate standing committees. Although titled "Select," the intelligence panels are hybrids of standing and select committees, adopting characteristics of both types. For instance, the panels have only temporary membership, as select committees have, because they are usually short-term constructions; yet each panel holds authority to report legislation to its own chamber, a power usually reserved to standing committees.

Jurisdiction and Authority

The Intelligence Committees have broad jurisdiction over the intelligence community and report authorizations and other legislation for consideration by their respective chambers. A recent change in the House places three members of the Intelligence Committee on a new Select Intelligence Oversight Panel on the Appropriations Committee (H.Res. 35, 110th Congress). The new panel, which appears unprecedented in the history of Congress, is to study and make recommendations to relevant appropriations subcommittees. This includes the Defense Appropriations Subcommittee, which continues to prepare the annual intelligence community budget, as part of the classified annex to the bill making appropriations for the Department of Defense.

Most of the jurisdiction of the current Intelligence Committees is shared. The select committees hold exclusive authorizing and legislative powers only for the Central Intelligence Agency, the Director of National Intelligence (as it had over the now-defunct Director of Central Intelligence), and the National Foreign Intelligence Program. This leaves the intelligence components in the Departments of Defense, Homeland Security, Justice, and Treasury, among other agencies, to be shared with appropriate standing committees.

The House and Senate intelligence panels have nearly identical jurisdictions for the intelligence community. The House panel's domain, however, also extends over an area that the Senate's does not: "tactical intelligence and intelligence-related activities," which covers tactical military intelligence. In another departure, the House select committee has been given authority to "review and study on an exclusive basis the sources and methods of entities" in the intelligence community.[8]

Membership and Leadership

The membership of the committees has been limited in time, staggered, and connected to the standing committee system and political party system in Congress. These features, moreover, differ between the two panels. Each select committee, for

---

[7] (...continued)
2006), Chapter 10.

[8] House Rule 3(l), added by H.Res. 5, 107th Cong., Jan. 3, 2001.

instance, reserves seats for members from the chamber's committees on Appropriations, Armed Services, Foreign Affairs/Foreign Relations, and Judiciary. The specifics differ, however: the Senate requires two persons, a majority and minority Member, from each of these standing committees, while the House calls for only one Member from each standing committee with overlapping jurisdiction.

The two panels also differ in size (21 on the House panel and 15 on the Senate counterpart, plus ex officio members on each), tenure, and other membership features, including partisan composition and leadership arrangements. Since its inception, the Senate panel has had only one more Member from the majority party than the minority (an eight-to-seven ratio); and its vice chairman, who takes over if the chair is unavailable, must come from the minority party. The House select committee, in contrast, reflected the full chamber party ratio when it was established in 1977: two-to-one plus one, resulting in an initial nine-to-four majority-minority party membership on the panel. In the meantime, however, the minority party has been granted additional seats on the committee and the majority-minority party ratio in the full House has grown closer. The result is a select committee membership party ratio of 12-to-9 in the 110th Congress.

Secrecy Controls

The committees also have different secrecy arrangements regarding controls over their classified holdings. Secrecy oaths distinguish the two chambers. All Members of the House, including, of course, those on the Intelligence Committee, must swear or affirm not to disclose classified information, except as authorized by the rules of the chamber; the current oath is modeled after a previous one which had been required only for the members of the House Permanent Select Committee on Intelligence. The Senate does not impose a similar obligation on its Members.[9]

Non-member access to classified materials also separates the two panels. The House committee has a more detailed and exacting set of requirements for non-members than its Senate counterpart.

In addition, the Senate panel is authorized to disclose classified information publicly on its own (following elaborate procedures in which the President and the full Senate have an opportunity to act). By comparison, the House select committee cannot do so, if the President objects to its release; in that case, the House itself makes the determination by majority vote.

Joint Committee on Atomic Energy as a Model

The Joint Committee on Atomic Energy (JCAE) — set up by the Atomic Energy Act of 1946, along with the Atomic Energy Commission (P.L. 585, 60 Stat. 772-773) — is often cited as an appropriate organizational model for a joint committee on

---

[9] CRS Report RS20748, *Protection of Classified Information by Congress*, by Frederick M. Kaiser.

intelligence, a reference the 9/11 Commission also adopted.[10] The JCAE, an 18-member panel composed of an equal number of Members from each house of Congress, held authority to report legislation to the floor of both chambers, a power unique among joint committees.[11] Many reasons have been offered for considering the JCAE as a model:

- favorable record for keeping highly confidential material secret;
- largely bipartisan approach to policy-making;
- considerable unity among its members;
- close working relationship with the executive (here, the Atomic Energy Commission) in this secretive and sensitive area;
- consolidated jurisdiction for a growing field;
- explicit, comprehensive oversight mandate, supported by a then-unprecedented directive that the executive keep the joint committee "fully and currently informed"; and
- ability to streamline the legislative process in general and to act rapidly, if necessary, in particular instances.

Given these attributes, the joint committee became a formidable congressional panel. In its prime, JCAE was even considered by some as "probably the most powerful congressional committee in the history of the nation."[12] Despite this — or perhaps because of it — the JCAE was abolished in 1977, nearly 30 years after its birth. It was evidently the victim of a number of reinforcing developments: concerns inside and outside Congress about JCAE's close, some thought cozy, relationship with the executive agency it was overseeing; changing executive branch conditions, such as the breakup of the Atomic Energy Commission into the Nuclear Regulatory Commission and the Energy Research and Development Administration, now the Department of Energy; new rivals in Congress, as the expanding nature of atomic energy and nuclear power extended into the jurisdictions of a number of House and Senate committees; efforts in the Senate at the time to realign and consolidate standing committee jurisdictions and reduce the number of assignments for each

---

[10] For background and further citations on the JCAE, see CRS Report RL32538, *9/11 Commission Recommendations: Joint Committee on Atomic Energy — A Model for Congressional Oversight?*, by Christopher M. Davis; Harold P. Green and Allen Rosenthal, *Government of the Atom: The Integration of Powers* (New York: Atherton Press, 1963); and Kaiser, "A Proposed Joint Committee on Intelligence," pp. 138-141.

[11] One caveat to the unique status of the JCAE is the Temporary Joint Committee on Deficit Reduction; it was authorized to report legislation but only on a narrow subject and on a case-by-case basis. In contrast to the JCAE, this joint panel was a short-term, periodic addition to Congress, set up by the Gramm-Rudman-Hollings Act of 1985. The panel could come into existence only when legislation on budget sequestration was needed and was empowered to report only a joint resolution setting forth specified reports from the Directors of the Office of Management and Budget and the Congressional Budget Office. P.L. 99-177, 99 Stat. 1037, 1100 (1985). This provision apparently was never activated and was not included in the 1987 revision of GRH.

[12] Green and Rosenthal, *Government of the Atom*, p. 266.

Member; and a relatively high number of vacancies on the JCAE (six of the 18 seats).[13]

Proposed Joint Committee on Intelligence Characteristics

Recommendations to create a joint committee on intelligence have surfaced over nearly five decades, most predating the establishment of the two select committees on intelligence in the mid-1970s. Although many of these suggestions, including that from the 9/11 Commission, have followed the design of the Joint Committee on Atomic Energy, not all have; consequently, the specifics in the blueprints have varied in a number of fundamental ways. Differences extend to (1) the range and exclusivity of the panels' jurisdiction; (2) makeup of their membership; (3) selection and rotation of chairmen; (4) possibility of and characteristics of a vice chairmanship; (5) requirements for representation of certain other committees as well as at-large members; (6) special secrecy requirements for members and staff, including a secrecy oath and security clearances; (7) staff size, method of selection, and restrictions on activities; (8) official disclosures of classified information; (9) mechanisms for investigating suspected unauthorized disclosures of such information; and (10) access by non-members to the joint committee's classified holdings. Even suggested methods of establishment have varied.

Methods of Establishment

A joint committee on intelligence could be created by a concurrent resolution, a joint resolution, or a regular bill. The Joint Committee on Atomic Energy, for instance, was established by public law through the regular bill process (i.e., the Atomic Energy Act of 1946, P.L. 580, 60 Stat. 772-773).

A concurrent resolution has the advantage (for its proponents) of requiring only the approval of Congress, while a joint resolution or regular bill must be signed by the President or his veto overridden. A joint resolution or a bill, however, may offer certain benefits to its supporters over a concurrent resolution. A number of existing provisions in public law, especially ones dealing with intelligence reporting requirements to Congress, designates the House and Senate select committees on intelligence as recipients (e.g., the intelligence oversight provisions and the reporting requirements for the CIA Inspector General, codified at 50 U.S.C. 413-415 and 50 U.S.C. 403q, respectively). A bill or joint resolution, when creating a joint committee, could amend these statutory provisions, whereas a concurrent resolution could not do so directly. But a concurrent resolution, although solely a congressional device, could have the same effect. By changing the rules of both chambers, a concurrent resolution could recognize that the powers, authority, and jurisdiction of the former select committees would be transferred to a new joint committee.

---

[13] Kaiser, "A Proposed Joint Committee on Intelligence," pp. 140-141.

Jurisdiction and Authority

A joint intelligence committee could consolidate jurisdiction for the entire intelligence community, extending to all intelligence entities as well as intelligence and intelligence-related activities, including significant anticipated activities (i.e., covert operations). Legislative authority over intelligence could be shared for all entities with overlapping jurisdiction; or, as is now the case in the House and Senate, it could be held exclusively for certain specified components (e.g., CIA and DNI), while being shared for others.

Membership

A bicameral body requires equal membership from both the Senate and House. In addition to bicameralism, a joint committee on intelligence could be directed to accommodate three other criteria: bipartisanship, representation of specified standing committees, and at-large selection of members.

For example, the membership from each chamber could be required to have representatives from standing committees with overlapping jurisdiction (e.g., Appropriations, Armed Services, Foreign Affairs/Foreign Relations, and Judiciary), as both the House and Senate Intelligence Committees do now. This selection might include both a majority and a minority party member from each represented committee. A JCI could also call for a specified number of members selected at-large, as the Senate intelligence panel does now. As an illustration, an 18-member JCI could include nine Senators and nine Representatives, with five majority and four minority party members from each chamber. At least one member, but not more than two, could come from each of the four committees with overlapping jurisdiction; this option (a maximum of eight from each chamber) would still allow for one selection at large from each house. By comparison, a larger committee or a panel requiring only a single member from each of the specified standing committees would allow for more members to be selected at-large.

Provision could also be made for *ex officio* members, particularly the majority and minority party leaders from the Senate and the Speaker and minority leader from the House.

Terms and Rotation

Membership on the joint committee could have no term limits or be given a maximum length of service (six or eight years, as the House and Senate Intelligence Committees have had, or shorter or longer terms). Under term limits, the total time on the committee might be measured either by continuous service or by non-continuous service accumulated over a specified number of Congresses (e.g., a total of eight years over six Congresses). If a JCI had maximum lengths of service, it could be treated as a temporary assignment, which might not count against other standing committee assignments in each chamber. By comparison, membership on

the JCI could be permanent.[14] If so, it might be treated as if it were a standing committee in each chamber, counting against other committee assignments.

Member terms could also be staggered, so that new members would arrive with each new Congress. Staggered terms, however, would mean that a portion of the original membership could not serve the maximum period, at least not as part of the original composition.

Leadership

The chair, selected at the beginning of each Congress or each session (as some proposals called for), could alternate between the two chambers and/or political parties. A vice chairmanship could also be established; this officer would replace the chair when he or she is absent (as occurs now on the Senate Intelligence Committee). The vice chair could be a member of the other body and/or the other political party.

Secrecy Controls

Various types of secrecy controls could be applied to a joint committee on intelligence to regulate access to its classified holdings by non-committee members, protect against the unauthorized disclosure of classified information, and allow its authorized release. Such controls could (1) set requirements for determining access by non-members; (2) require security clearances, oaths, and/or secrecy agreements for committee members and staff; and (3) provide for investigation of suspected security breaches, conducted by the House and Senate ethics committees.

Controls could also spell out procedures for disclosing classified information to which the President objects, either by a joint committee itself, by the joint committee in concert with either or both chambers, or by either or both chambers as the final arbiter. One of five distinct options might be adopted: (1) the joint committee on intelligence could act alone; (2) the panel could act only after one house responded to a request from it to release classified information; (3) the JCI could act only after both houses responded; (4) a single house could disclose the information; or (5) both chambers would have to agree to do so. Currently, disclosure procedures differ between the House and Senate intelligence panels. The House select committee does not have authority to release classified information on its own. The full House must act to disclose it, at the request of its intelligence panel, if the President objects to the release. On the Senate side, the select committee may disclose classified information on its own, after both the President and full Senate have acted.[15] It appears that this procedure has not been used by the Senate panel.

---

[14] The 9/11 Commission — referring to both a joint committee on intelligence and a new standing committee in each house — recommended that "Members should serve indefinitely on the committees, without set terms, thereby letting them accumulate expertise." 9/11 Commission, *Report*, p. 421.

[15] The select committee's charter provides for three responses from the full Senate to an Intelligence Committee request to release classified information, if the President objects to it. The chamber can (1) approve the disclosure; (2) disapprove the disclosure; or (3) "refer

(continued...)

Staffing

The number of staff on a new JCI would presumably be smaller than the combined total for both the House and Senate Intelligence Committees. Hiring could be accomplished in seven different ways: (1) by the majority party on the full JCI; (2) by the majority party from each chamber on the committee; (3) by full committee vote; (4) by the majority party and minority party separately; (5) by the chair alone; (6) by the chair and vice chair/ranking minority member together; or (7) by individual members (with each legislator selecting a single staff member). Additionally, staff could be selected by a combination of several compatible ways (e.g., individual member selections for some plus committee-wide selections for others). The staff could also be required to meet certain agreed upon criteria set by the committee, such as fitness for the duties and without regard to party affiliation.[16]

Staffers could be required to have an appropriate security clearance (for Top Secret and access to Sensitive Compartmented Information), as is now mandated by both House and Senate select committees. They could also be directed to sign a nondisclosure or secrecy agreement not to reveal classified information, again a requirement for the staff of both intelligence panels.

Budget and Funding

The budget for a joint committee on intelligence would presumably be smaller than the combined budgets of the House and Senate intelligence panels. Funding could be shared by both chambers, deriving equally from the contingent funds of the Senate and House.

Pros and Cons

Differences over the establishment of a joint committee on intelligence tie into practical matters as well as matters of principle.

Pros. Supporters of a joint committee on intelligence argue that it would make for a more effective and efficient overseer than the current arrangement, which the 9/11 Commission concluded "is now dysfunctional," because of limitations on the

---

[15] (...continued)
all or any portion of the matter back to the committee, in which case the committee shall make the final determination with respect to the public disclosure of the information in question" (Sec. 8(b)(5), S.Res. 400, 94th Cong., 2nd sess.).

[16] The 9/11 Commission, for instance, recommended that the "staff of this committee should be nonpartisan and work for the entire committee and not for individual members." 9/11 Commission, *Report*, p. 420.

two select committees.[17] According to its proponents, a single joint committee, housing fewer members and staff than the two existing ones combined, would:

- Strengthen oversight of intelligence for four primary reasons. The executive would be more open and forthright with a single, small oversight body than with two with a larger combined membership; the legislators and staff on the JCI, recognizing that there is no other authorizing panel to conduct oversight, would attach a greater importance to this responsibility; a committee composed of legislators from both chambers could better integrate and take advantage of congressional expertise and experience in the field; and a JCI could be established with fewer restraints and restrictions than the separate select committees now have.

- Improve coordination, cooperation, and comity between the House and Senate and among other relevant committees (with overlapping jurisdiction) in both chambers. A joint committee could serve as a conduit of information and advice and as a facilitator for policy formulation between the two chambers as well as between the political parties; a JCI could also encourage mutual respect and trust between the chambers and parties; this could occur by treating all of its members equally in committee leadership posts and voting, by merging the stands of Members of both houses in committee deliberations and decisions, by taking a joint committee consensus on legislation, endorsed by Members of both chambers, to the floor of each house, and by providing an opportunity for House Members to be involved, if only marginally and informally, in a Senate function (i.e., confirmation of presidential nominees).

- Streamline the legislative process, because only one committee, rather than two, would have to consider and report legislative proposals and authorizations to the floors of both chambers; members from the same joint committee, moreover, might comprise all or a majority of the membership of conference committees, which might be less necessary in the first place because of the bicameral, bipartisan makeup of a joint committee.

---

[17] Competing views on a joint committee on intelligence are available from Members and committees of Congress, among other sources. Supportive arguments are included in: U.S. Congress, Senate Temporary Select Committee to Study the Senate Committee System, *Report* (Washington: GPO, 1984), pp. 13-14; Sen. Howard Baker and Rep. Henry Hyde, statements before the Temporary Select Committee, *Senate Resolution 127, To Study the Senate Committee System* (Washington: GPO, 1984), part 1, pp. 5-11 and part 2, pp. 83-85; Rep. Henry Hyde, statement before the Joint Committee on the Organization of Congress, *Committee Structure*, hearings, 103rd Cong., 1st sess. (Washington: GPO, 1993), pp. 832-841; and Minority, Senate Select Committee on Secret Military Assistance to Iran and the Nicaraguan Opposition and House Select Committee to Investigate Covert Arms Transactions with Iran, *Report*, S.Rept. 100-216 and H.Rept. 100-433, 100th Cong., 1st sess. (Washington: GPO, 1987), p. 583.

- Respond rapidly to investigate a major development, when conditions dictated.

- Increase the stature of overseeing and legislating on intelligence matters and, thus, make serving on an intelligence panel more attractive and important than on either select committee. This could result from making the joint committee the equivalent of a standing committee, by granting it permanency and authority to report legislation to each chamber and giving the members indefinite tenure. A JCI with these characteristics would be unique in the current era, the first of its kind since 1977, and apparently one of only a few in the history of Congress, also elevating its stature.

- Make for more efficient government. A single panel, versus two, would probably reduce the amount of time that the Administration and intelligence officials would spend on Capitol Hill testifying, briefing, notifying, and meeting with members and panels.

- Improve the protection of classified information in Congress's possession. A smaller number of legislators and staff on a joint committee would have access to it, and a single office would be easier to secure.

- Encourage trust between Congress and the Executive in this sensitive field. This could occur by reducing the number of panels, Members, and staff with access to such highly classified information and by easing the cooperative relationship between the branches by way of a single committee, instead of two.

- Pinpoint responsibility in Congress for oversight and legislation affecting intelligence, thereby avoiding any confusion or uncertainty about it.

- Cut back the total number of committee seats for legislators in the House and Senate combined, by replacing the two panels with a single committee with fewer seats; for instance, a new 18-member joint committee with nine Senators and Representatives would be half the size of the combined total of 37 on the two select committees. The replacement would modestly help reduce the number of legislators holding too many committee assignments and/or being "spread too thin." Reducing the number of seats available for Representatives and Senators would allow them to concentrate on one less committee assignment.

- Reduce costs, because of fewer staff and a single suite of offices.

Cons. Critics of proposals for replacing the current House and Senate Intelligence Committees with a single joint committee contend that it would weaken oversight and compromise a fundamental feature of the Congress, namely, two

different (and sometimes competing) bodies.[18] As viewed by its opponents, a JCI would:

- Adversely affect oversight of intelligence. This would occur by reducing the number of legislators and staff who have an incentive and opportunity to conduct oversight and by reducing the number of separate panels, with different characteristics and incentive structures, to conduct it; in this regard, the number of committees to which the President reports covert action plans is now only two (the select committees on intelligence), having been reduced from eight in 1980, at the request of the executive.

- Undercut the legislative benefits (e.g. longer deliberation time and different viewpoints) of relying on two committees from separate and distinctive chambers. This usual situation allows two panels — each reflecting different chambers, types of constituencies, and electoral schedules — to examine the same legislation and authorizations and conduct oversight from different vantage points, based on their own priorities and demands; the loss of a second view would be felt not only in the initial committee deliberations but also in later conference committee action, which might be dominated by joint committee members.

- Cause a loss in continuity, stability, and experience. This would be especially evident in joint committee leadership, if the chair (and ranking member or vice chair) rotated every two years; this in turn would make membership on the joint committee less desirable than on other panels; the turnover could also extend to staff, because of the frequent change in leadership; finally, this loss of stability and experience could hamper Congress's ability to influence public policy and compete with the executive.

- Result in a more acute impact on Congress if a joint committee develops a close and supportive relationship with the executive entities it oversees, rather than a neutral and critical one. With a single panel, Congress would have only one locus for oversight and checks on the executive, not two; if this happens, the impact on Congress, on oversight, and on legislation would be more extensive

---

[18] Criticisms and concerns are voiced by Rep. Dan Glickman, Rep. Larry Combest, and Sen. Dennis DeConcini, statements before the Joint Committee on the Organization of Congress, *Committee Structure*, hearings, 103rd Cong., 1st sess., pp. 64-79 and 406-412; Rep. Larry Combest, Chairman of the House Permanent Select Committee on Intelligence, "IC21 — The Intelligence Community in the 21st Century, The Intelligence Community Act of 1996," Mar. 4, 1996, p. 7; U.S. Congress, House Permanent Select Committee on Intelligence. *IC21: Intelligence Community in the 21st Century* (staff study), committee print, 104th Cong., 2nd sess. (Washington: GPO, 1966), pp. 316-318 and 328; House Select Committee on Committees, *Final Report* (Washington: GPO, 1980), p. 416; and Majority, Senate and House Select Committees Investigating the Iran-Contra Affair, *Report*, p. 427.

and significant, because of the absence of a possible balance from a second committee.

- Operate contrary to the long-term tendency to end reliance on joint committees, either by abolishing them or not establishing them in the first place.[19] A JCI, if authorized to report legislation to the floor of both houses, would be unique currently; it would be the only such empowered joint committee since 1977 (when the JCAE was abolished), and one of the few in the history of the Congress; a joint committee on intelligence would also raise the prospect of similar panels for other policy areas, including homeland security, which have wide-ranging jurisdictions that cross a number of executive agencies and programs along with congressional committee jurisdictions.

- Harbor uncertainty regarding confirmation of presidential nominees. It might be unclear whether House Members should play any role at all in the process or, if so, perhaps only at certain stages (e.g., initial meetings and interviews, background investigations, formal hearings).

- Artificially make the political parties equal or nearly so. This could occur, even though the differences in party ratios in each chamber could be substantial, as they have been in the past.

- Artificially make the two chambers equal on the joint committee. The number of Members from each chamber would be the same, even though the House is more than four times larger than the Senate; because of this situation, Representatives would have proportionately fewer opportunities to serve on a joint committee than Senators.

- Cut back the possibility of serving on an intelligence panel for all Members of Congress, especially if there are no term limits on JCI membership. This reduction in numbers would, in turn, reduce the diversity and representational characteristics of the membership compared to two separate committees.

- Bring about a change in the different jurisdictions that the current select committees now hold. The House panel having a broader jurisdiction than its Senate counterpart.

---

[19] The 9/11 Commission (p. 421), for instance, did not advocate a joint committee for homeland security. Instead, it called for consolidating jurisdiction in a permanent standing committee in each chamber. For additional discussion on such a transformation, see CRS Report RS21901, *House Select Committee on Homeland Security: Possible Questions Raised If the Panel Were to Be Reconstituted as a Standing Committee*, by Judy Schneider.

- Not necessarily improve protection of classified information over the current two select committees. Their controls over it are exacting and their reputations in this regard are good; a JCI could also require new procedures for the public release of classified intelligence information held by the joint committee; this would raise the prospect of (and cause disagreement over) whether the joint committee alone could do so, whether one chamber could do so, or whether both houses must act together as the final arbiter.

- Add confusion and conflict over investigations of suspected unauthorized disclosures of classified information. This could arise, for instance, if the ethics committee from one chamber conducted investigations which involved members of the other body, even if only tangentially and in an initial inquiry.

- Raise practical difficulties in setting meeting schedules, times, and locations for panel members from two different chambers of Congress.

Alternatives to a Joint Committee

There are other options which might enhance and regularize congressional oversight of intelligence. These changes, both formal and informal, could have an impact not only on the structure of the current select committees on intelligence, but also on the relationship between the new panels, if approved. They could also affect each panel's relationship with other committees and Members in its respective chamber and its counterparts in the opposite chamber, as well as the relationship between the legislature and the executive.

Changing the Select Committees' Structure and Powers

Most direct and immediate among the options to increase and improve oversight of intelligence would be ways to enhance the status, stature, and resources of the existing select committees on intelligence or replace them with standing committees.[20] This might be accomplished through several different (and sometimes competing) means:

---

[20] The 9/11 Commission emphasized the need for "substantial change" in congressional oversight, either by establishing a joint committee or by creating "a single committee in each house of Congress, combining authorization and appropriating authorities .... " Each panel would be a standing committee and hold subpoena authority. The membership would be relatively small and serve without term limits. Its composition would be nearly equal between the parties, with the majority having only one more member than the minority, and representing four panels with overlapping jurisdiction (i.e., Armed Services, Judiciary, Foreign Affairs, and the Defense Appropriations Subcommittee) with one seat each on the new committee. 9/11 Commission, *Report*, p. 420-421. For further information and analysis, see CRS Report RS21908, *Senate Select Committee on Intelligence: Term Limits and Assignment Limitations*, by Judy Schneider.

- Grant the current select committees status as standing committees, along with indefinite tenure for their membership, to reduce turnover; increase experience, stability, and continuity; and make membership on the panel more attractive.

- Expand the authority of such committees, giving them power to report appropriations as well as authorizations and to hold subpoena authority on their own.

- Place members of the Select Committee on Intelligence on their chamber's Defense Appropriations Subcommittee or other subcommittee with jurisdiction over IC appropriations; or create a special advisory and oversight body on the Appropriations Committee, combining Intelligence Committee and Appropriations Committee members, as the House has done; under the latter plan, the new panel would report its findings and recommendations for IC funding to the defense or other appropriate subcommittee, thereby modestly expanding the effective jurisdiction and influence of the select committee.[21]

- Add professional staff, hire temporary consultants, or set up short-term task forces, especially in fields where the panels might require new or expanded expertise and skills.

Senate Action. Several of these suggestions were approved by the Senate on October 9, 2004, when it agreed to S.Res. 445 (108th Congress) affecting its oversight of intelligence. The resolution eliminated certain restrictions on serving on the select committee, reduced the number of members (from 17 to 15), and modified security procedures regarding the public disclosure of classified information. S.Res. 445, however, did not transfer authority and jurisdiction over intelligence appropriations to the Intelligence Committee; instead, it created an Intelligence Subcommittee on the Senate Appropriations Committee.

Additional steps have been taken in the 110th Congress. A prominent one is a Memorandum of Agreement (MOA), designed to improve coordination and transparency between the Intelligence Committee and Appropriations Committee.[22] The MOA — signed by the chairman of the select committee (but not its ranking

---

[21] This proposal materialized in 2007 in the House with members of the Intelligence Committee serving on a special oversight panel on the Appropriations Committee (H.Res. 35, 110th Congress). The concept was raised in late 2006 by Rep. Nancy Pelosi, then House Minority Leader and prospective Speaker of the House. Tim Starks, "Pelosi Wants Intelligence Appropriations Oversight Panel," *CQ.com*, Dec. 14, 2006; David Rogers, "Pelosi Plans Panel to Oversee Spy-Agency Funds," *Wall Street Journal*, Dec. 14, 2006, p. A3; and "Pelosi Looks to Boost Oversight of Intelligence and Ethics," *Washington Post*, Dec. 15, 2006.

[22] Hon. John D. Rockefeller, Chairman, Opening Statement, in U.S. Congress, Senate Select Committee on Intelligence, *Congressional Oversight*, hearing, 110th Cong., 1st sess., Nov. 13, 2007, p. 2.

minority member) and the chairs and ranking minority members of the Senate Appropriations Committee and its defense subcommittee — advanced several changes to accomplish this:

- notify staff and allow them to attend the intelligence hearings of the other body;
- allow each Intelligence Committee member who is also an appropriator to bring his or her intelligence staff members to Appropriations Committee hearings and markups;
- permit all Senators and cleared staff of one committee to review the bill, report, and classified annex of the other before action is taken; and
- give the chairmen and ranking minority members of each committee the opportunity to appear before the other panel to present their views prior to the markup of either the intelligence authorization or appropriations bills.[23]

Notwithstanding the effort, the effectiveness of the new arrangements under the Memorandum of Agreement has elicited differing impressions. The chairman of the Senate Intelligence Committee emphasized that the agreement "has made great strides toward bringing our committees together in a unity of effort that was lacking before."[24] A competing interpretation was offered by the Intelligence Committee's ranking minority member, who is also an appropriator. He determined that the MOA was "ineffective," adding that "in my experience I've seen more evidence of the need for a better synthesis of the two."[25]

House Action. A different option — reserving seats for Intelligence Committee members on the Defense Appropriations Subcommittee — was raised at the end of the 109th Congress by Representative Nancy Pelosi, then House Minority Leader and presumptive Speaker of the House in the 110th Congress.[26] The final product was a variation on this theme. H. Res 35 (110th Congress), which passed the House on January 9, 2007, created a new Select Intelligence Oversight Panel — consisting of 13 members and an eight-to-five inter-party ratio — with three representatives from the Intelligence Committee joining 10 from appropriations, including the chairman and ranking minority member of the full committee, the chairman and ranking minority member of the Defense Subcommittee, and six additional members from appropriations. This special panel is authorized to study and make recommendations to all appropriations subcommittees on relevant areas,

---

[23] Ibid., pp. 2-3.

[24] Ibid., p. 3.

[25] Hon. Christopher S. Bond, Opening Statement, in Senate Intelligence Committee, *Congressional Oversight*, pp. 4-5.

[26] Sources in footnote 21.

specifically the annual intelligence appropriations to the Defense Subcommittee, which retains authority to report it to the full committee.

Concerns about Restructuring the Intelligence Committees. The set of changes producing a restructured and strengthened Intelligence Committee in each chamber, as called for by the 9/11 Commission, might also generate concerns and criticisms . A standing committee — smaller than the existing select committees in each chamber, with representation from four standing committees with overlapping membership and indefinite tenure for its members — would substantially reduce (1) the number of Members in each chamber serving on such a panel at any one time; (2) the number of at-large seats available; (3) the number of vacancies available over time; and, thus, (4) the likelihood of a Member finding a seat on the committee. These changes in tandem could also lead to fewer former members from the committee, thus, reducing the ability of the full chamber and non-members to be knowledgeable about how the intelligence community operates and intelligence policy; and it could result in a decline of the ability to question if not challenge the committee. Arguably, this could result in a more likely prospect of a closed system, making it easier for the intelligence panels to dominate the agenda and debate in their respective chambers and in the full Congress.

A second set of cautions might surround the proposed new authority, particularly, adding appropriations to its authorizing control and independent subpoena power. Such subpoena authority, which could cover either or both materials and individual testimony, would be held (and used) without needing approval in each instance by the chamber. This might be seen as infringing on an important full-chamber power and removing a check on this particular committee, which would be already subject to fewer constraints than the current select committees have.

The addition of appropriations approval would apparently produce a unique situation in the contemporary Congress and a rarity in its entire history. A reversal of this plan — placing Intelligence Committee members on the defense appropriations subcommittee — also appears to be a rare, if not unprecedented action; it could better coordinate and complement the actions of both panels. This change, moreover, could indirectly increase the power of the select committee. By reserving seats for its members on the relevant appropriations subcommittee, the Intelligence Committee would play a more direct and influential role in appropriating IC funds than it does now. At this time, no other committee has a comparable guarantee of seats on a relevant appropriations subcommittee. Consequently, the left-out authorizing committees, particularly those dealing with sensitive national security matters, might make the same appeal as intelligence: that is, to have reserved seats on the appropriate appropriations subcommittee. Following either avenue, the intelligence panel's power would be enhanced if it held both appropriations and authorization authority, either directly or indirectly (via its members on the defense appropriations subcommittee).

In either event, however, the intelligence panel might be perceived as too powerful. It would hold two impressive and reinforcing authorities and would no longer be subject to a check and competition from a significant outside source (i.e.,

the Appropriations Committee in its chamber). At the same time, the transfer of appropriations would remove an important part of the Appropriations Committees' jurisdiction. Reserving seats for Intelligence Committee members on defense appropriations could also reduce competing viewpoints and an independent check on IC appropriations. Either change might encourage other authorizing committees to request the same treatment, that is, to control both appropriations and authorizations. Although the appropriations and authorization processes are parallel to one another, they are not identical and not always reinforcing or complementary. The combined authority could result in substantially more work for the Intelligence Committee in each session, with the need to "scrub" the intelligence budget twice each year. Or, alternatively, the transfer could lessen its examination of the appropriations and authorization, if each were to occur only in alternate sessions within a single Congress. The potential increase in the panel's workload could have two adverse ramifications: (1) short-change either the appropriations or authorization process, or both; or (2) reduce the panel's time for other legislative and oversight efforts.

By comparison to these two proposed changes — consolidating authorization and appropriations in the Intelligence Committee or reserving seats on the Defense Appropriations Subcommittee for Intelligence Committee members — the establishment of the special intelligence oversight panel on the House Appropriations Committee is more limited in its impact. Only three of its 13 seats are reserved for Intelligence Committee members; and the new panel can only make recommendations to the Defense Appropriations Subcommittee, which continues to report the annual intelligence community appropriations.

Improving Coordination Between the Two Intelligence Panels

Such changes would affect the Intelligence Committees' individual structure and powers. Others could be designed to increase coordination and shared responsibility between the two intelligence panels — so as to avoid duplication, encourage cooperation, develop working relationships across chambers, enhance understanding, and share expertise, information, and knowledge — while at the same time, maintaining the distinct characteristics of each panel. These might include joint hearings and cross-committee leadership meetings, which may already exist on a regular basis.

Joint Hearings. One option along these lines is to schedule joint hearings for relatively routine and regular matters, such as the initial annual authorization briefings from the Executive. Another opportunity for a joint session would occur when the inspectors general in the intelligence community, especially at the CIA, submit their semiannual reports to Congress. These shared enterprises could allow the combined membership to receive the same information and data as each panel would individually, establish working relationships among the two groups of members, encourage cross-fertilization among them, and reduce duplication for the Executive. Of course, followup hearings could be handled separately by the two panels and may even be stimulated by such joint efforts. The shared experience over the initial budget submission could also help to avoid duplication of effort over some modest matters, while helping to set priorities for more significant ones.

Joint hearings could also be conducted into critical events, as they were with the Select Intelligence Committees combined inquiry into 9/11 attacks.[27] Another example of an inquiry with panels from both chambers was the Iran-contra affair, an investigation conducted by two temporary committees working together and issuing a joint report.[28]

Leadership Meetings. Another means of encouraging inter-chamber cooperation is for the leadership of the two panels to meet regularly to discuss issues, concerns, and priorities (recognizing, of course, the practical and political limitations on such exchanges). These efforts might include only the full committee chairs or might extend to subcommittee heads and majority and minority members. These sessions could be supplemented by meetings of senior staff on both panels, at the direction of the leadership. Whatever the arrangement, a number of different opportunities exist to enhance awareness of common concerns and cooperation in examining them between the two panels.

Constraints on Coordination. Coordination between two panels from different chambers may encounter practical and political problems. Scheduling meetings and hearings, especially if a large number of members is involved, for instance, runs into several hindrances. These include: (1) different priorities and meeting arrangements for each committee; (2) competing chamber and committee responsibilities for Members, especially Senators, each of whom serve on more committees than Representatives; and (3) different electoral and campaign requirements, which affect the demands on Members and the time they spend in the capital. In addition, rival political affiliations and policy stands, along with competition between the chambers for influence over public policy, might make cooperative ventures few and far between.

Interchanges with Other Panels and Members

Other approaches to increasing the powers of each panel and their cooperative ventures might be considered: ease the exchange of information with non-committee members, allow for more oversight by other committees, and/or increase contacts among members of the appropriations and authorizing panels. Along these lines, the 9/11Commission wrote, the "new committee or committees should conduct studies of the activities of the intelligence agencies and report problems relating to the development and use of intelligence to all members of the House and Senate."[29]

---

[27] U.S. Congress, Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence, *Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*, S.Rept. 107-351 and H.Rept. 107-792, 107th Cong., 2nd sess. (Washington: GPO, 2002).

[28] U.S. Congress, Senate Select Committee on Secret Military Assistance to Iran and the Nicaraguan Opposition, and House Select Committee to Investigate Covert Arms Transactions with Iran, *Report on the Iran-Contra Affair*, S.Rept. 100-216 and H.Rept. 100-433, 100th Cong., 1st sess. (Washington: GPO, 1987).

[29] 9/11 Commission, *Report*, p. 420.

Placing Intelligence Committee members on the defense appropriations subcommittee or on a special appropriations intelligence oversight panel, as the House has done, also eases interchanges between these two committees. Other ways of increasing coordination between the appropriations and authorizing committees — through formalized member and staff involvement in the other panel's hearings, for instance — have been advanced in the Senate, as noted above.

Goals. This type of change could reduce the challenge of intelligence oversight on the select committees, bring different viewpoints to bear on intelligence matters, expand the knowledge of Members not on the panels, and allow for their informed judgments on intelligence policy and programs as well as on committee activities and operations. Strict controls over the classified information would have to be maintained. The current committee rules — which on the House side are more stringent than on any other committee — might be modified to accommodate additional sources for review and oversight. Such a revision could begin with a comparison of access controls by other panels, particularly the committees with overlapping membership. In addition, House and Senate chamber rules authorizing secret or closed sessions might be used more often to allow for an open exchange of information between the Intelligence Committees and all the Members of a particular chamber. Along with this, committee members might be allowed to present "declassified" versions of sensitive or otherwise classified reports to their colleagues, in secret or open sessions.

Techniques. Several potential techniques to expand non-committee involvement and non-member access to information follow:

- Ensure that relevant information is appropriately and expeditiously shared with committees with overlapping membership.
- Give greater allowance for other committees to conduct oversight of intelligence components, activities, and programs, including standing committees without overlapping membership.[30]
- Ease access for non-members to Intelligence Committee holdings, by reducing the exacting requirements over the availability of the classified.
- Encourage the Intelligence Committees, on their own initiative, to share information as appropriate with the full membership of their house.
- Make more information available to non-members by securing declassification of certain intelligence reports or by providing classified and declassified versions of IC reports (for the committees and for the general membership, respectively); the agencies proper or their inspectors general (charged with preventing and detecting

---

[30] See especially House Subcommittees on Efficiency and on National Security, *CIA Refusal*, 2001.

waste, fraud, and abuse) might do either or both, possibly at the request or directive of the Intelligence Committees.

Limitations. Interchanges between the Intelligence Committees, on the one hand, and other panels and Members, on the other, might be limited for several reasons. Concerns about the unauthorized disclosures of classified information might be raised as the possibility of leaks rises, because of the increased number of individuals with access to sensitive information. Along with this, intelligence agencies would likely be reluctant to respond to congressional requests for sensitive and classified information, even from the Intelligence Committees, if the agencies anticipate that all or some of it will be disclosed outside the sequestered Intelligence Committee rooms, possibly to the floors of both houses.

Another possibility, which might retard information-sharing by the Intelligence Committees, could be a concern about a reduction in their control over the intelligence agenda and debate. As more Members and panels became familiar with the relevant information and policies, more questions might arise relating to the committees' policy positions. This development might be seen as weakening the committees, a condition that might reduce their (and, in turn, Congress's) influence over intelligence agencies and policies in dealings with the Executive.

Other Proposals

Use of Congressional Support Agencies. Other options might enhance the oversight capabilities of the select committees on intelligence and other appropriate panels. One is increased use of the legislative support agencies — Congressional Budget Office, Congressional Research Service, and Government Accountability Office (GAO), formerly the General Accounting Office — where appropriate.[31] A supplemental proposal would be to clarify and expand GAO's

[31] The oversight roles of the support agencies are spelled out in CRS Report RL30240, *Congressional Oversight Manual*, by Frederick M. Kaiser, et al.

independent authority to audit all components of the intelligence community.[32] Legislation to accomplish this has been introduced in the 110th Congress.[33]

Applying GPRA Requirements to the CIA. A different scheme would affect the executive directly: place the CIA expressly under the requirements of the Government Performance and Results Act, commonly referred to by its initials (GPRA) or as the Results Act. This 1993 enactment emphasizes assessing agencies based on outcomes (that is, their performance and results) rather than outputs (for instance, meeting certain deadlines or expenditure levels).[34] The CIA remains the only significant exemption to GPRA's mandates. These include developing a broad mission statement; a five-year strategic plan flowing from it; an annual performance plan, setting specific objectives and ways to carry out the strategic plan; and a followup evaluation of the agency's accomplishments, failures to meet expectations, and reasons for both. These GPRA reports from the CIA could be submitted to the House and Senate Intelligence Committees in a classified version.

Changes Affecting the Inspectors General. A different set of alternatives would rely upon changes in offices of inspector general (OIGs), established in executive departments and entities to combat waste, fraud, and abuse and to keep the agency head and Congress fully and currently informed about these matters.[35] Changes that might directly or indirectly benefit congressional oversight of intelligence would be to (1) enhance the coordination among the relevant offices of inspectors general through existing or new councils and other mechanisms;[36] (2)

---

[32] Most significantly, GAO is limited in its independent authority to audit and investigate the CIA, which apparently is off-limits to the Office because of provisions in public law and congressional rules. The CIA, however, is the only intelligence component which makes such an across-the-board claim. See U.S. General Accounting Office, *Central Intelligence Agency: Observations on GAO Access to Information on CIA Programs and Activities*, statement by Henry J. Hinton, GAO-01-975T (Washington: GAO, 2001); *Information Sharing*, GAO-06-385, (Washington: GAO, 2006), pp. 6-7; and *DOD Personnel Security Clearances*, Letter to Honorable George V. Voinovich, Chairman, Senate Subcommittee on Oversight of Government Management, June 14, 2006, p. 1. See also U.S. House Government Reform Subcommittees on Government Efficiency and on National Security, *Is the CIA's Refusal to Cooperate with Congressional Inquiries a Threat to Effective Oversight of the Federal Government*, hearings, 107th Cong., 1st sess (Washington: GPO, 2001); Frederick M. Kaiser, "GAO Versus the CIA: Uphill Battles Against an Overpowering Force," *International Journal of Intelligence and Counterintelligence*, vol. 15 (2002), pp. 330-389; and CRS Report RL30349, *GAO: Government Accountability Office and General Accounting Office*, by Frederick M. Kaiser.

[33] Identical bills to expand and clarify GAO's independent audit authority over the intelligence community have been introduced in the 110th Congress: the Intelligence Community Audit Act of 2007, H.R. 978, introduced by Representative Bennie Thompson; and S. 82, introduced by Senator Daniel Akaka.

[34] P.L. 103-62, 107 Stat. 285.

[35] 5 U.S.C. Appendix. For an overview and other sources, see CRS Report 98-379, *Statutory Offices of Inspector General: Past and Present*, by Frederick M. Kaiser.

[36] In the 110th Congress, several legislative initiatives are designed to enhance the

(continued...)

establish a post of inspector general with comprehensive jurisdiction over the intelligence community;[37] (3) clarify and strengthen the jurisdiction and authority of the statutory OIGs over the administratively created counterparts within an agency or department; and (4) augment the authority, jurisdiction, independence, and reporting requirements of the IG in the Office of the Director of National Intelligence.[38]

Observations on Oversight of Intelligence

Obstacles to Oversight

Congressional oversight of intelligence meets obstacles that are not usually present in other areas.[39]

Secrecy Constraints. The most significant constraint is the high degree and pervasiveness of secrecy surrounding intelligence policy, information, activities, operations, resources, and personnel. For Congress, this means that the legislature, its committees, and its Members are circumscribed in a number of ways: what they know; who receives the information, how, and in what form and forum; who provides it; what information can be shared with other Members and panels, how, and in what detail; and what non-governmental sources can contribute to legislators' knowledge, to what degree, and in what ways.

---

[36] (...continued)
independence and coordination among inspectors general. This would occur through additional protections for the IGs and a new coordinative council, which would include the statutory IGs in the intelligence community (IC), among others operating under the IG Act and other laws. Prominent bills include H.R. 928, which passed the House, and S. 2324, as reported by the Senate Committee on Homeland Security and Governmental Affairs. CRS Report RL34176, *Statutory Inspectors General: Legislative Developments and Legal Issues*, by Vanessa K. Burrows and Frederick M. Kaiser.

[37] Along this line, the Senate intelligence panel has proposed a new Inspector General of the Intelligence Community. Notwithstanding its overarching jurisdiction, the IC inspector general would not replace the existing counterparts in various departments and agencies. U.S. Senate Committee on Intelligence, *Intelligence Authorization Act for Fiscal Year 2008*, S.Rept. 110-75, 110th Cong., 1st sess., pp. 16-19.

[38] The DNI, under authority establishing the post and office (P.L. 108-458), has complete discretion to create and construct an OIG in his Office, based on provisions he selects from the Inspector General Act of 1978, as amended. In 2006, the director established an inspector general post in his office. U.S. Office of the Director of National Intelligence, *Report on the Progress of the DNI in Implementing the Intelligence Reform Act of 2004*, May 2006. In the meantime, however, the House and Senate Intelligence Committees have raised questions about the IG's independence, capabilities, jurisdiction, and reporting to Congress. U.S. House Committee on Intelligence, *Intelligence Authorization Act for 2007*, H.Rept. 109-411, 109th Cong., 2nd sess.

[39] See CRS Report RL32617, *A Perspective on Congress's Oversight Function*, by Walter J. Oleszek.

The secrecy imperative also results in a system that is often closed to outsiders — not just the general public but also Representatives and Senators who do not have seats on the select committees on intelligence. The impact of official secrecy is evident in the restrictions on access to and disclosure of classified information in the panels' custody as well as on restraints covering what the select committee members themselves can discuss. These restrictions and their demanding requirements not only slow down or prevent access by non-members, because of an anticipated lengthy delay in complying with the procedures, but might also harbor a "chilling effect" for some, because of the strict limitations on disclosure and use of the information among colleagues outside the Intelligence Committees. As noted above, moreover, other access controls adopted by the executive set limits on the Government Accountability Office, Congress's chief audit and investigative agency.

The impacts and implications of secrecy are extensive and burdensome. The 9/11 Commission summarized the effects this way: "Secrecy stifles oversight, accountability, and information sharing."[40]

Appeal of Intelligence Oversight. Along with this is the apparently limited appeal of overseeing intelligence and making intelligence policy, including authorizing the budget. Congressional efforts here remain largely hidden and may have only marginal direct effects on Members' constituencies, districts, or states.[41]

Overcoming the Obstacles

Objectives and Goals. The impact of these limitations on Congress's oversight of intelligence is that it is significantly more difficult than in other fields. And the usual incentives for Members to serve on certain committees and conduct oversight appear to be more modest or even non-existent for intelligence.

Steps have been advanced, however, to increase Congress's capacity to overcome these hurdles. Prospects along this line include (1) heightening the appeal of serving on the intelligence panel; (2) enhancing the expertise and knowledge of Members (both on and off the panels); (3) reinforcing the shared responsibilities between an intelligence committee, on the one hand, and panels with overlapping memberships, on the other; (4) expanding the contacts and coordination between the intelligence authorizors and appropriators; (5) changing the relationship between the two chambers on intelligence matters, through, for instance, a joint committee or increased contacts between the existing committees; and (6) developing new connections between Congress and the executive that lends itself to more effective oversight.

The Joint Committee Approach and Alternatives. Growing out of these goals are a number of recommendations to strengthen oversight of intelligence, which have arisen since the genesis of the modern intelligence community six decades ago. Recent ones have come from the 9/11 Commission, which proposed

---

[40] 9/11 Commission, *Report*, p. 24.

[41] Ibid., pp. 420-421.

two distinct alternatives. One was to create a joint committee on intelligence. Yet over the years, the drafts for a JCI have differed in important respects: membership, leadership, jurisdiction, authority, staffing, and controls over classified information, among other matters. Moreover, rationales for a JCI have met with competing objections and concerns.

A second major option advanced by the 9/11 Commission was to enhance the powers and status of the Intelligence Committee in each house, along with realigning committee jurisdiction over intelligence appropriations, with the prospect of merging authorizing and appropriations in one committee. The Senate — in S.Res. 445 (108th Congress), approved October 9, 2004 — followed this path part of the way, when it removed the term limits on serving on its intelligence panel, reduced the number of members, and created a separate Subcommittee on Intelligence on the Appropriations Committee. In separate action, leaders on the Senate Intelligence and Appropriations Committees issued a Memorandum of Agreement in 2006 designed to improve coordination and transparency between the two. The House has traveled a different route, in creating a Select Intelligence Oversight Panel on the Appropriations Committee, which includes members of the Intelligence Committee.

Other approaches to change legislative oversight of intelligence have been proposed. These include several that would affect the executive directly as well as Congress's own structure and capabilities: increase the use of congressional support agencies; clarify and extend independent access for GAO to intelligence community agencies, particularly the CIA; require the CIA to meet the GPRA planning and reporting obligations, as other IC components must do; increase the independence of and the coordination among IC inspectors general; improve their reporting to Congress, where needed; and add a new inspector general with jurisdiction over the entire intelligence community.

Order Code RL33494

CRS Report for Congress

Security Classified and Controlled Information: History, Status, and Emerging Management Issues

Updated February 11, 2008

Harold C. Relyea
Specialist in American National Government
Government and Finance Division

Prepared for Members and Committees of Congress

Congressional Research Service

Security Classified and Controlled Information: History, Status, and Emerging Management Issues

Summary

The security classification regime in use within the federal executive branch traces its origins to armed forces information protection practices of the World War I era. The classification system — designating information, according to prescribed criteria and procedures, protected in accordance with one of three levels of sensitivity, based on the amount of harm to the national security that would result from its disclosure — attained a presidential character in 1940 when President Franklin D. Roosevelt issued the initial executive order prescribing these information security arrangements. Refinements in the creation, management, and declassification of national security information followed over the succeeding decades, and continue today. In many regards, these developments represent attempts to narrow the bases and discretion for assigning official secrecy to executive branch documents and materials. Limiting the quantity of security classified information has been thought to be desirable for a variety of important reasons: (1) promoting an informed citizenry, (2) effectuating accountability for government policies and practices, (3) realizing oversight of government operations, and (4) achieving efficiency and economy in government management.

Because security classification, however, was not possible for some kinds of information deemed in some quarters to be "sensitive," other kinds of designations or markings came to be applied to alert federal employees regarding its privileged or potentially harmful character. Sometimes these markings derived from statutory provisions requiring the protection of a type of information; others were administratively authorized with little detail about their use.

In the current environment, still affected by the long shadow of the terrorist attacks of September 11, 2001, several issues have arisen regarding security classified and controlled information. Volume is a concern: 8 million new classification actions in 2001 jumped to 14 million new actions in 2005, while the quantity of declassified pages dropped from 100 million in 2001 to 29 million in 2005. Expense is vexing: $4.5 billion spent on classification in 2001 increased to $7.1 billion in 2004, while declassification costs fell from $232 million in 2001 to $48.3 million in 2004, according to annual reports by the Information Security Oversight Office (ISOO) of the National Archives and Records Administration (NARA). Some agencies were recently discovered to be withdrawing archived records from public access and reclassifying them. Critically evaluating this activity, ISOO has indicated that the federal government needs to apply a more integrated approach among the classifying agencies. The force of, and authority for, information control markings, other than security classification labels, have come under congressional scrutiny, prompting concerns about their number, variety, lack of underlying managerial regimes, and effects. Among those effects, contend the Government Accountability Office and the manager of the Information Sharing Environment for the intelligence community, is the obstruction of information sharing across the federal government and with state and local governments. These and related matters, including remedial legislation (H.R. 984, H.R. 4806), are examined in this report, which will be updated as events warrant.

Contents

Classification Background 2

Control Markings Discovered 5

Control Markings Today 10

Comparison of Sensitive Security Information (SSI) Policies 12
- USDA Marking 12
- USDA Management 14
- TSA/DOT Marking 16
- TSA/DOT Management 16
- Management Regime Comparison 24

Implications for Information Sharing 26

Improving Classified Information Life Cycle Management 27

Remedial Legislation 31

Related Literature 32

List of Tables

Table 1. Management of Security Classified Information and SSI Compared . . 24
Table 2. Information Moving In and Out of Classified Status 28
Table 3. ISCAP Decisions 29

Security Classified and Controlled Information: History, Status, and Emerging Management Issues

Prescribed in various ways, federal policies may require the protection of, or provide a privileged status for, certain kinds of information. For the legislative branch, for example, the Constitution, in Article I, Section 5, specifies that each house of Congress "shall keep a Journal of its Proceedings, and from time to time publish the same, excepting such Parts as may in their Judgment require Secrecy." In the next section of the article, a privileged status for certain remarks of Members is established when the Constitution indicates that "for any Speech or Debate in either House, they shall not be questioned in any other Place."

Within the executive branch, it seems likely that one of the earliest-felt needs for secrecy concerned preparations and plans for the defense of the country. Following long-standing military practice, General George Washington and other officers in the Continental Army, seeking to ensure the protection of information, had written "Secret" or "Confidential" on strategic communiques to each other in the field and to headquarters. There was no immediate formalization of this practice by the new federal government, but it was from these roots that security classification would emerge. That history is briefly reviewed in the next section of this report.

The application of security classification subsequently came to be regulated through a narrowing of the bases and discretion for assigning official secrecy to executive branch materials. Due to that and other information management developments, new kinds of designations or markings came to be used to alert federal employees about the privileged status or sensitive content of a record or document. Sometimes these markings derived from statutory provisions requiring the protection of a type of information; many others were administratively created, but lacked detailed management regimes. Early congressional experience with these other markings is examined, providing a background for considering some of the current issues they raise.

Finally, the report considers some long-standing difficulties attending the management of security classified information — controlling the volume of such material and attendant costs. It looks, as well, at recent efforts by some agencies to withdraw archived records from public access and reclassify them, activity which the Information Security Oversight Office (ISOO) of the National Archives and Records Administration (NARA) critically evaluated and, as a reform for the underlying problem, suggested a more integrated approach among the classifying agencies.

Classification Background

Current security classification arrangements, prescribed by an executive order of the President, trace their origins to a March 1940 directive issued by President Franklin D. Roosevelt as E.O. 8381.[1] This development was probably prompted somewhat by desires to clarify the authority of civilian personnel in the national defense community to classify information, to establish a broader basis for protecting military information in view of growing global hostilities, and to manage better a discretionary power seemingly of increasing importance to the entire executive branch. Prior to this 1940 order, information had been designated officially secret by armed forces personnel pursuant to Army and Navy general orders and regulations. The first systematic procedures for the protection of national defense information, devoid of special markings, were established by War Department General Orders No. 3 of February 1912. Records determined to be "confidential" were to be kept under lock, "accessible only to the officer to whom intrusted." Serial numbers were issued for all such "confidential" materials, with the numbers marked on the documents, and lists of same kept at the offices from which they emanated. With the enlargement of the armed forces after the entry of the United States into World War I, the registry system was abandoned, and a tripartite system of classification markings was inaugurated in November 1917 with General Orders No. 64 of the General Headquarters of the American Expeditionary Force.

During World War II, in addition to the President's order and prevailing armed forces directives on marking and handling classified information, the Office of War Information, in September 1942, issued a government-wide regulation on creating and managing classified materials. Among other ad hoc arrangements of the era, personnel cleared to work on the Manhattan Project for the production of the atomic bomb, in committing themselves not to disclose protected information improperly, were "required to read and sign either the Espionage Act or a special secrecy agreement," establishing their awareness of their secrecy obligations and a fiduciary trust which, if breached, constituted a basis for their dismissal.[2]

A few years after the conclusion of World War II, President Harry S. Truman, in February 1950, issued E.O. 10104, which, while superseding E.O. 8381, basically reiterated its text, but added to *Restricted*, *Confidential*, and *Secret* a fourth *Top Secret* classification designation, making American information security categories consistent with those of our allies.[3] At the time of the promulgation of this order, however, plans were underway for a complete overhaul of the classification program, which would result in a dramatic change in policy.

---

[1] 3 C.F.R., 1938-1943 Comp., pp. 634-635.

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

[3] 3 C.F.R., 1949-1953 Comp., pp. 298-299.

E.O. 10290, issued in September 1951, introduced three sweeping innovations in security classification policy.[4] First, the order indicated the Chief Executive was relying upon "the authority vested in me by the Constitution and statutes, and as President of the United States" in issuing the directive. This formula appeared to strengthen the President's discretion to make official secrecy policy: it intertwined his responsibility as Commander in Chief with the constitutional obligation to "take care that the laws be faithfully executed."[5] Second, information was now classified in the interest of "national security," a somewhat new, but nebulous, concept, which, in the view of some, conveyed more latitude for the creation of official secrets. It replaced the heretofore relied upon "national defense" standard for classification. Third, the order extended classification authority to nonmilitary entities throughtout the executive branch, to be exercised by, presumably but not explicitly limited to, those having some role in "national security" policy.

The broad discretion to create official secrets granted by E.O. 10290 engendered widespread criticism from the public and the press. In response, President Dwight D. Eisenhower, shortly after his election to office, instructed Attorney General Herbert Brownell to review the order with a view to revising or rescinding it. The subsequent recommendation was for a new directive, which was issued in November 1953 as E.O. 10501.[6] It withdrew classification authority from 28 entities; limited this discretion in 17 other units to the agency head; returned to the "national defense" standard for applying secrecy; eliminated the "Restricted" category, which was the lowest level of protection; and explicitly defined the remaining three classification areas to prevent their indiscriminate use.[7]

Thereafter, E.O. 10501, with slight amendment, prescribed operative security classification policy and procedure for the next two decades. Successor orders built on this reform. These included E.O. 11652, issued by President Richard M. Nixon in March 1972,[8] followed by E.O. 12065, promulgated by President Jimmy Carter in June 1978.[9] For 30 years, these classification directives narrowed the bases and discretion for assigning official secrecy to executive branch documents and materials. Then, in April 1982, this trend was reversed with E.O. 12356, issued by President

---

[4] Ibid., pp. 789-797.

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

[6] 3 C.F.R., 1949-1953 Comp., pp. 979-986.

[7] U.S. Commission on Government Security, *Report of the Commission on Government Security* (Washington: June 1957), pp. 155-156.

[8] 3 C.F.R., 1971-1975 Comp., pp. 678-690.

[9] 3 C.F.R., 1978 Comp., pp. 190-205.

Ronald Reagan.[10] This order expanded the categories of classifiable information, mandated that information falling within these categories be classified, authorized the reclassification of previously declassified documents, admonished classifiers to err on the side of classification, and eliminated automatic declassification arrangements.[11]

President William Clinton returned security classification policy and procedure to the reform trend of the Eisenhower, Nixon, and Carter Administrations with E.O. 12958 in April 1995.[12] Adding impetus to the development and issuance of the new order were changing world conditions: the democratization of many eastern European countries, the demise of the Soviet Union, and the end of the Cold War. Accountability and cost considerations were also significant influences. In 1985, the temporary Department of Defense (DOD) Security Review Commission, chaired by retired General Richard G. Stilwell, declared that there were "no verifiable figures as to the amount of classified material produced in DOD and in defense industry each year." Nonetheless, it concluded that "too much information appears to be classified and much at higher levels than is warranted."[13] In October 1993, the cost of the security classification program became clearer when the General Accounting Office (GAO) reported that it was "able to identify government-wide costs directly applicable to national security information totaling over $350 million for 1992." After breaking this figure down — it included only $6 million for declassification work — the report added that "the U.S. government also spends additional billions of dollars annually to safeguard information, personnel, and property."[14] E.O. 12958 set limits for the duration of classification, prohibited the reclassification of properly declassified records, authorized government employees to challenge the classification status of records, reestablished the balancing test of E.O. 12065 (weighing the need to protect information vis-a-vis the public interest in its disclosure), and created two review panels — one on classification and declassification actions and one to advise on policy and procedure.

Most recently, in March 2003, President George W. Bush issued E.O. 13292 amending E.O. 12958.[15] Among the changes made by this directive were adding infrastructure vulnerabilities or capabilities, protection services relating to national security, and weapons of mass destruction to the categories of classifiable information; easing the reclassification of declassified records; postponing the automatic declassification of protected records 25 or more years old, beginning in

---

[10] 3 C.F.R., 1982 Comp., pp. 166-178.

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

[12] 3 C.F.R., 1995 Comp., pp. 333-356.

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

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

[15] 3 C.F.R., 2003 Comp., pp. 196-218.

mid-April 2003 to the end of December 2006; eliminating the requirement that agencies prepare plans for declassifying records; and permitting the Director of Central Intelligence to block declassification actions of the Interagency Security Classification Appeals Panel, unless overruled by the President.

The security classification program has evolved over 66 years. One may not agree with all of its rules and requirements, but attention to detail in its policy and procedure result in a significant management regime. The operative presidential directive, as amended, defines its principal terms. Those who are authorized to exercise original classification authority are identified. Exclusive categories of classifiable information are specified, as are the terms of the duration of classification, as well as classification prohibitions and limitations. Classified information is required to be marked appropriately along with the identity of the original classifier, the agency or office of origin, and a date or event for declassification. Authorized holders of classified information who believe that its protected status is improper are "encouraged and expected" to challenge that status through prescribed arrangements. Mandatory declassification reviews are also authorized to determine if protected records merit continued classification at their present level, a lower level, or at all. Unsuccessful classification challenges and mandatory declassification reviews are subject to review by the Interagency Security Classification Appeals Panel. General restrictions on access to classified information are prescribed, as are distribution controls for classified information. The ISOO, within NARA, is mandated to provide central management and oversight of the security classification program. If the director of this entity finds that a violation of the order or its implementing directives has occurred, it must be reported to the head of the agency or to the appropriate senior agency official so that corrective steps, if appropriate, may be taken. In general, very little of this management structure attends information control markings other than *Confidential*, *Secret*, and *Top Secret*.

Control Markings Discovered

In March 1972, a subcommittee of the House Committee on Government Operations — now the House Committee on Government Reform — launched the first oversight hearings on the administration and operation of the Freedom of Information Act (FOIA). Enacted in 1966, the FOI Act had become operative in July 1967. In the early months of 1972, the Nixon Administration was developing new security classification policy and procedure, which would be prescribed in E.O. 11652, issued in early March. The subcommittee's strong interest in this directive was reflected in its unsuccessful attempt to receive testimony from one of the directive's principal architects, David Young, Special Assistant to the National Security Council. The subcommittee sought his testimony as it examined the way in which the new order "will affect the economic and efficient operation of our security classification system, the rationale behind its various provisions, and alternatives to the present approach."[16] Although Young, through White House

---

[16] Letter to David Young, Apr. 24, 1972, appearing in U.S. Congress, House Committee on Government Operations, *U.S. Government Information Policies and Practices — Security*

(continued...)

Counsel John Dean III, declined the invitation to testify, the subcommittee was more successful in obtaining department and agency responses to its August 1971 questionnaire, which, among other questions, asked, "What legend is used by your agency to identify records which are *not* classifiable under Executive Order 10501 [the operative order at the time] but which are not to be made available outside the government?"[17] Of 58 information control markings identified in response to this question, the most common were *For Official Use Only* (11 agencies); *Limited Official Use* (nine agencies); *Official Use Only* (eight agencies); *Restricted Data* (five agencies); *Administratively Restricted* (four agencies); *Formerly Restricted Data* (four agencies); and *Nodis*, or no dissemination (four agencies). Seven other markings were used by two agencies in each case.[18] A CRS review of the agency responses to the control markings question prompted the following observation:

> Often no authority is cited for the establishment or origin of these labels; even when some reference is provided it is a handbook, manual, administrative order, or a circular but not statutory authority. Exceptions to this are the Atomic Energy Commission, the Defense Department and the Arms Control and Disarmament Agency. These agencies cite the Atomic Energy Act, N.A.T.O. related laws, and international agreements as a basis for certain additional labels. The Arms Control and Disarmament Agency acknowledged it honored and adopted State and Defense Department labels.[19]

At a May 1, 1972, hearing on the relationship of the FOI Act to the security classification system, Chairman William S. Moorhead of the Foreign Operations and Government Information Subcommittee (Committee on Government Operations) wondered aloud how the act's nine exemptions to the rule of disclosure could be expanded to the multiple information control markings which the departments and agencies had indicated they were using.[20] The following day, when the hearing continued, William D. Blair, Jr., Deputy Assistant Secretary for Public Affairs at the Department of State, explained that some information control markings were used to route otherwise classified information to a limited group of recipients, "those people who have responsibility for the subject matter concerned." He then addressed the relationship question raised by Chairman Moorhead, saying:

> But if a question came in under the Freedom of Information Act or from the Congress or other representative of the public for that given document, the fact that it is marked, let's say, NODIS, is not relevant. What is relevant to the making available of that document to the public is whether or not it was properly

---

[16] (...continued)
Classification Problems Involving Subsection (b)(1) of the Freedom of Information Act (Part 7), hearings, 92nd Cong., 2nd sess. (Washington: GPO, 1972), pp. 2452-2453.

[17] U.S. Congress, House Committee on Government Operations, *U.S. Government Information Policies and Practices — Security Classification Problems Involving Subsection (b)(1) of the Freedom of Information Act (Part 7)*, hearings, 92nd Cong., 2nd sess. (Washington: GPO, 1972), p. 2930 (emphasis in original).

[18] See ibid., pp. 2933-2934.

[19] Ibid., p. 2932.

[20] Ibid., p. 2284.

> classified under the Executive order and whether or not the Freedom of Information Act, for example, once we have reviewed the document, still pertains, whether we feel that the need for the classification still pertains and whether, in fact, we are authorized under the act to withhold it.[21]

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

> "Limited official use" is not a fixed distribution channel, such as some of these other terms you have mentioned. It simply is an administrative red flag put on that document which means that the document should be given the same degree of protection, physical protection as a classified document even though it is not, under the Executive order, classifiable.[22]

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

> Not necessarily sir. That may be the case. For instance, one set of files on which we use "Limited official use" quite commonly is personnel files. Well, we would be very likely to deny those personnel files if they were requested by a member of the public, on quite different grounds from classification — on grounds of invasion of privacy. But on the other hand we may use a term like "Limited official use" on an internal advisory document which we may be authorized under the Freedom of Information Act to withhold if it were requested; but we might decide not to claim that authority.[23]

Although an attempt was made to obtain further explanation of how information control markings were used, the questioner, a subcommittee staff member, concluded "that all you have convinced me of is to reinforce my belief that a distribution marking is merely a more restrictive or stricter type of classification marking."[24]

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

> In the first place, you have a determination as to whether the material is to be classified. Once the decision is made that the information should be classified, then the limitation of access has to do with the protection of that which is classified. We also have the responsibility to control the dissemination. That is what these access limitations are for, to control dissemination, to confine access

---

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

[22] Ibid., p. 2478.

[23] Ibid.

[24] Ibid., p. 2479.

> to the people who have a need to know to work with the information. It is a protection device. We must use protective devices of some sort.[25]

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

> I presume you wouldn't find "eyes only" in an authorized way upon any document that was not classified by one of the classifiers. Once it is classified you can use limitations on distribution to protect it. That is a protective device.[26]

To this response, Blair added:

> The purpose of classification is to determine what information is or is not available to the public outside of the government. These labels that you are referring to have nothing to do with that. They have absolutely no value for determining what information or what document may be given to a member of the public. They are simply a mailing device, if you like, a means by which a superior determines which of his subordinates he wishes to deal with this particular matter and be aware of this particular information.[27]

These explanations of information control markings being used as devices to limit the distribution of classified information within DOD and the State Department, however, did not appear to extend to all such markings. Blair, for instance, had testified that the *Limited official use* marking was applied, in his words, "quite commonly" to personnel files, which, for the most part, were not security classifiable materials at that time. Several entities indicating they used information control markings had no original classification authority. These included, among others, the American Revolution Bicentennial Commission (ARBC), the Department of Housing and Urban Development, and the Federal Trade Commission (FTC).[28] Does this situation mean that the control markings of these entities were applied only to limit the distribution of classified information received from other agencies? That is possible, but seems unlikely. The ARBC control marking, *Administratively confidential*, appears to have been designed for information of a different character from national security classified materials, while the FTC label, *For staff use only*, does not appear to have provided much limitation on the distribution of classified information.

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

---

[25] Ibid., p. 2497.

[26] Ibid.

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

[28] See ibid., p. 2935.

> Can you assure us today that these kinds of distribution access stamps will not be used on unclassified material in any Executive agency or department? If you can guarantee that, then I will go along and say [Section] 4(a) is a big improvement. But I do not think that is going to be the case from other testimony we have had. I think people are going to substitute LIMDIS, NODIS, and all these other stamps for the stamps authorized under the Executive order and we are going to proliferate more and more and more.[29]

Erickson offered a two part response:

> First, it is our hope within the Department of Justice and I think in other agencies, too, that the use of this sort of a restricted distribution will be severely limited or removed. But, more importantly, it [Section 4(a)] specifically limits the use of such designations to the point where they must conform with the provision of this order and would have no effect in terms of classification. It will not prevent the information from otherwise being made available. It may in part restrict the distribution within the department but certainly if a request were made under the Freedom of Information Act it has no applicability.[30]

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

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

> One of the difficult problems related to the effective operation of the security classification system has been the widespread use of dozens of special access, distribution, or control labels, stamps, or markings on both classified and unclassified documents. Such control markings were not specifically authorized in Executive Order 10501, but have been utilized for many years by many executive agencies having classification authority and dozens of other agencies who do not possess such authority. The use of such stamps has, in effect, been legitimized in section 9 of the new Executive Order 11652.[31]

On this matter, the report concluded that, "while there is a clear rationale for the use of such access or control markings, the basic problem is the effect of the proliferation of their use on the effective operation of the classification system. This problem," it continued, "fully explored with executive branch witnesses during the hearings, is one that this committee believes should be carefully monitored by the [newly created] Interagency Classification Review Committee and by department

---

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

[30] Ibid., p. 2706.

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

heads to assure that it does not interfere with the overall effectiveness and integrity of the classification system."[32]

Control Markings Today

That such interference with the security classification program by these types of information control markings — in terms of both their confusion and presumed coequal authority with classification markings — has occurred in the post-9/11 environment may be discerned in a press account. In late January 2005, *GCN Update*, the online, electronic news service of *Government Computer News*, reported that "dozens of classified Homeland Security Department documents" had been accidently made available on a public Internet site for several days due to an apparent security glitch at the Department of Energy. Describing the contents of the compromised materials and reactions to the breach, the account stated the "documents were marked 'for official use only,' the lowest secret-level classification." The documents, of course, were not security classified, because the marking cited is not authorized by E.O. 12958. Interestingly, however, in view of the fact that this misinterpretation appeared in a story to which three reporters contributed, perhaps it reflects, to some extent, the current state of confusion about the origin and status of various new information control markings which have appeared of late.[33] In some instances, the phraseology of the markings is new, and, in at least one case, the asserted authority for the label is, unlike most of those of the past, statutory. Among the problems they generate, however, the one identified over three decades ago by the House Committee on Government Operations endures.

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

> The status of sensitive information outside of the present classification system is murkier than ever.... "Sensitive but unclassified" data is increasingly defined by the eye of the beholder. Lacking in definition, it is correspondingly lacking in policies and procedures for protecting (or not protecting) it, and regarding how and by whom it is generated and used.[34]

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

> The process for classifying secret information in the federal government is disciplined and explicit. The same cannot be said for unclassified but security-related information for which there is no usable definition, no common

---

[32] Ibid., p. 78.

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

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

> understanding about how to control it, no agreement on what significance it has for U.S. national security, and no means for adjudicating concerns regarding appropriate levels of protection.[35]

Concerning the current *Sensitive But Unclassified* (SBU) marking, a 2004 report by the Federal Research Division of the Library of Congress commented that guidelines for its use are needed, and noted that "a uniform legal definition or set of procedures applicable to all Federal government agencies does not now exist." Indeed, the report indicates that SBU has been utilized in different contexts with little precision as to its scope or meaning, and, to add a bit of chaos to an already confusing situation, it is "often referred to as Sensitive Homeland Security Information."[36]

Assessments of the variety, management, and impact of information control markings, other than those prescribed for the classification of national security information, have been conducted by CRS, GAO, and the National Security Archive, a private-sector research and resource center located at The George Washington University. In March 2006, GAO indicated that, in a recent survey, 26 federal agencies reported using 56 different information control markings to protect sensitive information other than classified national security material.[37] That same month, the National Security Archive offered that, of 37 agencies surveyed, 24 used 28 control markings based on internal policies, procedures, or practices, and eight used 10 markings based on statutory authority.[38] These numbers are important in terms of the variety of such markings. GAO explained this dimension of the management problem:

> [T]here are at least 13 agencies that use the designation For Official Use Only [FOUO], but there are at least five different definitions of FOUO. At least seven agencies or agency components use the term Law Enforcement Sensitive (LES), including the U.S. Marshals Service, the Department of Homeland Security (DHS), the Department of Commerce, and the Office of Personnel Management (OPM). These agencies gave differing definitions for the term. While DHS does not formally define the designation, the Department of Commerce defines it to include information pertaining to the protection of senior government officials, and OPM defines it as unclassified information used by law enforcement personnel that requires protection against unauthorized disclosure to protect the

---

[35] James Jay Carafano and David Heyman, "DHS 2.0: Rethinking the Department of Homeland Security," *Heritage Special Report SR-02* (Washington: Dec. 13, 2004), p. 20.

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

[37] U.S. Government Accountability Office, *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism- Related and Sensitive but Unclassified Information*, GAO Report GAO-06-385 (Washington: Mar. 2006), pp. 5, 25.

[38] National Security Archive, *Pseudo-Secrets: A Freedom of Information Act Audit of the U.S. Government's Policies on Sensitive Unclassified Information* (Washington: Mar. 2006), pp. 9-11.

> sources and methods of investigative activity, evidence, and the integrity of pretrial investigative reports.[39]

Apart from the numbers, however, is another aspect of the management problem, which GAO described in the following terms:

> There are no governmentwide policies or procedures that describe the basis on which agencies should use most of these sensitive but unclassified designations, explain what the different designations mean across agencies, or ensure that they will be used consistently from one agency to another. In this absence, each agency determines what designations to apply to the sensitive but unclassified information it develops or shares.[40]

Comparison of Sensitive Security Information (SSI) Policies

To identify some of the management problems and concerns attending current information control markings, the following case study comparison is provided. *Sensitive Security Information* (SSI) refers to a specific category of government information that has been deemed to require protection against unauthorized disclosure. It is both a concept and a control marking used by the Department of Agriculture (USDA), on the one hand, and jointly by the Transportation Security Administration (TSA) of the Department of Homeland Security as well as by the Department of Transportation, on the other hand, but with different underlying authorities, conceptualizations, and management regimes for it.

USDA Marking

Sensitive Security Information (SSI) appears to be a relatively new information concept and control marking for USDA. Other similar designations, however, are also in use within the department. An information security program statement indicates that "USDA refers to unclassified sensitive information as 'Sensitive Security Information' (SSI). Basically," it continues, "it's to be treated the same as 'Sensitive But Unclassified Information' or 'For Official Use Only Information.'"[41] As a USDA website page, this document provides links to a USDA SSI cover sheet and the department's SSI management regulation, both of which are printable, and a brief Power Point presentation designed to assist USDA employees in understanding the SSI concept. Another USDA website page provides more details concerning *For Official Use Only* (FOUO) and similar designations. It states at the

---

[39] U.S. Government Accountability Office, *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism- Related and Sensitive but Unclassified Information*, p. 24.

[40] Ibid., p. 5.

[41] U.S. Department of Agriculture, Personnel and Document Security Division, Office of Procurement and Property Management, "Information Security Program," undated, available at [http://www.usda.gov/da/infosec/sensitive.htm].

outset that FOUO "is a document designation, not a classification," and explains that this term is used by "a number of other federal agencies to identify information or material which, although unclassified, may not be appropriate for public release." Some of these other agencies are identified, as are some agencies which use different, but comparable, designations, which are provided as well. The discussion of FOUO, which relies upon Department of Defense policy and practice, cautions that information so marked "does not mean it is automatically exempt from public release under" the Freedom of Information Act (FOIA), specifies how unclassified documents and materials containing FOUO shall be marked and safeguarded, and warns that "[a]dministrative penalties may be imposed for misuse of FOUO information," as well as criminal penalties, "depending on the actual content of the information (privacy, export control, etc.)."[42]

Sensitive but Unclassified (SBU) information is discussed in Chapter 10, part 2, of the USDA *Cyber Security Manual, Series 3500*, also known as DM3550-02 of February 17, 2005. SBU information is identified, in part, in terms of examples, which include: "Social Security Numbers, Employee Emergency Data, For Official Use Only Documents, For Limited Official Use Documents, Funding/Budget Documents, Grant/Contract Documents, IT [information technology] Security Plans, Formulas/Trade Secrets, Internet Protocol (IP) Addresses, Network Design Diagrams."[43] Thus, another information control designation, *For Limited Official Use*, is identified, and, furthermore, the chapter states that "SBU information also includes Sensitive Security Information (SSI)," but notes, as the examples reflect, "the SBU category contains information that is not security related but is still sensitive in terms of its risk of exposure."[44] Thereafter, the chapter refers to "SBU/SSI." Various procedures for the processing, handling, and storage of SBU/SSI are specified.[45] Among these is a stipulation that access to SBU/SSI "will be provided to employees with a Need-To-Know," a standard long-governing access to security classified information. Furthermore, "when SBU/SSI data must be shared with contractors and entities outside USDA a *Non-Disclosure Agreement Form* ... must be executed ... to preclude possible organizational or personal conflicts of interest."[46] A copy of this agreement is provided at the end of the chapter. It concludes with a specification of various management responsibilities.

---

[42] U.S. Department of Agriculture, Personnel and Document Security Division, Office of Procurement and Property Management, "For Official Use Only (FOUO) and Similar Designations," undated, available at [http://www.usda.gov/da/ocpm/Security%20Guide/S2unclas/Fouo.htm].

[43] U.S. Department of Agriculture, Office of the Chief Information Officer, *USDA Cyber Security Manual, Series 3500*, Chapter 10, part 2 (DM3550-002), Feb. 17, 2005, p. 8, chapters separately dated and available at [http://www.ocio.usda.gov/directives/index.html].

[44] Ibid., p. 1.

[45] Ibid., pp. 3-4.

[46] Ibid., p. 4 (emphasis in original).

USDA Management

The control and protection of *Sensitive Security Information* (SSI) is discussed in USDA Departmental Regulation 3440-002 of January 30, 2003.[47] The regulation specifies that the "USDA will withhold from release sensitive information that is not appropriate for public disclosure consistent with laws, regulations and court decisions," but also stresses that, "if USDA originates documents that it believes should be classified, Departmental Administration (DA) should be notified as soon as possible." As noted earlier, the Secretary of Agriculture was presidentially authorized to classify information originally as *Secret* (but not *Top Secret*) in September 2002. The regulation also proffers the following proscription: "Information must not be designated as Sensitive Security Information (SSI) to conceal violations of law; inefficiency; administrative error; prevent embarrassment to a person, organization, department or agency; or restrain competition." This ban is similar to one prescribed for security classification.[48]

The regulation provides a lengthy definition of SSI, set out below:

> Sensitive Security Information means unclassified information of a sensitive nature, that if publicly disclosed could be expected to have a harmful impact on the security of Federal operations or assets, the public health or safety of the citizens of the United States or its residents, or the nation's long-term economic prosperity; and which describes, discusses, or reflects:
>
> 1. The ability of any element of the critical infrastructure of the United States [also defined in the regulation] to resist intrusion, interference, compromise, theft, or incapacitation by either physical or computer-based attack or other similar conduct that violates Federal, State, or local law; harms interstate, international commerce of the United States; or threatens public health or safety;
> 2. Any current viable assessment, projection, or estimate of the security vulnerability of any element of the critical infrastructure of the United States, specifically including, but not limited to vulnerability assessment, security testing, risk evaluation, risk-management planning, or risk audit; [and]
> 3. Any currently applicable operational problem or solution regarding the security of any element of the critical infrastructure of the United States, specifically including but not limited to the repair, recovery, redesign, reconstruction, relocation, insurance, and continuity of operations of any element.

---

[47] U.S. Department of Agriculture, *Control and Protection of "Sensitive Security Information,"* Departmental Regulation 3440-002, Jan. 30, 2003, available at [http://www.ocio.usda.gov/directives/doc/DR3440-002.htm].

[48] Section 1.7 of E.O. 12958, as amended, states, in part: "(a) In no case shall information be classified in order to: (1) conceal violations of law, inefficiency, or administrative error; (2) prevent embarrassment to a person, organization, or agency; (3) restrain competition; or (4) prevent or delay the release of information that does not require protection in the interest of the national security. (b) Basic scientific research information not clearly related to the national security shall not be classified."

As a fourth item in the above quoted definition of SSI, the regulation provides the following categories "for illustration purposes only as examples of the types of information (regardless of format) that may be categorized as SSI."

1. Physical security status of USDA laboratories, research centers, field facilities, etc., which may also contain vulnerabilities;
2. Investigative and analytical materials concerning information about physical security at USDA facilities such as the above-named facilities;
3. Information that could result in physical risk to individuals;
4. Information that could result in serious damage to critical facilities and/or infrastructures; [and]
5. Cyber Security information, which includes, but is not limited to
    a. Network Drawings or Plans
    b. Program and System Security Plans
    c. Mission Critical and Sensitive Information Technology (IT) Systems and Applications
    d. Capital Planning and Investment Control Data (I-TIPS)
    e. IT Configuration Management Data and Libraries
    f. IT Restricted Space (Drawings, Plans and Equipment Specifications as well as actual space)
    g. Incident and Vulnerability Reports
    h. Risk Assessment Reports, Checklists, Trusted Facilities Manual and Security Users Guide [and]
    i. Cyber Security Policy Guidance and Manual Chapters

Specific responsibilities are prescribed for senior USDA officials, heads of department organizations, the Office of the Chief Information Officer, and the Office of the General Counsel. Among the responsibilities specified for USDA agencies and staff offices are the following:

- Ensure that adequate security measures and procedures are implemented to protect SSI.
- Ensure that employees of their organization are aware of their responsibility to protect SSI.
- Determine the potential harm resulting from the loss, misuse, or unauthorized access to or modification of SSI in their custody.
- Ensure that prompt and appropriate disciplinary action is taken against personnel responsible for unauthorized disclosure of SSI.

Regarding FOIA requests for access to SSI, the regulation instructs that these should be processed "in accordance with USDA regulations and the Attorney General's FOIA Memorandum of October 12, 2001," which is appended to the regulation, "with consideration of all applicable FOIA exemptions, including" four identified as "Potentially Applicable to SSI."

The departmental regulation does not cite any statutory authority for its issuance.

TSA/DOT Marking

Originally established within the Department of Transportation (DOT) by the Aviation and Transportation Security Act (ATSA) of 2001,[49] the Transportation Security Administration (TSA) was subsequently transferred to the newly created Department of Homeland Security (DHS) by the Homeland Security Act of 2002.[50] The ATSA was signed into law two months after the September 11 terrorist attacks on the World Trade Center and the Pentagon. Shortly thereafter, in a February 15, 2002, notice, DOT announced that TSA was assuming civil aviation security functions and responsibilities as provided by the ATSA, as well as those being transferred which had previously been performed by the Federal Aviation Administration (FAA), another DOT subunit.[51] A week later, DOT issued in final form, without prior notice or opportunity for public comment, new civil aviation security rules.[52] These rules were prompted by the enactment of the ATSA and the assumption of FAA civil aviation security functions and responsibilities by the TSA. Among them was a new part 1520 of Title 49 of the *Code of Federal Regulations* concerning the protection of "Sensitive Security Information." This new concept, it was explained, "includes information about security programs, vulnerability assessments, technical specifications of certain screening equipment and objects used to test screening equipment, and other information."[53] A little over two years later, however, these rules were superseded.

TSA/DOT Management

On May 18, 2004, DOT and DHS jointly published, as an interim, final rule with request for comments, revised regulations concerning the protection of SSI. In the summary, it was noted that "TSA is revising its regulation governing the protection of sensitive security information (SSI) in order to protect the confidentiality of maritime security measures adopted under the U.S. Coast Guard's regulations, published on October 22, 2003, implementing the Maritime Transportation Security Act (MTSA) and other activities related to port and maritime security." It was further explained that, "with this revision to the regulations, TSA is requiring employees, contractors, grantees, and agents of DHS and DOT to follow the same requirements governing protection of SSI as those in the transportation sector who are subject to the regulation."[54] The interim rule was issued as 49 C.F.R. Part 15 for the Office of the Secretary of Transportation and as 49 C.F.R. Part 1520 for the TSA.

In the review of the statutory and regulatory background to the rule, the observation was proffered that, "situations in which information constitutes both SSI

---

[49] 115 Stat. 597.

[50] 116 Stat. 2135 at 2185.

[51] *Federal Register*, vol. 67, Feb. 20, 2002, pp. 7939-7940.

[52] Ibid., Feb. 22, 2002, pp. 8340-8384.

[53] Ibid., p. 8342.

[54] Ibid., vol. 69, May 18, 2004, p. 28066.

and CII," the latter being another type of data known as critical infrastructure information, "may be limited." Pursuant to the Critical Infrastructure Information (CII) Act, a subtitle of the Homeland Security Act,[55] CII, it was explained, "is voluntarily submitted by the private sector to the Federal Government" and the statute "generally prohibits Federal agencies from disclosing such information, except within the Federal Government and to State and local governments in order to protect critical infrastructure." The following comparison was then offered:

> information constituting SSI generally is not voluntarily submitted to the government, which is required for the CII designation. In addition, SSI relates to both critical and noncritical infrastructure assets. There may be cases, however, where the owner or operator of a critical transportation asset voluntarily submits information, such as a vulnerability assessment, to TSA or the Coast Guard. If that information were to be designated by DHS as CII, it would be governed by the requirements of handling of CII, rather than by the SSI regulation.
>
> Another key difference between SSI and CII is the extent to which a Federal employee may disclose such information. Under the SSI regulation, TSA may disclose SSI to persons with a need to know in order to ensure transportation security. This includes persons both within and outside the Federal Government. The CII Act, however, generally prohibits disclosure of properly designated CII outside the Federal Government. Thus, the interim final rule clarifies that in cases where information is both SSI and CII, the receipt, maintenance, or disclosure of such information by a Federal agency or employee is governed by the CII Act and any implementing regulations, by not the interim final rule.[56]

The interim final rule was composed of 10 subsections. The first of these pertained to the scope of the part, explaining it "does not apply to the maintenance, safeguarding, or disclosure of classified national security information," and the second defined terms used in the part.[57] The third subsection explained what constituted SSI in the following terms:

> (a) *In general....* SSI is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which ... would —
>
> (1) Constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file);
>
> (2) reveal trade secrets or privileged or confidential information obtained from any person; or
>
> (3) Be detrimental to transportation safety.
>
> (b) *Information constituting SSI.* Except as otherwise provided in writing ... in the interest of public safety or in furtherance of transportation security, the following information, and records containing such information, constitute SSI:
>
> (1) *Security programs and contingency plans.* Any security program or security contingency plan issued, established, required, received, or approved by DOT or DHS, including —

---

[55] See 116 Stat. 2150.

[56] *Federal Register*, vol. 69, May 18, 2004, p. 28069.

[57] Ibid., pp. 28078, 28082.

(i) Any aircraft operator or airport operator security program or security contingency plan under this chapter;

(ii) Any vessel, maritime facility, or port area security plan required or directed under Federal law;

(iii) Any national or area security plan prepared under 46 U.S.C. 70103; and

(iv) Any security incident response plan established under 46 U.S.C. 70104.

(2) *Security Directives.* Any Security Directive or order —

(i) Issued by TSA under 49 CFR 1542.303, 1544.305, or other authority;

(ii) Issued by the Coast Guard under the Maritime Transportation Security Act, 33 CFR part 6, or 33 U.S.C. 1221 *et seq.* Related to maritime security; or

(iii) Any comments, instructions, and implementing guidance pertaining thereto.

(3) *Information Circulars.* Any notice issued by DHS or DOT regarding a threat to aviation or maritime transportation, including any —

(i) Information Circular issued by TSA under 49 CFR 1542.303 or 1544.305, or other authority; and

(ii) Navigation or Vessel Inspection Circular issued by the Coast Guard related to maritime security.

(4) *Performance specifications.* Any performance specification and any description of a test object or test procedure, for —

(i) Any device used by the Federal government or any other person pursuant to any aviation or maritime transportation security requirement of Federal law for the detection of any weapon, explosive, incendiary, or destructive device or substance; and

(ii) Any communications equipment used by the Federal government or any other person in carrying out or complying with any aviation or maritime transportation security requirements of Federal law.

(5) *Vulnerability assessments.* Any vulnerability assessment directed, created, held, funded, or approved by the DOT, DHS, or that will be provided to DOT or DHS in support of a Federal security program.

(6) *Security inspection or investigative information.* (i) Details of any security inspection or investigation of an alleged violation of aviation or maritime transportation security requirements of Federal law that could reveal a security vulnerability, including the identity of the Federal special agent or other Federal employee who conducted the inspection or audit.

(ii) In the case of inspections or investigations performed by TSA, this includes the following information as to events that occurred within 12 months of the date of release of the information: the name of the airport where a violation occurred, the airport identifier in the case number, a description of the violation, the regulation allegedly violated, and the identity of any aircraft operator in connection with specific locations or specific security procedures. Such information will be released after the relevant 12-month period, except that TSA will not release the specific gate or other location on an airport where an event occurred, regardless of the amount of time that has passed since its occurrence. During the period within 12 months of the date of release of the information, TSA may release summaries of an aircraft operator's, but not an airport operator's, total security violations in a specified time range without identifying specific violations or locations. Summaries may include total enforcement actions, total proposed civil penalty amounts, number of cases opened, number of cases referred to TSA or FAA counsel for legal enforcement action, and number of cases closed.

(7) *Threat information.* Information held by the Federal government concerning threats against transportation or transportation systems and sources

and methods used to gather or develop threat information, including threats against cyber infrastructure.

(8) *Security measures.* Specific details of aviation or maritime transportation security measures, both operational and technical, whether applied directly by the Federal government or another person, including —

(i) Security measures or protocols recommended by the Federal government;

(ii) Information concerning the deployments, numbers, and operations of Coast Guard personnel engaged in maritime security duties and Federal Air Marshals, to the extent it is not classified national security information; and

(iii) Information concerning the deployments and operations of Federal Flight Deck Officers, and number of Federal Flight Deck Officers aggregated by aircraft operator.

(9) Security screening information. The following information concerning security screening under aviation or maritime transportation security requirements of Federal law:

(i) Any procedures, including selection criteria and any comments, instructions, and implementing guidance pertaining thereto, for screening of persons, accessible property, checked baggage, U.S. mail, stores, and cargo, that is conducted by the Federal government or any other authorized person.

(ii) Information and sources of information used by a passenger or property screening program or system, including an automated screening system.

(iii) Detailed information about the locations at which particular screening methods or equipment are used, only if determined by TSA to be SSI.

(iv) Any security screener test and scores of such tests.

(v) Performance or testing data from security equipment or screening systems.

(vi) Any electronic image shown on any screening equipment monitor, including threat images and descriptions of threat images for threat image projection systems.

(10) *Security training materials.* Records created or obtained for the purpose of training persons employed by, contracted with, or acting for the Federal government or another person to carry out any aviation or maritime transportation security measures required or recommended by DHS or DOT.

(11) *Identifying information of certain transportation security personnel.*

(i) Lists of the names of or other identifying information that identify persons as —

(A) Having unescorted access to a secure area of an airport or a secure or restricted area of a maritime facility, port area, or vessel; or

(B) Holding a position as a security screener employed by or under contract with the Federal government pursuant to aviation or maritime transportation security requirements of Federal law, where such lists are aggregated by airport;

(C) Holding a position with the Coast Guard responsible for conducting vulnerability assessments, security boardings, or engaged in operations to enforce maritime security requirements or conduct force protection;

(D) Holding a position as a Federal Air Marshal; or

(ii) The name or other identifying information that identifies a person as a current, former, or applicant for Federal Flight Deck Officer.

(12) *Critical aviation or maritime infrastructure asset information.* Any list identifying systems or assets, whether physical or virtual, so vital to the aviation or maritime transportation system that the incapacity or destruction of such assets would have a debilitating impact on transportation security, if the list is —

(i) Prepared by DHS or DOT; or

(ii) Prepared by a State or local government agency and submitted by the agency to DHS or DOT.

(13) *Systems security information.* Any information involving the security of operational or administrative data systems operated by the Federal government that have been identified by the DOT or DHS as critical to aviation or maritime transportation safety or security, including automated information security procedures and systems, security inspections, and vulnerability information concerning those systems.

(14) *Confidential business information.* (i) Solicited or unsolicited proposals received by DHS or DOT, and negotiations arising therefrom, to perform work pursuant to a grant, contract, cooperative agreement, or other transaction, but only to the extent that the subject matter of the proposal relates to aviation or maritime transportation security measures;

(ii) Trade secret information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out aviation or maritime transportation security responsibilities; and

(iii) Commercial or financial information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out aviation or maritime transportation security responsibilities, but only if the source of the information does not customarily disclose it to the public.

(15) *Research and development.* Information obtained or developed in the conduct of research related to aviation or maritime transportation security activities, where such research is approved, accepted, funded, recommended, or directed by the DHS or DOT, including research results.

(16) *Other information.* Any information not otherwise described in this section that TSA determines is SS under 49 U.S.C. 114(s) or that the Secretary of DOT determines is SSI under 49 U.S.C. 40119. Upon the request of another Federal agency, the Secretary of DOT may designate as SSI information not otherwise described in this section.[58]

The fourth subsection generically identified persons subject to the requirements of the part, and restrictions on the disclosure of SSI by these "covered persons" were prescribed in the fifth subsection. These included taking "reasonable steps to safeguard SSI in that person's possession or control from unauthorized disclosure," and, when not in physical possession of SSI, storing it in "a secure container, such as a locked desk or file cabinet, or in a locked room." Unless otherwise authorized in writing, SSI could be disclosed "only to covered persons who have a need to know," who were described in the sixth subsection. "If a covered person receives a record containing SSI that is not marked," he or she must so mark the material and inform the sender of the need to so identify SSI. Furthermore, when a covered person "becomes aware that SSI has been released to unauthorized persons," he or she "must promptly inform TSA or the applicable DOT or DHS component or agency."[59]

The seventh subsection pertained to marking records containing SSI, including the front and back covers, the title page, and each page of the document with the

---

[58] Ibid., pp. 28079-28080, 28082-28084.

[59] Ibid., pp. 28080-28081, 28084.

Sensitive Security Information label. A distribution limitation statement was also prescribed for inclusion with the marked record.[60]

SSI disclosure was discussed in the eighth subsection. Pursuant to "a proper Freedom of Information Act or Privacy Act request," a responsive record may be disclosed "with the SSI redacted, provided the record is not otherwise exempt from disclosure" under other provisions of these laws. The part did not preclude the disclosure of SSI "to a committee of Congress authorized to have the information or to the Comptroller General, or to any authorized representative of the Comptroller General." Discretionary allowance was made for the disclosure of SSI in an administrative enforcement proceeding, but provision was made for requiring a security background check for parties to the proceedings to whom SSI would be disclosed.[61]

The ninth subsection indicated that violation of the part "is grounds for a civil penalty and other enforcement or corrective action ..., and appropriate personnel actions for Federal employees." The subsection continued, saying: "Corrective action may include issuance of an order requiring retrieval of SSI to remedy unauthorized disclosure or an order to cease future unauthorized disclosure."[62]

Finally, the 10th subsection, while acknowledging Federal Records Act requirements to preserve records containing documentation of a federal agency's policies, decisions, and essential transactions, authorized the destruction of SSI when it is no longer needed to carry out agency functions. "A covered person," according to the subsection, "must destroy SSI completely to preclude recognition or reconstruction of the information when the covered person no longer needs the SSI to carry out transportation security measures," but this provision "does not require a State or local government agency to destroy information that the agency is required to preserve under State or local law."[63]

As produced in the 2004 edition of Title 49, *Code of Federal Regulations*, Part 15 cited one statutory provision as authority for its issuance: 49 U.S.C. 40119, directing the conduct of research and development activities to develop, modify, test, and evaluate a system, procedures, facility, or device to protect passengers and property against acts of criminal violence and piracy in transportation. Part 1520, however, cited several statutory provisions in this regard:

- 46 U.S.C. §§ 70102-70106, basically deriving from the MTSA, and authorizing United States facility and vessel vulnerability assessments, a national maritime transportation security plan, security incident response plans for vessels and facilities that may be involved in a transportation security incident, the issuance of

---

[60] Ibid., pp. 28081, 28085.

[61] Ibid., pp. 28081, 28085.

[62] Ibid., pp. 28082, 28085.

[63] Ibid.

transportation security cards, and the establishment of maritime safety and security teams.[64]

- 46 U.S.C. § 70117, basically deriving from the MTSA, and establishing a civil penalty for violations of the port security chapter or any regulation issued pursuant to it.[65]

- 49 U.S.C. § 114, basically deriving from the ATSA and mandating the TSA and the related DOT Transportation Security Oversight Board,[66] and which was subsequently amended by the Homeland Security Act to authorize (with the addition of Subsection 114(s)) the prescribing of "regulations prohibiting the disclosure of information obtained or developed in carrying out security under authority of" the ATSA "if the Under Secretary decides that disclosing the information would (A) be an unwarranted invasion of personal privacy; (B) reveal a trade secret or privileged or confidential commercial or financial information; or (C) be detrimental to the security of transportation."[67]

- 49 U.S.C. § 40113, prescribing general authority for the Secretary of Transportation, Under Secretary of Transportation for Security, or Administrator of the FAA, as appropriate, to take necessary action to carry out this part, including conducting investigations, prescribing regulations, standards, and procedures, and issuing orders.

- 49 U.S.C. §§ 44901-44907, prescribing security requirements for the Administrator of the FAA to prescribe regulations concerning the screening of passengers and property, the conditions for refusal of transport by intrastate and foreign air carriers, and the protection of passengers and property on an aircraft operating in air transportation or intrastate air transportation against an act of criminal violence or aircraft piracy; to assess, in conjunction with the Director of the FBI, current and potential threats to the domestic air transportation system; and to not approve a security program of a foreign air carrier unless it requires the foreign air carrier, in its operations to and from airports in the United States, to adhere to the identical security measures that the Administrator requires air carriers serving the same airports to adhere to. These provisions also require, under guidelines prescribed by the Secretary of Transportation, that an air carrier, airport operator, ticket agent, or an individual employed by same, receiving information about a threat to civil aviation provide that information promptly to the Secretary; and direct the Secretary,

---

[64] See 116 Stat. 2064 at 2068-2075.

[65] 116 Stat. 2084.

[66] 115 Stat. 597.

[67] 116 Stat. 2135 at 2312.

at intervals considered necessary, to assess the effectiveness of the security measures at foreign airports served by an air carrier from which a foreign air carrier serves the United States or that poses a high risk of introducing danger to international air travel, as well as other airports the Secretary considers appropriate.

- 49 U.S.C. §§ 44913-44914, concerning the deployment and purchase of explosives detection equipment and the development of airport construction guidelines.

- 49 U.S.C. §§ 44916-44918, directing the Administrator of the FAA to require each air carrier and airport that provides for intrastate, interstate, or foreign air transport to conduct periodic vulnerability assessments of the security systems of that air carrier or airport, to perform periodic audits of such assessments, and to conduct periodic and unannounced inspections of security systems of airports and air carriers to determine the effectiveness and vulnerabilities of such systems;[68] authorizing the Under Secretary for Transportation Security to deploy and otherwise provide for the training, supervision, equipping, and air carrier accommodation of federal air marshals; and authorizing the development of detailed guidance for a scheduled passenger air carrier flight and cabin crew training program to prepare crew members for potential threat conditions.[69]

- 49 U.S.C. §§ 44935-44936, directing the Administrator of the FAA to prescribe standards for the employment and continued employment of, and contracting for, air carrier personnel and airport security personnel, as well as requiring by regulation employment investigations, including criminal history record checks, for individuals employed in, or applying for, positions in airport operations and security.

- 49 U.S.C. § 44942, authorizing the Under Secretary for Transportation Security to establish performance goals and objectives for aviation security.

- 49 U.S.C. § 46105, concerning the effectiveness of prescribed regulations and orders of the Secretary of Transportation, Under Secretary for Transportation Security, and Administrator of the FAA regarding security duties and powers, as well as the amendment, modification, suspension, or superseding of such issuances.

This represents a slight increase in statutory authority cited in support of Part 1520 as it appears in the 2004 *Code of Federal Regulations* when compared with the version appearing in the 2002 edition.

---

[68] Added by 110 Stat. 3253.

[69] Added by 115 Stat. 606 and 610.

Management Regime Comparison

Presidentially prescribed arrangements for the management of classified national security information have been operative for over half a century. The initial directive in this regard, as noted earlier, was issued in March 1940, and, thereafter, successor orders largely narrowed the bases and discretion for assigning official secrecy, and increasingly detailed the management regime for security classified materials. In **Table 1** below, various aspects of the current management regime for classified information, as prescribed by E.O. 12958, as amended, are set out in comparison with the SSI management arrangements prescribed by USDA and TSA/DOT.

Table 1. Management of Security Classified Information and SSI Compared

Management Consideration	E.O. 12958, as amended	USDA SSI (Reg. 3440-002)	TSA/DOT SSI (49 CFR 15) (49 CFR 1520)
Principal terms defined	Yes	Yes	Yes
Original users of marking authority specified	Yes	Yes	No - generic covered persons
Delegation of marking authority in writing	Yes	Not clear	No
Exclusive categories of protectable information specified	Yes	Yes	Yes
Duration of marking or protection specified	Yes	Yes	No
Date or event for termination of marking/protection specified	Yes	No	No
Identity of original marker specified	Yes	No	No
Prohibitions and limitations for markings specified	Yes	Yes	No
Authorized challenges on propriety of marking	Yes	No	No
Mandatory reviews to determine continued need for protection	Yes	No	No
Appellate review of unsuccessful challenges or mandatory review outcomes	Yes	No	No
System oversight vested in specified entity or official	Yes	Yes	No

In general, the management regime for SSI prescribed by USDA does not appear to be as detailed as the regime prescribed by E.O. 12958, as amended, for classified national security information. However, the USDA regime for SSI does appear to be more detailed than the one prescribed by TSA for SSI, particularly regarding specification of users of the marking authority, limiting the duration of marking or protection, specifying prohibitions and limitations on the use of marking, and vesting system oversight in Departmental Administration (DA). This comparison is based upon the content of relevant regulations, but does not take into consideration actual implementation or administrative practice regarding those regulations.

In June 2005, the Government Accountability Office (GAO) completed an assessment of TSA management of SSI. Among the results of that assessment are the following comments:

- TSA does not have written policies and procedures, beyond its SSI regulations, providing criteria for determining what constitutes SSI.[70]

- In addition to lacking written guidance concerning SSI designation, TSA has no policies and procedures specifying clear responsibilities for officials who can designate SSI.[71]

- TSA lacks adequate internal controls to provide reasonable assurance that its SSI designation process is being consistently applied across TSA and for monitoring compliance with the regulations governing the SSI designation process, including ongoing monitoring of the process.[72]

- TSA has not developed policies and procedures for providing specialized training for all of its employees making SSI designations on how information is to be identified and evaluated for protected status.[73]

With a view to bringing "clarity, structure, and accountability to TSA's SSI designation process," GAO recommended "that the Secretary of the Department of Homeland Security direct the Administrator of the Transportation Security Administration to take the following four actions":

- establish clear guidance and procedures for using the TSA regulations to determine what constitutes SSI;

- establish clear responsibility for the identification and designation of information that warrants SSI protection;

---

[70] U.S. Government Accountability Office, *Transportation Security Administration: Clear Policies and Oversight Needed for Designation of Sensitive Security Information*, GAO Report GAO-05-677 (Washington: June 2005), p. 3.

[71] Ibid., p. 4.

[72] Ibid., p. 5.

[73] Ibid., p. 6.

- establish internal controls that clearly define responsibility for monitoring compliance with regulations, policies, and procedures governing the SSI designation process and communicate that responsibility throughout TSA; and

- establish policies and procedures within TSA for providing specialized training to those making SSI designations on how information is to be identified and evaluated for protected status.[74]

Implications for Information Sharing

The importance of information sharing for combating terrorism and realizing homeland security was emphasized by the National Commission on Terrorist Attacks Upon the United States.[75] When fashioning the Homeland Security Act of 2002, Congress recognized that the variously identified and marked forms of sensitive but unclassified (SBU) information could be problematic with regard to information sharing. Section 892 of that statute specifically directed the President to prescribe and implement procedures for the sharing of information by relevant federal agencies, including the accommodation of "homeland security information that is sensitive but unclassified."[76]

On July 29, 2003, the President assigned this responsibility largely to the Secretary of Homeland Security.[77] Nothing resulted.

The importance of information sharing was reinforced two years later in the report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction.[78] Congress again responded by mandating the creation of an Information Sharing Environment (ISE) when legislating the Intelligence Reform and Terrorism Prevention Act of 2004.[79] Preparatory to implementing the ISE provisions, the President issued a December 16, 2005, memorandum recognizing the need for standardized procedures for SBU information and directing department and agency officials to take certain actions relative to that objective.[80] In May 2006, the newly appointed manager of the ISE agreed with a

---

[74] Ibid., p. 7.

[75] See U.S. National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington: GPO, 2004), pp. 416-419.

[76] 116 Stat. 2135 at 2253.

[77] E.O. 13311 in 3 C.F.R., 2003 Comp., pp. 245-246.

[78] See U.S. Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States* (Washington: GPO, 2005), pp. 429-450.

[79] 118 Stat. 3638 at 3664.

[80] The White House Office, Memorandum for the Heads of Executive Departments and Agencies, "Guidelines and Requirements in Support of the Information Sharing

(continued...)

March GAO assessment[81] that, oftentimes, SBU information, designated as such with some marking, was not being shared due to concerns about the ability of recipients to protect it adequately.[82] In brief, it appears that pseudo-classification markings have, in some instances, had the effect of deterring information sharing for homeland security purposes.

Improving Classified Information Life Cycle Management

In the current environment, still affected by the long shadow of the terrorist attacks of September 11, 2001, some long-standing difficulties attending the life cycle management of security classified information have become particularly acute. In July 2005, the *New York Times* observed editorially that the "Bush Administration is classifying the documents to be kept secret from public scrutiny at the rate of 125 a minute. The move toward greater secrecy," it continued, "has nearly doubled the number of documents annually hidden from public view — to well more than 15 million last year, nearly twice the number classified in 2001."[83] As the number of classification actions has been largely increasing, the editorial also noted, the volume of declassified material has been decreasing, as the data in **Table 2** below indicate. The situation appears to have slightly improved in 2005. These activities have related costs. Security classification expenses — which include personnel security, physical security, education and training, and management and planning — far exceed expenditures for declassification.

Some relief of the situation may result from the automatic action — declassification, exemption for continued protection, or referral to other agencies — on classified records 25 or more years old mandated by the Clinton executive order and now scheduled to occur by December 31, 2006. Using agencies' supplied information concerning their efforts to meet the deadline, ISOO, as of September 21, 2005, estimated that 155 million pages of classified records were subject to automatic action, and "believes, for the most part, that the Executive branch is progressing toward fulfilling its responsibilities for these records by the deadline." Of 46 agencies affected, "ISOO was confident that 22 of those agencies will be prepared to implement the Automatic Declassification program by the deadline" and will

---

[80] (...continued)
Environment," Dec. 16, 2005, Washington, DC.

[81] U.S. Government Accountability Office, *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism- Related and Sensitive but Unclassified Information*, p. 25.

[82] Prepared statement of Thomas E. McNamara, Program Manager for the Information Sharing Environment, Office of the Director of National Intelligence, before the House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, May 10, 2006, Washington, D.C., pp. 8-9.

[83] Editorial, "The Dangerous Comfort of Secrecy," *New York Times*, July 12, 2005, p. A22.

"work closely with the remaining 24 agencies to ensure that they allocate sufficient resources to meet the requirement."[84]

Table 2. Information Moving In and Out of Classified Status

Fiscal Year	New Classification Actions	Declassified Pages	Classification Cost	Declassification Cost
2001	8,650,735	100,104,990	$4.5 billion	$232 million
2002	11,271,618	44,365,711	$5.5 billion	$113 million
2003	14,228,020	43,093,233	$6.4 billion	$54 million
2004	15,645,237	28,413,690	$7.1 billion	$48 million
2005	14,206,773	29,540,603	$7.7 billion	$57 million
2006	20,556,445	37,647,993	$8.2 billion	$44 million

Source: Data from U.S. National Archives and Records Administration, Information Security Oversight Office, *Report to the President 2001* (Washington: Sept. 2002), pp. 7-8, 16; U.S. National Archives and Records Administration, Information Security Oversight Office, *Report to the President 2002* (Washington: June 2003), pp. 14-15, 26; U.S. National Archives and Records Administration, Information Security Oversight Office, *Report to the President 2003* (Washington: Mar. 2004), pp. 20, 25; U.S. National Archives and Records Administration, Information Security Oversight Office, *Report to the President 2004* (Washington: Mar. 2005), pp. 15, 17; U.S. National Archives and Records Administration, Information Security Oversight Office, *Report to the President 2005* (Washington: May 2006), pp. 13, 15; U.S. National Archives and Records Administration, Information Security Oversight Office, *Report to the President 2006* (Washington: May 2007), pp. 6, 22, 29-30; U.S. National Archives and Records Administration, Information Security Oversight Office, *2003 Report on Cost Estimates for Security Classification Activities* (Washington: July 2004), pp. 2-3; U.S. National Archives and Records Administration, Information Security Oversight Office, *Report on Cost Estimates for Security Classification Activities for 2004* (Washington: May 2005), p. 3; U.S. National Archives and Records Administration, Information Security Oversight Office, *Report on Cost Estimates for Security Classification Activities for 2005* (Washington: 2006), pp. 2, 5.

Whereas the automatic declassification effort is aimed at reducing the quantity of older records which no longer merit protected status or preservation, the Interagency Security Classification Appeals Panel (ISCAP), also created by the Clinton order, is available to address qualitative issues concerning classified information. ISCAP is composed of senior level representatives of the Secretary of State, Secretary of Defense, Attorney General, Director of Central Intelligence, Archivist of the United States, and Assistant to the President for National Security Affairs. The President selects the panel's chair from among its members. The director of the Information Security Oversight Office (ISOO), which is the government-wide overseer of the security classification program, serves as the ISCAP executive secretary. The panel makes final determinations on classification challenges appealed to it by government employees or the public; approves, denies, or amends exemptions from automatic declassification sought by agencies; makes final determinations on mandatory declassification review requests appealed to it;

---

[84] U.S. National Archives and Records Administration, Information Security Oversight Office, *Report to the President 2005* (Washington: May 2006), p. 19.

and generally advises and assists the President in the discharge of his discretionary authority to protect the national security of the United States. The recent review activities of ISCAP are detailed in **Table 3**.

Table 3. ISCAP Decisions

Year	Documents Reviewed	Declassified in Full	Declassified in Part	Affirmed Classification
2001	34	8 (23%)	21 (62%)	5 (15%)
2002	49	9 (18%)	17 (35%)	23 (47%)
2003	106	3 (3%)	80 (75%)	23 (22%)
2004	159	11 (7%)	30 (19%)	118 (74%)
2005	81	21 (26%)	44 (54%)	16 (20%)
2006	675	139 (21%)	294 (43%)	242 (36%)

Source: Data from U.S. National Archives and Records Administration, Information Security Oversight Office, *Report to the President 2001*, p. 5; U.S. National Archives and Records Administration, Information Security Oversight Office, *Report to the President 2002*, p. 9; U.S. National Archives and Records Administration, Information Security Oversight Office, *Report to the President 2003*, p. 9; U.S. National Archives and Records Administration, Information Security Oversight Office, *Report to the President 2004*, p. 7; U.S. National Archives and Records Administration, Information Security Oversight Office, *Report to the President 2005* (Washington: May 2006), p. 5; U.S. National Archives and Records Administration, Information Security Oversight Office, *Report to the President 2006* (Washington: May 2007), p. 6.

Finally, an issue recently arose concerning the selective withdrawal of declassified records from public access at the National Archives and Records Administration (NARA) for reclassification. This activity came to public attention on February 21, 2006, when the National Security Archive, a private sector research and resource center located at The George Washington University, published a report about the discovery on its website.[85] A news account was also simultaneously published in the *New York Times*.[86] Initial reported indications were that, beginning in 1999, intelligence agencies, pursuant to a secret agreement with the National Archives and Records Administration (NARA), began secretly removing declassified records from public access and had reclassified more than 55,000 of them. The effort was apparently an attempt to reverse what some regarded as a hasty compliance with the Automatic Declassification program prescribed in the Clinton order and directed at classified records more than 20 years old. It was discovered, however, that several

---

[85] Matthew M. Aid, *Declassification in Reverse: The U.S. Intelligence Community's Secret Historical Document Reclassification Program*, National Security Archive Report (Washington: Feb. 21, 2006), available at [http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB179/].

[86] Scott Shane, "U.S. Reclassifies Many Documents in Secret Review," *New York Times*, Feb. 21, 2006, pp. A1, A16.

of the reclassified documents had been previously published in the Department of State's history series, *Foreign Relations of the United States*. Other reclassified records were regarded to be rather innocuous, such as a 1948 memorandum on a Central Intelligence Agency (CIA) plan to float balloons over communist countries in Eastern Europe and drop propaganda leaflets; a premature CIA assessment in October 1950 that Chinese intervention in the Korean War was "not probable in 1950," but actually occurred late in that month; and a 1962 telegram from Ambassador to Yugoslavia George F. Kennan containing an English translation of a Belgrade newspaper article on the Chinese nuclear weapons program. The *Times* story indicated that the director of ISOO, after reviewing 16 withdrawn records and concluding that none of them should have been reclassified, had ordered an audit of the reclassification effort.

The results of the ISOO audit were released on April 26, 2006. Agencies conducting the re-reviews of withdrawn records since 1995 included the CIA, the Department of Energy, the Department of the Air Force (USAF), and the Federal Emergency Management Agency. Their efforts "resulted in the withdrawal of at least 23,315 publicly available records; approximately 40 percent were withdrawn because the reviewing agency purported that its classified information had been designated unclassified without its permission and about 60 percent were identified by the reviewing agency for referral to another agency for declassification or other public disclosure review."[87] In reviewing a sample of 1,353 of the withdrawn records, ISOO concluded that 64 percent of them "did, in fact, contain information that clearly met the standards for continued classification," said the audit report. ISOO also found that 24% of the sampled records "were clearly inappropriate for continued classification," and "an additional 12 percent were questionable." Overall, said the audit report, "Depending upon the review effort, the sample of records withdrawn clearly met the standards for continued classification anywhere from 50 percent to 98 percent of the time."[88]

Why did this withdrawal and reclassification of records happen? ISOO offered the following explanation:

> There are a number of contributing factors to the issues identified by this audit. Sufficient quality control and oversight by both the agencies and ISOO has been lacking, as has proper documentation for declassification decisions. In addition, NARA has, at times, acquiesced too readily to the re-review efforts or withdrawal decisions of agencies. Additionally, NARA has not had the necessary resources available to keep pace with agencies' re-review activity, let alone the overall declassification activity of the recent past which has resulted

---

[87] U.S. National Archives and Records Administration, Information Security Oversight Office, *Audit Report: Withdrawal of Records from Public Access at the National Archives and Records Administration for Classification Purposes* (Washington: Apr. 26, 2006), p. 1; also see Christopher Lee, "Some Archives Files Wrongly Kept Secret," *Washington Post*, Apr. 27, 2006, p. A25; Scott Shane, "National Archives Says Records Were Wrongly Classified," *New York Times*, Apr. 27, 2006, p. A24.

[88] U.S. National Archives and Records Administration, Information Security Oversight Office, *Audit Report: Withdrawal of Records from Public Access at the National Archives and Records Administration for Classification Purposes*, p. 1.

in the accumulation of hundreds of millions of previously classified pages which require processing by NARA. The most significant deficiency identified by this audit, however, was the absence of standards, including requisite levels of transparency, governing agency re-review activity at NARA. Absent these, NARA along with CIA and USAF resorted to ad hoc agreements that, in retrospect, all recognize should never have been classified in the first place.[89]

Regarding remedial actions, the audit report offered the following:

As a result of this audit, the affected agencies have agreed to abide by interim guidance that includes provisions that require the public to be informed that records have been formally withdrawn from public access at NARA due to classification action as well as how many records are affected. Prior to official promulgation in regulation, this interim guidance will be fully coordinated, to include an opportunity for public comment. In addition, in response to many of the challenges highlighted by this audit, the principal agencies involved in conducting classification reviews of records accessioned into NARA have agreed, in principle, to create a pilot National Declassification Initiative, in order to more effectively integrate the work they are doing in this area. This initiative will address the policies, procedures, structure, and resources needed to create a more reliable Executive branch-wide declassification program.

* * * * * * * * * *

In response to the findings of this audit, the Director [of ISOO] is writing to all agency heads asking for their personal attention in a number of critical areas, to include facilitating classification challenges and routinely sampling current classified information in order to determine the validity of classification actions. In addition, ISOO will be initiating a number of training efforts in support of these objectives. Finally, agency heads will be requested to provide a status report within 120 days on the action taken with respect to these initiatives as well as with regard to the recommendations contained within this audit report. ISOO will report publicly on these actions.[90]

Remedial Legislation

H.R. 984 (Waxman)

Executive Branch Reform Act of 2007. Among other provisions, Section 7 would require each federal agency, not later than six months after the date of the enactment of the legislation, to submit to the Archivist of the United States and specified congressional committees a report, with certain details, describing their use of "pseudo" classification designations; would require the Archivist, not later than nine months after the date of the enactment of the legislation, to issue to specified congressional committees a report based on the agency submissions, as well as input from the Director of National Intelligence, federal offices, and contractors, with an opportunity for public comment on this report; would require the Archivist, not later

---

[89] Ibid., p. 2.

[90] Ibid.

than 15 months after date of the enactment of the legislation, to promulgate regulations banning the use of "pseudo" classification designations, with standards for exceptions for control markings other than those used for classifying national security information; and would require the Archivist to review existing statutes that allow agencies, offices, and contractors to control, protect, or otherwise withhold information based on security concerns, and make recommendations on potential changes to the statutes so reviewed with a view to improving public access to information governed by them. Introduced February 12, 2007, and referred to the Committee on Oversight and Government Reform.

H.R. 4806 (Harman)

Reducing Over-Classification Act. Requires the Secretary of Homeland Security to develop a strategy that will (1) allow the security classification of records only after unclassified, shareable versions of intelligence have been produced; (2) develop a new "sensitive and shared" information program that will provide protections for certain sensitive and unclassified information for limited periods of time under narrowly tailored circumstances; (3) propose new incentives and disincentives to encourage Department of Homeland Security personnel to classify records properly and to use "sensitive and shared" markings sparingly; (4) create training programs and auditing mechanisms for all department employees in order to ensure that the mandated strategy is being implemented properly; (5) establish an independent department declassification review board to expedite the declassification of records when the need for public access outweighs the need to classify; and (6) propose legislative solutions to ensure that the strategy is implemented in a way that not only promotes security, but also fosters both information sharing and the protection of privacy and other civil rights.[91] Introduced December 18, 2007, and referred to the Committee on Homeland Security.

Related Literature

National Security Archive. *Pseudo-Secrets: A Freedom of Information Act Audit of the U.S. Government's Policies on Sensitive Unclassified Information.* Washington: March 2006. 50 pp.

U.S. Congress. House Committee on Government Reform. Subcommittee on National Security, Emerging Threats, and International Relations. *Emerging Threats: Overclassification and Pseudo-Classification.* Hearing, 109th Congress, 1st Session. March 2, 2005. Washington: GPO, 2005. 205 pp.

U.S. Government Accountability Office. *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information.* GAO Report GAO-06-385. Washington: March 2006. 72 pp.

---

[91] See *Congressional Record*, daily edition, vol. 153, Dec. 19, 2007, p. E2611.

——. *Managing Sensitive Information: Departments of Energy and Defense Policies and Oversight Could Be Improved.* GAO Report GAO-06-369. Washington: March 2006. 23 pp.

——. *Transportation Security Administration: Clear Policies and Oversight Needed for Designation of Sensitive Security Information.* GAO Report GAO-05-677. Washington: June 2005. 57pp.

U.S. Office of the Director of National Intelligence. *Information Sharing Environment Implementation Plan.* Washington: November 2006. 160pp.

CRS Report RL33303. *"Sensitive But Unclassified" Information and Other Controls: Policy and Options for Scientific and Technical Information*, by Genevieve J. Knezo.

——. Federal Research Division. *Laws and Regulations Governing the Protection of Sensitive but Unclassified Information.* By Alice R. Buchalter, John Gibbs, and Marieke Lewis. Washington: September 2004. 28 pp.

U.S. National Archives and Records Administration. Information Security Oversight Office. *Audit Report: Withdrawal of Records from Public Access at the National Archives and Records Administration for Classification Purposes.* Washington: April 26, 2006. 28 pp.

BACKGROUND
GOVERNMENT-WIDE INTELLIGENCE COMMUNITY MANAGEMENT REFORMS
February 29, 2008

Oversight of the Intelligence Community

A. Overview of the IC

The "intelligence community" refers to a statutorily-defined federation of the executive branch agencies and organizations that conduct intelligence activities for the protection of U.S. national security and the conduct of foreign relations.[1]

ODNI oversees and coordinates the intelligence activities of the other members of the IC, which are:

- Central Intelligence Agency (CIA)
- United States Department of Defense (DoD)
  - Office of the Secretary of Defense, Under Secretary of Defense for Intelligence
  - National Security Agency (NSA)
  - National Reconnaissance Office (NRO)
  - National Geospatial-Intelligence Agency (NGA)
  - Defense Intelligence Agency (DIA)
  - Army Military Intelligence
  - Air Force Intelligence
  - Marine Corps Intelligence Activity
  - Office of Naval Intelligence (ONI)
- Department of Homeland Security
  - Office of Intelligence and Analysis
  - Coast Guard Intelligence
- Department of Justice
  - Federal Bureau of Investigation (FBI)
  - Drug Enforcement Administration (DEA), Office of National Security Intelligence
- Department of State, Bureau of Intelligence and Research
- Department of Energy, Office of Intelligence
- Department of the Treasury, Office of Intelligence and Analysis[2]

---

[1] *See* 50 U.S.C. § 401a; Intelligence Community website, www.intelligence.gov/1-definition.shtml.
[2] *See* 50 U.S.C. § 401a(4); Intelligence Community website, http://www.intelligence.gov/1-members.shtml.

B. The Intelligence Reform and Terrorism Prevention Act of 2004

For decades, the elements of the IC acted largely independently, with limited direction by the Director of Central Intelligence.[3] In the years since September 11, 2001, and with the passage of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Public Law 108-458, the IC has undergone extensive restructuring.

IRTPA was the most comprehensive reform of the IC since its establishment.[4] IRTPA created a Director of National Intelligence (DNI) to serve as the head of the intelligence community.[5] IRTPA gave DNI substantially stronger central authorities than the Director of Central Intelligence formerly held, and specified that the Director of National Intelligence could not simultaneously serve as the Director of the CIA.[6]

DNI acts as the principal advisor to the President, the National Security Council, and the Homeland Security Council for intelligence matters related to national security.[7] DNI has broad responsibility for ensuring that timely, objective intelligence is provided to the President, military, heads of executive-branch agencies and departments government-wide, and Congress.[8] In light of this responsibility, IRTPA gave DNI the responsibility to establish objectives, priorities, and guidance for intelligence collection, analysis, and dissemination.[9]

Additionally, IRTPA provides DNI new and enhanced authority for IC budget development and transfers of funds.[10] IRTPA also provides DNI with significant government-wide IC personnel authorities.[11] Finally, IRTPA provides DNI authority over major acquisitions.[12]

---

[3] *See, e.g.*, Statement of J. Mitchell McConnell, Director of National Intelligence, before the Senate Select Committee on Intelligence, February 14, 2008, at 2 (hereinafter "McConnell Statement").

[4] *See, e.g.*, Congressional Research Service, *Intelligence Issues for Congress* (Updated February 11, 2008), Order Code RL33539, at 2.

[5] *See* 50 U.S.C. § 403(a)-(b).

[6] *See* 50 U.S.C. §§ 403, 403-1; Congressional Research Service, *Director of National Intelligence Statutory Authorities: Status and Proposals* (Updated January 24, 2008), Order Code RL34231 (hereinafter "*DNI's Statutory Authorities*"), at Summary & pp. 6-9.

[7] *See* 50 U.S.C. § 403(b).

[8] *See* 50 U.S.C. § 403-1(a).

[9] *See* 50 U.S.C. § 403-1(f).

[10] *See* 50 U.S.C. § 403-1(c)-(e); *DNI's Statutory Authorities*, at pp. 6-7.

[11] *See* 50 U.S.C. § 403-1(e)-(f), (l)-(m); *DNI's Statutory Authorities*, at pp. 7-8.

[12] The Secretary of Defense holds joint authority with the DNI with respect to IC components in DoD. *See* 50 U.S.C. § 403-1(q); *DNI's Statutory Authorities*, at p. 8.

C. Recent and Proposed IC Management Reforms

According to ODNI, in the time since the office was established, it has implemented management reforms across the IC in the following areas:

- Enhanced intelligence collaboration and information sharing within the IC and with other partners.
- Improved security for information technology (IT) networks.
- Instituted a joint duty program to provide incentives to future senior leaders to gain experience in more than one component of the IC.
- Established a National Intelligence University and started joint training of intelligence officers.
- Integrated and coordinated the government-wide IC budget.
- Established a network of civil liberties and privacy officers at all IC components.[13]

In addition, ODNI has proposed to implement a series of community-wide management reforms, including:

- Implementing a common IC performance appraisal system and pay-for-performance compensation system.
- Improving IC-wide equal opportunity and diversity program.
- Further modernizing information sharing policies and procedures and creating the "Single Information Environment," an integrated information environment for the IC, and "A-Space" a collaborative IT workspace.
- Reforming and streamlining acquisition processes.
- Implement security clearance reforms intended to save time and money.
- Modernize the community's business practices, including improving budget planning, performance management, and financial systems.
- Formalizing an IC-wide framework for policy guidance, training, and best practices to protect privacy and civil liberties through the network of civil liberties and privacy officers.[14]

The Fiscal Year 2008 Intelligence Authorization Act (H.R. 2082) would provide additional flexibility to the DNI's personnel authorities. The conference report passed by both the House and Senate would grant the DNI authority to provide higher pay for critical positions and prohibits the implementation of pay-for-performance compensation

---

[13] *See* McConnell Statement at pp. 6-7; Statement of Donald Kerr, Principal Deputy Director of National Intelligence, before the House Permanent Select Committee on Intelligence, December 6, 2007 (hereinafter "Kerr Statement"), at pp. 5-10.

[14] *See* McConnell Statement at pp. 7-10; Kerr Statement at pp. 5-16; Statement of Ronald Sanders, Associate Director of National Intelligence for Human Capital, before the Subcommittee on the Federal Workforce, Postal Service, and the District of Columbia of the House Committee on Oversight and Government Reform, February 12, 2008.

reform within any element of the IC until 45 days after the DNI submits to the Congress a detailed plan for the implementation of the compensation plan at the element of the IC in question. The President has indicated that he will veto the bill, however his decision is not based on the personnel provisions, but rather because it would ban the use of "enhanced interrogation methods."

D. Oversight of the Intelligence Community

Ensuring effective cooperation and information sharing among the various IC components government presents DNI with a daunting task, the success of which carries high stakes. The challenges created by IC restructuring and management reforms increase the difficulty of the IC's work. Comptroller General David Walker has labeled the IC as one of the "three biggest transformation challenges that exist in the Federal Government from a management standpoint."[15]

The 9/11 Commission report concluded that congressional oversight of intelligence was dysfunctional and should be improved.[16] With the current transformational challenges, combined with the inherent difficulty and importance of the IC's work, the need for more effective oversight and accountability of the intelligence community has never been greater.

The primary congressional committees conducting oversight of the IC are the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI).[17] Various House and Senate committees, including committees with jurisdiction over homeland security, governmental affairs, and armed services, have oversight and legislative jurisdiction over certain aspects of the IC.[18]

The need for congressional oversight can outstrip the capacity and expertise of congressional committees. As an example, the 9/11 Commission was created to provide an independent review of the performance of intelligence agencies prior to September 11,

---

[15] Transcript of Senate Homeland Security and Governmental Affairs Committee Hearing entitled "GOA's Role in Supporting Congressional Oversight: An Overview of Past Work and Future Challenges and Opportunities" (March 21, 2007).

[16] *See, e.g.*, Congressional Research Service, *Congressional Oversight of Intelligence: Current Structure and Alternatives* (Updated February 8, 2008), Order Code RL32525, at p. 1 (hereinafter "*Congressional Oversight of Intelligence*").

[17] *See* 50 U.S.C. § 401a(7); SSCI website, intelligence.senate.gov; HPSCI website, intelligence.house.gov.

[18] *See Intelligence Issues for Congress*, at 11; Frederick M. Kaiser, "GAO Versus the CIA: Uphill Battles Against and Overpowering Force," *International Journal of Intelligence and Counterintelligence*, 15: 330-389 (2002), at p. 331 (hereinafter "Uphill Battles"), at 364-65; HSGAC website, hsgac.senate.gov; COGR website, oversight.house.gov; HSC website, http://homeland.house.gov.

2001, that was more extensive than the Joint Inquiry completed by HPSCI and SSCI.[19] Moreover, the congressional committees focused on intelligence matters may lack the expertise to oversee adequately the government-wide IC management reforms now underway.

GAO, often referred to as the investigative arm of Congress, augments Congress's oversight capacity. GAO's approximately 3300 employees perform reviews, audits, and investigations of federal executive branch programs and activities.[20] Unlike individual IGs, GAO can provide crosscutting, multi-agency reviews on business processes, programs, or other topics.[21]

GAO could provide a valuable tool to Congress in oversight of the IC, particularly with comprehensive audits, performance assessments, or project reviews.[22] Moreover, GAO has developed expertise in evaluating management issues across the entire federal government and has substantive expertise in management topics such as personnel systems, acquisitions and contract management, information sharing, and business practices, which has aided government agencies as they seek to improve their performance.

The IC often has limited or refused cooperation with GAO because of the high degree of secrecy surrounding intelligence matters.[23] For example, DNI took the position that a 2006 GAO report on government sharing of sensitive but unclassified information was beyond GAO's authority, and DNI refused to comment on the report.[24]

1. *Legislative Proposals*

a. *Reaffirming GAO's role*

In January 2007, Senator Akaka introduced the Intelligence Community Audit Act of 2007 (S. 82), co-sponsored by Senators Lautenberg, McCaskill, and Dodd, reaffirming GAO's authority to evaluate IC programs and activities. S. 82 has been referred to SSCI. Representative Bennie Thompson introduced a companion bill (H.R. 978) in the House of

---

[19] *See, e.g., Intelligence Issues for Congress*, at pp. 9-10.

[20] *See* GAO website, gao.gov, gao.gov/about/workforce.

[21] *See* Letter from David Walker, Comptroller General of the Untied States, to Senators Rockefeller and Bond, March 1, 2007, available upon request.

[22] *See ibid.*; Uphill Battles at p. 369;

[23] *See generally* Uphill Battles.

[24] *See* Government Accountability Office, Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information (March 2006), GAO-06-385, at pp. 6-7, 29-31, 71.

Representatives that has been referred to both HPSCI and the Committee on Oversight and Government Reform.

More specifically, S. 82 would reaffirm GAO's authority to perform audits and evaluations of financial transactions, programs, and activities of elements of the intelligence community, and to obtain the documents needed to do so. The bill contains certain provisions to enhance the protection of classified material, including: specifying that GAO could audit or evaluate sources and methods or covert actions only upon request from SSCI, HPSCI, or the House or Senate majority or minority leader; restricting dissemination of reports on sources and methods or covert actions to the original requester, the DNI, and the relevant IC component; and affirming that GAO staff would be subject to the same confidentiality requirements and same statutory penalties for unauthorized disclosure as IC employees.

b. Intelligence Authorization Act Provisions to Create an IC Inspector General

Inspectors general (IG) can assist Congress in its oversight functions. The CIA has an inspector general with agency-wide auditing, investigative, and inspection powers that reports its findings to SSCI and HPSCI.[25] A CIA inquiry into the CIA IG's work launched in October 2007 and the announcement by the CIA of the creation of a special ombudsman to oversee the IG's work, have raised concerns in Congress that the CIA has been seeking to limit the IG's independence.

ODNI does not have an IG created by statute, but the Director has administratively established an IG post in his office.[26] HPSCI and SSCI have questioned whether the ODNI's IG has sufficient independence and authority and have raised concerns about restrictions on the IG's communications with Congress.[27] The IC components that are within other cabinet departments do not have their own IGs.

The Fiscal Year 2008 Intelligence Authorization Act (H.R. 2082) would create an IC-wide Inspector General.[28] The Inspector General for the IC would have overarching jurisdiction across the IC, but it would not replace any of the existing IGs in the various departments housing components of the IC.

---

[25] *See* Fiscal Year 1990 Intelligence Authorization Act, Public Law 101-193 (creating a statutory CIA IG); Uphill Battles at 366.

[26] *See Congressional Oversight of Intelligence* at pp. 22-23 n. 37.

[27] *See ibid.*; Intelligence Authorization Act for 2007 (H.R. 5020), H. Report 109-411, 109th Cong., 2nd Sess., at 26-27.

[28] As noted above, Congress enacted H.R. 2082, but the President is expected to veto it.

2. *Enhancing the Existing Committee Structure*

The 9/11 Commission recommended creating joint appropriating and authorizing committees for intelligence in each house of Congress or creating a bicameral House-Senate intelligence committee.[29] Although no action has been taken on either of these proposals, SSCI and the Senate Committee on Appropriations and its defense subcommittee have signed a memorandum of agreement designed to improve communication and cooperation between the committees.[30]

Proponents of creating a joint bicameral intelligence committee argue that it would improve communication from the executive and coordination between the House and Senate, while improving the protection of classified information and streamlining the legislative process.[31] Critics of this proposal fear that it actually would weaken oversight by reducing the number of members and staff conducting oversight and legislative work and by causing a loss in expertise if the chair of the joint committee (and presumably his or her staff) were rotated between the chambers of Congress every two years.[32]

Additional Resources

Intelligence Community website, www.intelligence.gov/index.shtml

Office of the Director of National Intelligence website, www.dni.gov

Congressional Research Service, *Intelligence Issues for Congress* (Updated February 11, 2008), Order Code RL33539

Congressional Research Service, *Congressional Oversight of Intelligence: Current Structure and Alternatives* (Updated February 8, 2008), Order Code RL32525

Congressional Research Service, *Director of National Intelligence Statutory Authorities: Status and Proposals* (Updated January 24, 2008), Order Code RL34231

Statement of J. Mitchell McConnell, Director of National Intelligence, before the Senate Select Committee on Intelligence, February 14, 2008

---

[29] *See generally Congressional Oversight of Intelligence* at pp. 1-18 (discussing both proposals).

[30] *See Congressional Oversight of Intelligence* at pp. 15-16.

[31] *See Congressional Oversight of Intelligence* at pp. 10-11 (discussing these and other possible benefits of creating a joint committee).

[32] *See Congressional Oversight of Intelligence* at pp. 12-14 (discussing these and other possible disadvantages of creating a joint committee).

Statement of Donald Kerr, Principal Deputy Director of National Intelligence, before the House Permanent Select Committee on Intelligence, December 6, 2007

Frederick M. Kaiser, "GAO Versus the CIA: Uphill Battles Against and Overpowering Force," *International Journal of Intelligence and Counterintelligence*, 15: 330-389 (2002)

Post-Hearing Questions for the Record
Submitted to the Honorable Slade Gorton
From Senator Daniel K. Akaka

"Ensuring Full Implementation of the 9/11 Commission's Recommendations"
January 9, 2007

1. As a result of the Consolidated Appropriations Act of 2005, each agency is required to have a Chief Privacy Officer assume primary responsibility for privacy and data protection policy. Successful implementation of this requirement is essential since, in 2005, the Government Accountability Office reported that federal agencies are not following all privacy and data security requirements. This trend is troubling in light of the increasing use of personal information by intelligence and law enforcement agencies.
   A. What recommendations do you have to strengthen Chief Privacy Officers at federal agencies, particularly those agencies with intelligence and law enforcement functions?
   B. What do you believe the relationship should be between the Privacy and Civil Liberties Oversight Board and agency privacy officials?

   (A) The best way to strength Chief Privacy Officers at federal agencies is for agency heads to include them fully in the decision making process. The best way to encourage agency heads to follow this course is through robust oversight by the congressional committees of jurisdiction.

   (B) The relationship between agency privacy officials and the Privacy and Civil Liberties Oversight Board should be a close and cooperative one. Agency privacy officials should stay in close touch with the Board on both emerging problems and best practices as solutions. Agency privacy officials should serve as an early warning mechanism for the Board as to the issues that require the Board's attention. An important part of the Board's work, in turn, should be to address itself to real-world problems as identified by privacy officials from the agencies.

2. The 9-11 Commission called for the creation of a Director of National Intelligence (DNI) with the task of eliminating stovepipes, driving reform, and creating a unity of effort. The Commission's final report noted that the success of the DNI would require active Congressional oversight. I share the Commission's concern. That is s why I reintroduced the Intelligence Community Audit Act of 2007 last week, which reaffirms the authority of the Government Accountability Office (GAO) to audit the financial transactions and evaluate the programs and activities of the intelligence community. The legislation does not interfere with the clear responsibility of the intelligence committees for intelligence sources and methods or covert activities. Rather, my bill clarifies GAO's authority to conduct audits and evaluations relating to the management and administration of elements of the intelligence community in areas such as strategic planning, financial

management, information technology, human capital, knowledge management, information sharing, and change management – on behalf of other relevant Congressional committees.

Do you believe that Congressional oversight committees would benefit from the ability to task GAO to conduct audits and evaluations of the intelligence community?

The GAO should have the authorities with respect to the Intelligence Community as it does with respect to other agencies of the federal government. In short, the GAO should have the authority to audit financial transactions and evaluate the programs and activities of the intelligence community.

The intent of the Intelligence Community Audit Act of 2007 (S.82), is a very good one. Congressional oversight committees would benefit from the ability to task GAO to conduct audits and evaluations of the intelligence community. The Intelligence Community, in turn, would benefit from its agencies being held to the same high standards of performance as other agencies of the Federal Government.
From an accountability standpoint, there is much to be said for granting the GAO authority to audit intelligence agencies in a manner similar to that of other federal agencies.

The most direct way in which to assure the success of the DNI, however, is to broaden his authority over other intelligence agencies in a manner consistent with the 9/11 Commissioner's report and with the original 2004 Senate bill, unfortunately watered down in conference with the House.

Post-Hearing Questions for the Record
Submitted to the Honorable Lee H. Hamilton
From Senator Daniel K. Akaka

"Ensuring Full Implementation of the 9/11 Commission's Recommendations"
January 9, 2007

1. The 9-11 Commission called for the creation of a Director of National Intelligence (DNI) with the task of eliminating stovepipes, driving reform, and creating a unity of effort. The Commission's final report noted that the success of the DNI would require active Congressional oversight. I share the Commission's concern. That is s why I reintroduced the Intelligence Community Audit Act of 2007 last week, which reaffirms the authority of the Government Accountability Office (GAO) to audit the financial transactions and evaluate the programs and activities of the intelligence community. The legislation does not interfere with the clear responsibility of the intelligence committees for intelligence sources and methods or covert activities. Rather, my bill clarifies GAO's authority to conduct audits and evaluations relating to the management and administration of elements of the intelligence community in areas such as strategic planning, financial management, information technology, human capital, knowledge management, information sharing, and change management - on behalf of other relevant Congressional committees.

   Do you believe that Congressional oversight committees would benefit from the ability to task GAO to conduct audits and evaluations of the intelligence community?

   Answer: It has long been my view that that GAO should have the same authorities with respect to the Intelligence Community as it does with respect to other agencies of the federal government. In short, the GAO should have the authority to audit financial transactions and evaluate the programs and activities of the intelligence community.

   The intent of the Intelligence Community Audit Act of 2007 (S.82), is a very good one. Congressional oversight committees would benefit from the ability to task GAO to conduct audits and evaluations of the intelligence community. The Intelligence Community, in turn, would benefit from its agencies being held to the same high standards of performance as other agencies of the Federal Government.

2. As a result of the Consolidated Appropriations Act of 2005, each agency is required to have a Chief Privacy Officer assume primary responsibility for privacy and data protection policy. Successful implementation of this requirement is essential since, in 2005, GAO reported that federal agencies are not following all privacy and data security requirements. This trend is troubling in light of the increasing use of personal information by intelligence and law enforcement agencies.

A. What recommendations do you have to strengthen Chief Privacy Officers at federal agencies, particularly those agencies with intelligence and law enforcement functions?

B. What do you believe the relationship should be between the Privacy and Civil Liberties Oversight Board and agency privacy officials?

Answer: (A) The best way to strengthen Chief Privacy Officers at federal agencies is for agency heads to include them fully in the decision making process. The best way to encourage agency heads to follow this course is through robust oversight by the congressional committees of jurisdiction.

(B) The relationship between agency privacy officials and the Privacy and Civil Liberties Oversight Board should be a close and cooperative one. Agency privacy officials should stay in close touch with the Board on both emerging problems and best practices as solutions. Agency privacy officials should serve as an early warning mechanism for the Board as to the issues that require the Board's attention. An important part of the Board's work, in turn, should be to address itself to real-world problems as identified by privacy officials from the agencies.

Woodrow Wilson
International
Center
for Scholars

LEE H. HAMILTON
President and Director

SENATOR DANIEL K. AKAKA
WASHINGTON, D.C.
2007 FEB -2 PM 4:19

January 24, 2007

The Hon. Daniel K Akaka
Chairman
Subcommittee on Oversight of Government Management,
The Federal Workforce and the District of Columbia
Committee on Homeland Security and Government Affairs
United States Senate
Washington, D.C. 20510-6250

Dear ~~Mr. Chairman~~:

It was a pleasure to see you at the hearing on January 9th and I regret that our schedules precluded a round of questions and answers between us. I also want to thank you for your letter of January 10, 2007 and your excellent question concerning the authorities of the Government Accountability Office (GAO).

It has long been my view that that GAO should have the same authorities with respect to the Intelligence Community as it does with respect to other agencies of the federal government. In short, I agree with you that the GAO should have the authority to audit financial transactions and evaluate the programs and activities of the intelligence community.

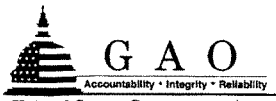
The intent of your bill, the Intelligence Community Audit Act of 2007 (S.82), is a very good one. I concur with you that Congressional oversight committees would benefit from the ability to task GAO to conduct audits and evaluations of the intelligence community. The Intelligence Community, in turn, would benefit from its agencies being held to the same high standards of performance as other agencies of the Federal Government.

With best wishes,

Sincerely,

Lee H. Hamilton

With best!
Lee



Comptroller General
of the United States

United States Government Accountability Office
Washington, DC 20548

March 11, 2008

The Honorable Daniel K. Akaka
Chairman
The Honorable George V. Voinovich
Ranking Minority Member
Subcommittee on Oversight of Government Management,
the Federal Workforce, and the District of Columbia
Committee on Homeland Security and Governmental Affairs
United States Senate

Subject: *Question for the Record Related to the Number of GAO Staff Who Hold Security Clearances*

On February 29, 2008, I testified before your Subcommittee at a hearing on "Government-wide Intelligence Community Management Reforms." This letter responds to a question from Senator Akaka regarding the number of GAO staff who have Top Secret security clearances and the number of GAO staff who hold SCI clearances that I promised to provide for the record.

According to GAO's Office of Security, as of March 5, 2008, GAO had 3,153 total staff of whom 1,000 held Top Secret security clearances and 73 held SCI clearances.

If you or other members of the Subcommittee have any additional questions, please contact Davi M. D'Agostino, Director, at (202) 512-5431 or dagostinod@gao.gov.

David M. Walker
Comptroller General
of the United States

cc: Richard Kessler
Lisa Powell
Thomas Bishop
Jessica Nagasako

United States Government Accountability Office
Washington, DC 20548

April 25, 2008

The Honorable Daniel K. Akaka
Chairman
The Honorable George V. Voinovich
Ranking Minority Member
Subcommittee on Oversight of Government Management,
the Federal Workforce, and the District of Columbia
Committee on Homeland Security and Governmental Affairs
United States Senate

Subject: *Intelligence Reform: Post-Hearing Questions for the Record Related to the Structure of the Intelligence Community and Oversight*

On February 29, 2008, then-Comptroller General David M. Walker testified before your Subcommittee at a hearing on Government-wide Intelligence Community Management Reforms.[1] This letter responds to your request for additional information on that subject. Your questions and our responses follow.

1. **As a member of the Homeland Security and Governmental Affairs Committee, I have been concerned about the transformational challenges that the Department of Homeland Security (DHS) faces bringing together 22 agencies into a cohesive department. DHS still faces significant difficulties getting all of its components cooperating on management and operational issues.**

   The Intelligence Community (IC) is much more decentralized than a department, and the Director of National Intelligence (DNI) does not have line management authority over heads of intelligence community elements, except for the Central Intelligence Agency (CIA).

   a. **How does this decentralized structure affect the challenges of implementing the management reforms that the DNI has proposed?**

The decentralized structure of the Intelligence Community increases the difficulty of implementing management reforms consistently. Specifically, with the exception of the CIA, the other 15 Intelligence Community members are components of cabinet-

[1] GAO, *Intelligence Reform: GAO Can Assist the Congress and the Intelligence Community on Management Reform Initiatives*, GAO-08-413T (Washington, D.C.: Feb. 29, 2008).

level departments, including the Departments of Defense (DOD), Energy, Homeland Security, Justice, State, and the Treasury. Each department has its own authorities and management practices. Furthermore, some agencies within a department have their own authorities and management practices. For example, while 8 of the 16 Intelligence Community components are organizationally aligned within DOD, 4 of these components are associated with the individual military services, which have their own Title 10 authorities. Therefore, while the DNI might advocate specific management reforms, the extent to which these reforms are implemented, if at all, depends on the extent to which they are aligned with the other agencies' goals and priorities. As a result, it would be more difficult to achieve consistency within Intelligence Community components than it would be to do so within a single cabinet-level department.

b. Have you observed tensions between the priorities of the DNI and intelligence officials who are part of agencies—particularly those that are not primarily focused on intelligence, like the State Department or Department of Energy? If so, does this have any implications for the IC's management initiatives?

We have not conducted review work that specifically addresses this issue or the agencies that you identified. We would note, however, that our recent work on intelligence, surveillance, and reconnaissance (ISR) requirements has noted some tensions between DOD and the Intelligence Community.[2] For example, DOD and the Office of the Director of National Intelligence (ODNI) maintain separate processes for identifying future ISR requirements. In addition, the complex and diverse context of the organizational cultures, funding arrangements, requirements processes, and missions of the other members of the Intelligence Community supported by DOD presents a challenge for DOD in integrating its ISR enterprise. Observers have noted in the past that cultural differences between the defense and national intelligence agencies and their different organizational constructs often impede close coordination.[3] Even within DOD, certain elements of the Intelligence Community—the National Geospatial-Intelligence Agency and the National Security Agency—are, at the same time, both combat support agencies and national intelligence agencies. This complexity can complicate the implementation of cross-cutting management reforms in areas such as strategic human capital transformation.

c. What implications, if any, does the decentralized structure of the IC have for effective congressional oversight?

The fragmented and decentralized structure of the Intelligence Community can also lead to congressional oversight challenges. Specifically, multiple congressional committees have authorization, appropriation, budget, and oversight jurisdiction over ODNI and the 16 different Intelligence Community members. For example, while the House and Senate select committees on intelligence have various jurisdictions (e.g.,

---

[2] GAO, *Intelligence, Surveillance, and Reconnaissance: DOD Can Better Assess and Integrate ISR Capabilities and Oversee Development of Future ISR Requirements*, GAO-08-374 (Washington, D.C.: Mar. 24, 2008).

[3] These observers include Congress, the congressionally chartered Space Commission, a joint task force of the Defense Science Board, and a private sector organization.

authorization and oversight) over ODNI and the CIA, they share jurisdiction over the DOD intelligence components with the armed services committees. The same multi-jurisdictional situation applies for intelligence components that are organizationally aligned with the other cabinet-level departments.

d. What implications, if any, does the decentralized structure of the IC have for GAO's role in reviewing IC management reforms?

GAO regularly reviews issues that cut across multiple cabinet-level departments and agencies, and could provide a holistic approach to reviewing Intelligence Community management reforms, regardless of that community's organizational structure. However, GAO will be limited in its ability to provide a comprehensive view of these reforms without gaining access to all of the Intelligence Community members, especially with regard to the ODNI, which would most likely be the proponent for any Intelligence Community-wide management reforms.

GAO's statutory authority permits us to evaluate a wide-range of Intelligence Community programs and activities, including management and administrative functions that intelligence agencies have in common with all federal agencies. However, since 1988, the Department of Justice has maintained that Congress intended the intelligence committees to be the exclusive means of oversight of the Intelligence Community. In 2006, ODNI agreed with the Department of Justice's position, stating that the review of intelligence activities is beyond GAO's purview. We strongly disagree with that view, but without support from Congress, the current limits on our access will not materially change. However, we recently received two requests from the House Permanent Select Committee on Intelligence to examine personnel security clearance processes used by the intelligence community. Also, we would need the support of the intelligence committees, which generally have not requested GAO reviews of intelligence agencies' programs and activities for a number of years. Finally, we would need greater cooperation and access from the Intelligence Community itself in order for us to review that community's management reforms.

If you or other members of the Subcommittee have any additional questions, please contact me at (202) 512-5600 or Davi M. D'Agostino, Director, at (202) 512-5431 or dagostinod@gao.gov.

Janet A. St Laurent

Janet A. St Laurent
Managing Director, Defense Capabilities
and Management