PROTECTION OF PRIVACY IN THE DHS INTELLIGENCE ENTERPRISE PART I AND II

HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

APRIL 6, 2006 and MAY 10, 2006

Serial No. 109–72

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE

27–629 PDF WASHINGTON : 2006

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

PETER T. KING, California, *Chairman*

DON YOUNG, Alaska
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania, *Vice Chairman*
CHRISTOPHER SHAYS, Connecticut
JOHN LINDER, Georgia
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
JIM GIBBONS, Nevada
ROB SIMMONS, Connecticut
MIKE ROGERS, Alabama
STEVAN PEARCE, New Mexico
KATHERINE HARRIS, Florida
BOBBY JINDAL, Louisiana
DAVE G. REICHERT, Washington
MICHAEL MCCAUL, Texas
CHARLIE DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

ROB SIMMONS, Connecticut, *Chairman*

CURT WELDON, Pennsylvania
MARK E. SOUDER, Indiana
DANIEL E. LUNGREN, California
JIM GIBBONS, Nevada
STEVAN PEARCE, New Mexico
BOBBY JINDAL, Louisiana
CHARLIE DENT, Pennsylvania
GINNEY BROWN-WAITE, Florida
PETER T. KING, New York
ZOE LOFGREN, California
LORETTA SANCHEZ, California
JANE HARMAN, California
NITA M. LOWEY, New York
SHEILA JACKSON-LEE, Texas
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida
BENNIE G. THOMPSON, Mississippi

CONTENTS

PROTECTION OF PRIVACY IN THE DHS INTELLIGENCE ENTERPRISE PART I

Thursday, April 6, 2006

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING AND TERRORISM RISK ASSESSMENT,
Washington, DC.

The subcommittee met, pursuant to call, at 9:20 a.m., in Room 311, Cannon House Office Building, Hon. Rob Simmons [chairman of the subcommittee] presiding.

Present: Representatives Simmons, Gibbons, Dent, Brown–Waite, Lofgren, and Thompson.

Mr. SIMMONS. [Presiding.] The subcommittee will be meeting today to hear testimony on the protection of privacy in the Department of Homeland Security Intelligence Enterprise.

We will be hearing testimony from four witnesses today. Our first panel, we will hear from Ms. Maureen Cooney, acting chief privacy officer of the Department of Homeland Security.

On our second panel, we will hear from Mr. Kirk Herath, chief privacy officer and associate general counsel at the Nationwide Insurance Companies; Mr. Jonathan Turley, Shapiro professor of Public Interest Law at the George Washington University Law School; and Lieutenant General Patrick Hughes, vice president of Homeland Security at L–3 Communications.

And I thank all of our panelists for coming today.

The right to privacy is implicit in the Fourth Amendment right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures, and it shall not be violated.

It is embedded in the founding ideals of this nation. Justice William O. Douglas, in Griswold v. Connecticut, wrote that the right to privacy is "older than the Bill of Rights, older than our political parties."

We are all acutely aware of the privacy issues facing the government today, especially as the president and Congress work to defend America against those who wish to commit mass murder.

And I remind my colleagues and others of a passage in the 9/11 Commission report, which states, "We learned that the institutions charged with protecting our borders, civil aviation and national security did not understand how grave this threat could be and did not adjust their polices, plans and practices to deter or defeat it.

We learned of fault lines within our government between the foreign and domestic intelligence and between and within agencies. We learned of the pervasive problems of managing and sharing information across large and unwieldy government that has been built in a different era to confront different dangers. We hope that the terrible losses chronicled in this report can create something positive—an America that is safer, stronger and wiser."

And, indeed, the creation of the Department of Homeland Security was a response to that effort to create something positive, something safer, stronger and wiser, but at the same time, something that respects our Constitution and our Bill of Rights and the rights that are detailed therein.

The House Permanent Select Committee on Intelligence is leading the effort to examine the NSA Terrorist Surveillance Program, and the House Judiciary Committee is taking a close look at the Foreign Intelligence Surveillance Act. Speaking for myself, I support both of those committee initiatives.

We are here today to ensure that the Department of Homeland Security is also paying proper attention to privacy matters at the department and the department's intelligence activities.

The Department of Homeland Security has a legally mandated duty to protect the privacy of U.S. persons in the course of its intelligence work and in its information collection activities. However, just 2 days ago, the General Accounting Office issued a report stating that federal agencies, including DHS, lacked polices that specifically address their use of personal information from commercial sources.

Ms. Cooney, I hope you will be able to address some of these issues for us in your testimony today.

While DHS receives information from commercial sources, it also receives information from intelligence and law enforcement communities as through the regulatory screening activities of the department.

This information is vital to America's border security, critical infrastructure protection, transportation security, and a number of other security activities. Gathering, processing, analyzing and sharing information intelligence will be vital to preventing the next attack on our homeland. We must ensure, however, that the department protects the privacy of the American people while also protecting them from terrorist attack.

The chair now recognizes the ranking minority member of the committee, the gentlelady from California, Ms. Lofgren, for any statement she might wish to make.

Ms. LOFGREN. Thank you, Mr. Chairman.

Welcome, Ms. Cooney, and also Mr. Harris and Mr. Turley.

I appreciate being recognized for this statement. Our topic is privacy rights. I think the elephant in the room is the issue of the NSA Warrantless Eavesdropping Program. NSA eavesdropping is an important issue for the subcommittee to address under its oversight responsibilities over intelligence and information sharing techniques.

The Bush administration has failed repeatedly to give Congress meaningful answers about this eavesdropping program, and the Congress so far has failed to hold it accountable through oversight.

The administration seems unwilling to provide Congress with the information it needs to conduct its proper oversight role.

I have tried to secure information about this Warrantless Eavesdropping Program. I have asked the Department of Defense and the Department of Justice to investigate this program, but they have declined.

I asked President Bush to direct that a special council be appointed to investigate. He has not answered the letter, but through his press secretary, declined.

To date, press reports are all the information about this program that members of Congress and the public have. Congress should not accept this.

One serious question about this Warrantless Eavesdropping Program is whether it complies with the law. This subcommittee should get an answer to that question.

Whenever possible, it is important to work in a bipartisan fashion. Indeed, 2 weeks ago, the chairman and I produced a legislation jointly, and I think we set a land-speed record for a subcommittee markup. It is not comfortable or enjoyable to be critical when you sit next to somebody on a frequent basis and hope to work with them, but the hope for comity can never be an excuse for ducking the need to take action.

As a ranking member, I cannot and do not control the agenda of our subcommittee. The chairman sets the agenda. I have sought to have this committee discharge its oversight responsibility in the matter of the NSA through written request by staff, written request by myself, as well as personal conversations, but these efforts resulted in today's hearing that will not serve as the needed oversight of the NSA Warrantless Surveillance Program.

I tried to secure a witness from the NSA to testify today, and as part of the record, I ask unanimous consent to place material about this in the record of this hearing.

Mr. SIMMONS. Without objection, so ordered.

Ms. LOFGREN. Thank you.

I appreciate that Professor Turley is here today to testify about the NSA Eavesdropping Program. I thank him for his testimony, which I have reviewed. His observations about the administration's legal claims in support of this program are important, and it is viewed the administration's legal claims present risks, not only for our intelligence gathering process, but also for our constitutional separation of powers are significant.

While I am thankful to have Professor Turley's testimony, Congress needs to hear more than legal arguments from scholars about this program. We need to do our oversight job and find out what is actually going on by calling the witnesses who have direct knowledge of what the government is actually doing.

There is only one intelligence subcommittee as the Homeland Security Committee and we are it. We cannot get thorough information on the NSA Eavesdropping Program without a government witness with firsthand knowledge about it.

So today is a lost opportunity for this subcommittee. But today, actually right now, the attorney general of the United States is testifying before the House Judiciary Committee. The attorney general knows all about the NSA program and is in a position to an-

swer questions about it. I don't know if he will, but the opportunity to question him about what he knows about the NSA program is a far sight more promising than what we will have allowed this hearing to be.

So I will excuse myself now to see whether the attorney general will permit the Congress to discharge its oversight obligations. With regrets, the structure of this hearing ensures that we will not succeed in that mission in this subcommittee today.

And I would also like to present to the chair a letter from the minority pursuant to Rule 2M. We are seeking an additional hearing.

Thank you, Mr. Chairman. I am going to go see Mr. Gonzales.

Mr. SIMMONS. Normally, I would yield to the distinguished ranking member of the committee, but the ranking member of the subcommittee has made a few statements that I would have to respond to.

This subcommittee has had this civil rights and privacy hearing on the schedule for some time, and we have been open to any witnesses that the minority would submit to us.

It is my understanding that the individual that the ranking member refers to could not make it today, and so in a bipartisan fashion, we extended to the minority the opportunity of introducing that information into the record at a later date and holding the record open, which I thought was a fair proposal.

We also offered to postpone this hearing to a later date.

Ms. LOFGREN. That is incorrect, sir.

Mr. SIMMONS. Well, that is what I suggested to my staff. We also discussed the issue of recessing and reconvening. So from my perspective, at least from where I sit, every effort has been made to make this a productive hearing.

It is very disappointing to me to hear a prepared statement typed and prepared, obviously, in advance, and only to receive it here on the record. That to me is a disappointing thing to have to experience, but I guess I can say that in my experience on the Hill, both as a staffer on the Senate Intelligence Committee for 4 years and in my 5 years as a member of Congress, doing my best to provide bipartisan oversight. I have encountered disappointments.

Ms. LOFGREN. If I will just—

Mr. SIMMONS. If the lady would allow me to finish my statement.

Ms. LOFGREN. Certainly.

Mr. SIMMONS. I have encountered those disappointments, and I will not allow those disappointments to prevent me from continuing to conduct the activities of this subcommittee in a bipartisan fashion to the best of my ability.

And now the chair would like to recognize the distinguished ranking member of the full committee, Mr. Bennie Thompson of Mississippi. The gentleman is recognized.

Mr. THOMPSON. Thank you, Mr. Chairman. In the interest of being fair and balanced, I will yield my time to the ranking member for a response.

Ms. LOFGREN. And I thank the ranking member. I would just note that I have now served in Congress for a little over 11 years, and I have never encountered a situation such as this in those 11 years. The NSA is reluctant to testify. They need to be ordered to

testify by, not the ranking member because I lack that power, but by the chairman.

We have endeavored to secure that. We have asked for—perhaps the chairman did order his staff to delay. They have refused our staff the opportunity. So I don't want to get in a he-said-she-said. There is no point in that. But I am severely disappointed that we have failed to discharge our oversight hearing. I will always work in a bipartisan way when there is an opportunity.

In the last Congress, Mr. Thornberry and I actually almost melded our staffs. We didn't have a majority and minority report at the end of the Congress. We had one report. I hope that we can do that again this year, but so far, I had to conclude that we may not achieve that level of success. That is not the topic here today.

I will just say, this is an opportunity—was an opportunity to discharge the oversight obligations that we have as the Intelligence Subcommittee over the NSA. We will not accomplish that in this subcommittee today, and I think that is a disappointment. Perhaps we will remedy that in the future. And if so, I will eagerly be a participant with the chairman.

And I would yield back to the ranking member, and I will now adjourn to the attorney general.

Mr. THOMPSON. Thank you very much.

Reclaiming my time, Mr. Chairman.

I am pleased that the committee is turning its attention to the question of privacy protections in the department's Intelligence Enterprise. The Privacy Office has done a tremendous job in making privacy an integral part of the department's various initiatives and technology program.

The more often we respect privacy from the beginning, the more likely expensive department programs won't have to be canceled for ignoring this cherished right. Respecting privacy makes good business sense.

While I look forward to Ms. Cooney's testimony about how privacy should inform the department intelligence process, I note that she could do her job more effectively if she had more powers.

I believe that the privacy officer must be able to access all the records and speak to all the people she needs to in order to conduct truly effective privacy impact assessments. To boost her independence, moreover, the privacy officer should serve a set term and should be able to report her findings to Congress directly rather than having to rely on an internal review process at the department that has often resulted in delays.

As one observer has noted, while a truly vigorous and independent privacy officer can be inconvenient for government officials over the short term, over the long run, vigorous checks and balances will strengthen the Department of Homeland Security by inspiring greater public confidence in DHS programs. This is especially important in an intelligence context.

As a recently publicized NSA Domestic Surveillance Program has demonstrated, there must be effective oversight within agencies and by Congress itself in order to ensure that the war on terror does not also become a war on privacy and other civil liberties.

I hope all the witnesses, including Professor Turley, will address this issue so we can learn more about what the department might

do to guard against the kinds of abuses we have seen with the NSA and what steps Congress should take to ensure that the NSA program does not undermine the public support for our efforts to secure the homeland.

Welcome to our witnesses.

And I yield back, Mr. Chairman.

Mr. SIMMONS. I thank the gentleman for his statement. And I assure him that one of the purposes of this hearing is to learn how the privacy office is performing its duties, and if, in fact, issues that are currently in regulation need to be in statute. It would be our responsibility to act positively in that fashion.

Mr. GIBBONS. Mr. Chairman, parliamentary inquiry.

Mr. SIMMONS. Yes, Mr. Gibbons?

Mr. GIBBONS. Mr. Chairman, would you tell me what the jurisdiction of this committee is? Do we have jurisdiction over NSA?

Mr. SIMMONS. I have discussed that with the parliamentarian of the House of Representatives, and I have been told that we do not.

Mr. GIBBONS. I had objected to, in addition, of Ms. Lofgren's letters regarding her request on NSA to the committee. And I would say that as a concept of jurisdictional oversight that comments about this committee's failure to bring NSA before it certainly lacks our jurisdiction, and I would hope that my objection to the addition of Ms. Lofgren's letters regarding NSA to this committee would stand.

Mr. SIMMONS. I appreciate the gentleman's comment.

In January of this year, I did write to the chair and ranking members of the intelligence committee and asked permission to have access to the information within their committee dealing with the National Security Surveillance Program.

That permission was not granted, and at the time, I was told that the House of Representatives would pursue oversight of those activities through the two committees which have jurisdiction, which are the Intelligence Committee and the Judiciary Committee.

So that fact is well known, and the ranking member of the subcommittee does know that the Judiciary Committee on which she serves has jurisdiction.

Mr. GIBBONS. I had voiced my objection at the time the letter was admitted, but I did not get a response out of you, so I would just state for the record that I did object to her inclusion of that letter.

Mr. SIMMONS. The objection is heard, and without objection, it is sustained.

Mr. THOMPSON. Excuse me, Mr. Chairman. By sustaining the objection, what are you saying?

Mr. SIMMONS. The subcommittee, a few moments ago, agreed by unanimous consent to include a letter into the record from, I believe, an individual from the National Security Agency. I do not know what that letter is. Nobody on the subcommittee knows what that letter is, or at least not on this side.

The gentleman from Nevada has expressed an objection to including that letter in the record now that he knows more about it.

Am I correct, Mr. Gibbons?

Mr. GIBBONS. That is absolutely correct, and it is based on the jurisdiction of this committee. If the letter were in about the Homeland Security Department, that would be another story, but it is based on jurisdiction outside this committee, and I don't know what the content of the letter is, and I don't know what it was about. I don't think it is official for this committee to take up matters.

Mr. THOMPSON. Well, Mr. Chairman, I would like to say under the rules according to the minority interpretation, we believe we do have jurisdiction, and we just have a difference of opinion.

Mr. SIMMONS. Why don't we agree if it is agreeable that we will review the transcript and make a determination at a later date, and I will withdraw my offer to sustain the gentleman's objection.

Mr. GIBBONS. I don't have a problem with bringing it before the committee and having the committee in general look at it and make that decision.

Mr. SIMMONS. Is that agreeable to the ranking member?

Mr. THOMPSON. In terms of withdrawing it and looking at it later?

Mr. SIMMONS. Yes.

Mr. THOMPSON. No problem.

Mr. SIMMONS. I thank the gentleman.

I also thank the patience of our witnesses here today as we try to work our way through certain issues and get started.

The chair now calls our first panel, Ms. Maureen Cooney, acting chief privacy officer of the Department of Homeland Security. During her time with DHS Privacy Office, Ms. Cooney has served as chief of staff and as director of International Privacy Policy before becoming acting chief privacy officer.

Ms. Cooney worked on international privacy and security issues as legal adviser for the International Consumer Protection at the U.S. Federal Trade Commission, and her legal career includes broad experience with the national services and enforcement issues, including international work on anti-money laundering and foreign compliance issues, information sharing and privacy and security matters. She is a graduate of Georgetown University and holds a JD from the Georgetown University Law Center.

I notice, Ms. Cooney, that you have substantial testimony that you wish to make. Normally, we limit it to 5 minutes, but if you need to exceed that, please be my guest. And welcome.

STATEMENT OF MAUREEN COONEY, ACTING CHIEF PRIVACY OFFICER, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. COONEY. Thank you. Good morning. Chairman Simmons, Ranking Member Thompson and members of the subcommittee, it is an honor to testify before you today on privacy activities across the Department of Homeland Security.

As the subcommittee well knows, the Department of Homeland Security was the first agency to have a statutorily required privacy officer. The inclusion of a senior official accountable for privacy policy and protection within the department honors the value placed on privacy as an underpinning of the American freedoms and democracy we seek to protect.

Privacy is a cultural value at DHS. Secretary Chertoff recently noted that as a young department, we have the opportunity to

build into the sinews of this organization respect for privacy and the thoughtful approach to privacy.

He went on to express a belief that I share. We want the government to be a protector of privacy, and we want to build security regimes that maximize privacy protection and that do it in a thoughtful and intelligent way. If it is done right, it will be not only a long-lasting ingredient of what we do in Homeland Security, but a very good template for what governments ought to do in general when it comes to protecting people's personal autonomy and privacy.

The chief privacy officer and the DHS Privacy Office have a special role working in partnership and collaboration across the department, to integrate privacy into the consideration of the ways in which the department assesses its programs, uses technologies and handles information.

The Privacy Office has oversight of privacy policy matters and information disclosure policy, including compliance with the Privacy Act of 1974, the Freedom of Information Act, and the Completion of Privacy Impact Assessment.

The Privacy Office also evaluates new technologies used by the department for their impact on personal privacy. Further, under Section 222, the chief privacy officer is required to report to Congress on these matters, as well as on complaints about possible privacy violations.

The DHS Privacy Office takes an operational approach to advancing privacy policy. We embed adherence to good privacy practices in the investment and oversight and design phases or programs through accountability and transparency tools, including privacy notices required under the Privacy Act, the use of privacy impact assessments and privacy audits and complaint reviews.

Our approach is consistent for all DHS programs and initiatives, and we have found that it works equally well for the law enforcement, homeland security and intelligence functions of the Department.

As mentioned, one of the main mechanisms for operationalizing privacy protections is through the consistent use of the privacy impact assessment process throughout the department.

The General Accountability Office released a report earlier this week on government use of commercial reseller data and compliments, in fact, the Department of Homeland Security's privacy impact assessment process and guidance, which has been shared with our federal partners across the government.

They also complimented the department on its dialogue on that very issue and the guidance which we are currently writing and collaborating on with within the department.

Privacy impact assessments required by Section 208 of the E-Government Act of 2002 and Section 222 of the Homeland Security Act allow us to access the privacy impact of utilizing new or significantly changing information systems that collect personally identifiable information, including attention to mitigating privacy risks.

Although the E-Government Act allows exceptions from the PIA requirement for national security systems, as a matter of good privacy practice, the Privacy Office at the Department of Homeland Security requires that all DHS systems, including national security

systems, undergo a PIA—privacy impact assessment—if they contain personal information.

We use the PIA process as a good government information management tool and privacy protective process across the department's programs.

In cases where the publication of a PIA would be detrimental to national security, the PIA document may not be published or may be published in a redacted form. This means that information systems that are part of the Intelligence Enterprise at the department also undertake these important analyses to ensure the privacy considerations are fully integrated into their deployment of programs.

Let me quickly turn to information sharing. The Department of Homeland Security was created, in significant part, to foster information sharing for homeland security purposes. The Privacy Act, of course, provides the statutory authority for both inter-and intra-agency information sharing.

The Privacy Office policy supports the exchange of information between the department's component organizations whenever those organizations establish an appropriate need based on an express purpose.

We work with department components to facilitate the timely exchange of information in a privacy-sensitive manner, while working toward the goal of the right persons getting the right information at the right time.

The department must also foster external information sharing for homeland security purposes with all of our partners at the federal, state, local, tribal and private sector levels. As the department incorporates the need to share in its internal and external information sharing design, it is, of course, paramount that privacy be built into the process.

We have worked collaboratively with our intelligence and analysis colleagues for whom information sharing is part of their critical mission—to also ensure that personally identifiable information of U.S. persons is treated in a manner that fully conforms with their rights and is handled sensitively.

The DHS policy on handling U.S. person information contains a significant role for the DHS privacy officer to review activities that could involve a potential violation of the privacy rights of U.S. citizens and also requires the privacy officer to collaborate on new initiatives to ensure that they enhance and do not erode privacy protections relating to the collection, use and maintenance of personal information.

Members of the committee, we take this responsibility very seriously. We look forward to working with you on this effort and ask for your support. Thank you for inviting me today.

[The statement of Ms. Cooney follows:]

PREPARED STATEMENT OF MAUREEN COONEY

APRIL 6, 2006

Introduction

Chairman Simmons, Ranking Member Lofgren, and Members of the Subcommittee, it is an honor to testify before you today on privacy activities at the United States Department of Homeland Security, with particular reference to privacy as part of the Department's Intelligence Enterprise.

Because this marks my first appearance before the Subcommittee, I would like to offer some biographical background. It is my honor to currently serve as the Acting Chief Privacy Officer for the Department of Homeland Security. I come to this post with 20 years of federal experience in risk management and compliance and enforcement activities as well as in consumer protection work on global information privacy and security issues post 9-11. I was recruited from the Federal Trade Commission to join the Department of Homeland Security more than two years ago as Chief of Staff of the Privacy Office and Senior Advisor for International Privacy Policy. Since that time, it has been my privilege to help build the DHS Privacy Office, under the leadership of former Chief Privacy Officer, Nuala O'Connor Kelly, and Secretaries Chertoff and Ridge.

As the Subcommittee well knows, the Department of Homeland Security was the first agency to have a statutorily required Privacy Officer. The inclusion of a senior official accountable for privacy policy and protections within the Department honors the value placed on privacy as an underpinning of our American freedoms and democracy. It also reflects Congress' understanding of the growing sensitivity and awareness of the ubiquitous nature of personal data flows in the private and public sectors and a recognition of the impact of those flows upon our citizens' lives.

In addressing the Department's Data Privacy and Integrity Advisory Committee, which was created to advise the Secretary and the Chief Privacy Officer on significant privacy issues, Secretary Michael Chertoff recently noted that the Department has the opportunity to build into the "sinews of this. . .organization, respect for privacy and a thoughtful approach to privacy." Secretary Chertoff expressed a belief that I share:

> *We want the government to be a protector of privacy, and we want to build security regimes that maximize privacy protection and that do it in a thoughtful and intelligent way . . . . [I]f it's done right,[it] will be not only a long-lasting ingredient of what we do in Homeland Security, but a very good template for what government ought to do in general when it comes to protecting people's personal autonomy and privacy.*[1]

The Chief Privacy Officer[2] and the DHS Privacy Office have a special role, working in partnership and collaboration across the Department, to integrate privacy into the consideration of the ways in which the Department assesses its programs and uses technologies, handles information, and carries out our protective mission. The Privacy Office has oversight of privacy policy matters and information disclosure policy, including compliance with the *Privacy Act of 1974,* the *Freedom of Information Act,* and the completion of Privacy Impact Assessments on all new programs, as required by the *E-Government Act of 2002* and Section 222 of the *Homeland Security Act of 2002.* The Privacy Office also evaluates new technologies used by the Department for their impact on personal privacy. Further, under Section 222, the Chief Privacy Officer is required to report to Congress on these matters, as well as on complaints about possible privacy violations.

Today, I would like to describe for you how the Privacy Office has worked to build privacy into the sinews of our organization so that a culture of privacy informs the way in which we carry out our national mission of protecting our homeland. I'll explain our operational approach of embedding adherence to good privacy practices into the programs of the Department, through the budget and design phases of programs, through accountability and transparency tools, including reviews of privacy notices (systems of records notices), the use of privacy impact assessments, and privacy audits and reviews. Our approach is consistent for all DHS programs and ini-

---

[1] March 7, 2006 public Meeting of the Department of Homeland Security Data Privacy and Integrity Advisory Committee, Ronald Reagan Building and International Trade Center, Washington, D.C.

[2] The DHS Chief Privacy Officer is the first statutorily required privacy officer in the federal government. Section 222 of the Homeland Security Act, as amended, provides in pertinent part, the responsibilities of the DHS Chief Privacy Officer are to assume primary responsibility for privacy policy, including—

(1) assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection and disclosure of personal information;

(2) assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974;

(3) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government;

(4) conducting a privacy impact assessment of proposed rules of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected; and

(5) preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of the Privacy Act of 1974, internal controls and other matters.

tiatives and we have found that it works equally well for the law enforcement, homeland security and intelligence functions of the Department.

I would then like to focus on the mandates of information sharing and intelligence activities and how those imperatives for national preparedness can be achieved while integrating privacy attentiveness and protections into Departmental operations.

Building a Culture of Privacy

The Privacy Office works in partnership with each DHS Directorate and component to promote a business ethic of privacy attentiveness and responsible stewardship for the personal information that we collect, use and disseminate. This is fundamental to the Department's overall achievement of its mission and for engendering the trust of the American people and visitors to our nation.

We operationalize privacy at the outset of DHS program initiation through two primary means. First, the Privacy Office works to incorporate privacy in the development processes used to build DHS information systems. Second, the Privacy Office confirms that privacy is embedded in the information systems that involve personal data through the privacy assessment process. These two methods allow the Privacy Office to "bake" privacy into Departmental operations.

Building privacy into the development process starts with the investment review processes for major programs and information systems at the Department. In partnership with the DHS Management Directorate, the Privacy Office participates on three separate committees that review project proposals and set performance criteria for program and technology investment budget approvals. We thus can use the "power of the purse" to ensure that program personnel are attentive to privacy requirements.

The Privacy Office then works to operationalize privacy protections through "privacy gateways" that focus on the projected design and use of an information technology system. In collaboration with the Office of the Chief Information Officer, the Privacy Office is developing these "privacy gateways" for the systems development life cycle review of technology deployed for Departmental programs to ensure that privacy practices are integrated through a monitored and auditable process.

Consequently, Department design and deployment initiatives move forward only after proper attention has been paid not only to operational issues, but also to privacy issues. In fact, privacy is considered a cornerstone of the Department's program architecture, consistent with the mandate to protect the homeland while preserving essential liberties.

Once funding for an information system is determined and privacy is considered in the systems development life cycle, the Privacy Office monitors privacy compliance through the use of a Privacy Impact Assessment (PIA). Conducting PIAs demonstrates the Department's efforts to assess the privacy impact of utilizing new or significantly changing information systems, including attention to mitigating privacy risks. Touching on the breadth of privacy issues, PIAs allow the examination of the privacy questions that may surround a program or system's collection of information, as well as, the system's overall development and deployment.

When worked on early in the development process, PIAs provide an opportunity for program managers and system owners to build privacy protections into a program or system in the beginning. This avoids forcing the protections in at the end of the developmental cycle when remedies can be more difficult and costly to implement. In accordance with Section 208 of the *E-Government Act of 2002* and OMB's implementing guidance, the Department of Homeland Security is required to perform PIAs whenever it procures new information technology systems or substantially modifies existing systems that contain personal information. The Chief Privacy Officer reviews and signs off on all Departmental PIAs and then they are published.

Although the *E-Government Act* allows exceptions from the PIA requirement for national security systems, as a matter of good privacy practice, the Privacy Office requires that all DHS systems, including national security systems, undergo a PIA if they contain personal information. We use the PIA process as a good government information management tool and privacy protective process across the Department's programs. In cases where the publication of the PIA would be detrimental to national security, the PIA document may not be published or may be published in redacted form. This means that information systems that are part of the Intelligence Enterprise at the Department undertake these important analyses to ensure that privacy considerations are fully integrated. Our intelligence information systems are better considered and developed as a result of conducting PIAs.

Transparency and Accountability

To assure that information in DHS record systems is handled in a manner consistent with the fair information practices principles set out in the Privacy Act of 1974, the Privacy Office carefully reviews new Systems of Records Notices and new initiatives that seek to collect information to be placed under existing SORNs. The Privacy Office works closely with the Office of the General Counsel on the legal issues attendant to these SORNs and with all DHS program offices to analyze the ways in which the information will be shared through approved routine uses. In addition to SORNs, we benchmark programs' compliance with fair information practices principles based upon their development and adherence to internal policies, procedures, and public statements of program goals. To that end, we are working on a privacy tool that will assist programs in doing periodic self assessments against similar measures.

Another way the Privacy Office encourages transparency and accountability is through outreach and public workshops. Just yesterday, the Privacy Office hosted a public event concerning *Transparency and Accountability: The Use of Personal Information within the Government.* We explored the front end of the privacy process—how public notices inform the public of the intended use of personal information by government—and the back end of the process—how government can live up to the promises made in public notices through mechanisms for appropriate access, including through *Privacy Act* disclosures, *Freedom of Information Act* disclosures, and other appropriate means.

Privacy Audits and Reviews

The Privacy Office also has an important oversight function within the Department in assessing whether the fair information practices embedded in the *Privacy Act of 1974* are appropriately implemented in our programs, along with other relevant frameworks. We do this through privacy audits and providing guidance at points along the development of programs. While the Privacy Office has an important internal role, it also receives and reports on complaints and concerns from the public about the privacy attentiveness of DHS programs. In response, we undertake reviews of those concerns and report on them to the Secretary and to Congress, per Section 222 of the *Homeland Security Act,* providing constructive guidance.

Privacy Protection and Public Security through Information Sharing and Intelligence

The Department of Homeland Security was created, in significant part, to foster information sharing for homeland security purposes. And from its beginning, the Department has undertaken the important work of removing the invisible barriers that block appropriate information flows within the Department. The *Privacy Act,* of course, provides the statutory authority for intra-agency information sharing when there is a need to know, and Privacy Office policy supports the exchange of information between the Department's component organizations whenever the organizations establish an appropriate need based on an express purpose. The Privacy Office, therefore, works with Department components to facilitate the exchange of information in a privacy sensitive manner, while working toward the goal of the right persons getting the right information at the right time.

The Department must also foster external information sharing for homeland security purposes with all of our partners at the Federal, state, local, tribal and private sector levels. As the Department incorporates the "need to share," in its information sharing design it is, of course, paramount that privacy be built into the process. Our work on internal information sharing complements and informs the Department and Privacy Office's efforts to assist with external information sharing efforts.

Just as the sharing model has changed, so must the paradigm shift to enhanced, stronger, and embedded privacy protections because, as Secretary Chertoff has said, "When we share information, if we do it in a disciplined way, we actually elevate the security of both those who share—and those who receive—the information." The Privacy Office has therefore worked diligently to help create an information sharing model that allows for robust information exchanges for homeland security purposes even while it fosters robust privacy protections.

In particular, we have worked collaboratively with our Intelligence and Analysis colleagues, for whom information sharing is part of their critical mission, to ensure that personally identifiable information of U.S. persons is treated in a manner that fully conforms with their rights and is handled sensitively. The DHS policy on handling U.S. person information developed by the Intelligence and Analysis section of DHS contains a significant role for the DHS Privacy Officer to review activities that could involve a potential violation of the privacy rights of U.S. citizens and also requires the Privacy Officer to collaborate on new initiatives to ensure that they enhance and do not erode privacy protections relating to the collection, use and main-

tenance of personal information. This policy is another example of the way that the Privacy Office has helped to construct a culture of privacy at DHS and has worked to make privacy an operational imperative as we move forward with our mission.

Related to these activities is the fact that over the past four years, the Administration has provided new tools to permit federal agencies to exchange information. Most recently, in Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans,* which was issued on October 25, 2005, the President made clear his intent that all federal agencies work to prepare an environment in which information flows support counterterrorism functions. The Executive Order specifically recognizes the importance of protecting the "freedom, information privacy, and other legal rights of Americans." This message is further reflected in the *Presidential Memorandum* of December 16, 2005, to all federal departments and agencies providing guidelines and specific requirements to build the new Information Sharing Environment.

As part of this Memorandum, the President issued Guideline 5 stating that "the Federal Government has a solemn obligation, and must continue fully, to protect. . .the information privacy rights and other legal rights of Americans. . ." in the building of an information sharing environment.

In parallel with the President's efforts, Congress enacted three laws providing the U.S. Government with greater authority for collecting, analyzing, and disseminating terrorist information: the *USA PATRIOT Act of 2001,* the *Homeland Security Act of 2002,* and the Intelligence *Reform and Terrorism Prevention Act of 2004* (IRTPA). This last statute puts in place a mechanism to formalize the creation of the information sharing environment on an interagency level and it, too, provides that the privacy rights of individuals must be central to the environment's creation.

"Need to Share" and the Role of the DHS Privacy Office

Recent legislative enactments confirm what the National Commission on Terrorist Attacks Upon the United States recommended and that the President has required in his Executive Orders on information sharing, that we have moved from a "need to know" environment to a "need to share" environment. This "need to share" presents significant improvements to information exchange, but it also presents significant challenges to individual expectations for privacy and to institutional privacy safeguards. At the Department of Homeland Security, as we move forward in our ability to share data, we are aware of our responsibility for the privacy, security and authorized use of the data entrusted to us.

Specifically, technology and information policy should be maximized to build privacy protections into data sharing models. But technology and privacy awareness, while important tools in protecting individual privacy interests, will not be enough to address current challenges. As we move forward, we will also need to establish and enforce concrete safeguards to prevent unauthorized access, use, or disclosure.

The Privacy Office has provided expertise and guidance for building the ISE by working closely with the Information Sharing Environment Program Manager (ISE/PM) and various steering groups on issues not only dealing directly with privacy, but also with subjects such as governance, operations, and harmonization of technologies. Through these efforts, the Privacy Office is assisting with facilitating the incorporation of privacy protections at the roots of the ISE development.

Currently, the Privacy Office is a member of an interagency working group, operating under the joint leadership of the Director of National Intelligence and the Department of Justice, as specified by the President under Guideline 5. This group will conduct a review of current executive department and agency information sharing policies and procedures regarding the protection of information privacy and other legal rights of Americans; and develop guidelines designed to be implemented by executive departments and agencies to ensure that the information privacy and other legal rights of Americans are protected in the development and use of the ISE, including in the acquisition, access, use, and storage of personally identifiable information.

The review of policies is focusing on coordinating and consolidating the work already done to focus on the key issues to harmonizing privacy protections. This review will lead into the development of appropriate guidelines that will outline a process for the operation of the entire ISE.

Conclusion

The Privacy Office will continue to work to ensure that privacy is woven into the very fabric of the Department as a guiding principle and value through operationalizing privacy throughout the Department and responding to privacy concerns about information sharing environments in positive, constructive ways.

In addition, as the Acting Chief Privacy Officer of DHS, I endeavor at all times to keep an open door to the privacy community around the nation and the world

to ensure that the Department benefits from the range and depth of privacy practitioners and concerned citizens everywhere.

We face great challenges. But we must achieve both security and privacy and, with both, sustain our values and freedoms. I do not doubt that we can move forward together and achieve our mission of protecting and preserving our lives and our way of life, preserving our Liberty and with it, our privacy. I appreciate the opportunity to testify before this important committee today. I look forward to hearing the other witnesses' testimony and to answering your questions.

Mr. SIMMONS. Thank you very much for that testimony.

I have a couple of questions, and then we will defer to the members of the subcommittee for their questions.

Do you believe the Privacy Office has the support and the backing of DHS senior leadership and, in particular, leadership in the intelligence component in order to effectively fulfill your mission?

Ms. COONEY. Thank you for the question, Mr. Chairman.

Yes, absolutely. I do feel that we have always had the support since the time that I joined the Department of Homeland Security under both Secretary Ridge and now Secretary Chertoff, both of our secretaries.

And the reason I am concentrating on that is because in any organization, in privacy matters or any compliance and enforcement matters, you need leadership from the top in order to embed it within the culture of the organization.

Both of our secretaries have been extremely supportive. They have been supportive of our privacy officers, of the more than 400 employees who work on Privacy Acts and Freedom of Information Acts issues every day in the department. And, in particular, if I might say, our intelligence partners have always been very supportive.

I know that General Hughes is here today testifying. He was a wonderful partner during his tenure at the department. And Mr. Allen could not be more supportive and his staff.

Mr. SIMMONS. The issue of privacy frequently comes up in the context of collection activities. The Department of Homeland Security generally speaks of acquiring or gathering information which presumably they obtain from other agencies who also have their own privacy officers and presumably abide by their own privacy regulations. But the Department of Homeland Security might also collect information, for example, at the border or during a Coast Guard intercept.

How do you deal with that kind of activity to ensure that the right to privacy is protected in the collection activities of the your own organization?

Ms. COONEY. I would say broadly, and particularly with the components that you are mentioning—border security, which would be customs and border protection, or if it is TSA, or immigration and customs enforcement—each of those particular entities under the DHS umbrella have very specific standards and processes that they use in collecting information.

And a major part of that is compliance with the Privacy Act of 1974, which, as is true with any federal agency, requires that an agency only collects information that is mission critical, information that assists us in carrying out our particular duties as government employees.

We review in the Privacy Office in collaboration with those component agencies those policies and procedures and in particular, do privacy audits on those collection mechanisms.

Mr. SIMMONS. I thank you. My time has expired.

The chair recognizes the gentleman from Mississippi.

Mr. THOMPSON. Thank you very much, Mr. Chairman.

Ms. Cooney, for the record, do you have subpoena power or anything with your office in collecting data?

Ms. COONEY. No, Congressman Thompson, we don't.

Mr. THOMPSON. Have you felt that you could do your work—have you had any problems getting data?

Ms. COONEY. Initially, with one of our complaint reviews—that is one of our responsibilities—we did have some difficulty in getting full information within the department. I will say, since that initial experience, I am not aware of difficulty in that area.

If I may, in my 20 years of federal service, a good part of that has been in compliance and enforcement work. And it is not unusual that you ask for information even under a subpoena. And people think they are being fully compliant and are not, and you ask again, and you say, "Anything else?," and they give you more.

We are diligent and persistent in our activities even without some type of authority that you are mentioning. And within the government, that is standard process, and I assume that our staff will always be persistent in carrying out our compliance responsibilities.

Mr. THOMPSON. Do you have the ability to take sworn testimony?

Ms. COONEY. We do not, sir.

Mr. THOMPSON. Would that help you?

Ms. COONEY. In certain cases, it could be helpful. I think it would be—what I would say on that is, as we partner in the agency in other areas, we do have partners within the agency who have that ability, particularly the inspector general.

With one of our major reviews, we did partner with the inspector general and referred part of our conclusion to the inspector general for his further review. He had the ability to use subpoena power to take sworn statements. To the extent that that works effectively in the absence of powers on our own, we would certainly leverage every opportunity in the department to make sure there is full compliance with all privacy laws.

Mr. THOMPSON. So if you had the ability to subpoena witnesses for information or the ability to take affidavits, would that enhance your ability as chief privacy officer to function?

Ms. COONEY. I know that our department—well, let me say it this way: It could. It might be helpful. To date, I guess I would say, again, to date, I don't think that we have seen that we have not received the information that we have needed in order to carry out our abilities.

Sometimes issues that I look at—and I am a lawyer, but I don't practice as a lawyer in the agency. I practice as a policymaker. But as a lawyer, thinking through that background, I would always want to be careful in our taking statements of not jeopardizing a case that someone else in another area of the department has authority for, which is why I think at least to date, it is important in the absence of having subpoena powers or the ability to take af-

fidavits, to be mindful that in the pursuit of our own activities, we need to be careful to partner with people who may need to follow up on an investigation.

Mr. THOMPSON. Well, I understand that. But I am trying to be respectful of your office and try to figure out other than friendly persuasion what real authority do you have to actually get the information.

Ms. COONEY. I would say our greatest assistance in getting the information that we have needed is leadership from the secretary's office, from the secretary himself. It was true under Secretary Ridge, and it was true very recently in a review that we did under Secretary Chertoff, not unlike the type of leadership buy-in that you need in a corporation. And that is what we have relied on.

Mr. THOMPSON. So in absence of authority to do your job, you depend on leadership persuasion from the top?

Ms. COONEY. Absolutely. We need their support in doing our job just as our colleagues do in theirs.

Mr. THOMPSON. So can you initiate an investigation on your own?

Ms. COONEY. Yes, we do do that, absolutely.

Mr. THOMPSON. Without any leadership from the top? You have sole authority?

Ms. COONEY. That is right. We inform the secretary, as would be responsible, and then we pursue our responsibilities under the statute, under Section 222, that requires us to look at complaints and concerns about agency programs and processes. Yes, sir.

Mr. THOMPSON. Thank you, Mr. Chairman. My time is expired.

Mr. SIMMONS. I thank the gentleman for his questions.

The gentleman from Pennsylvania, Mr. Dent, is recognized.

Mr. DENT. Thank you, Mr. Chairman.

Good morning.

Ms. COONEY. Good morning.

Mr. DENT. Do you believe that the department is doing an effective job in protecting the privacy of American citizens?

Ms. COONEY. Yes, Mr. Dent. I do believe we are. We are certainly trying very hard. I can tell you that the staff of the Privacy Office works extremely diligently, very long hours, is a very energetic staff, and that we have built various active partnerships across the department.

I think all through our processes, from investment review, to life cycle development reviews of technologies that the department might deploy in programs, to our privacy impact assessments when programs are getting ready to be developed, and all through that developmental process, to the audit reviews afterwards, and then on reviews of complaints, I think we are being extremely proactive.

I might add, we have an internal DHS data and privacy integrity board made up of senior managers, in particular, guidance that we are trying to fashion on the use of commercial reseller data. That particular internal board will meet next week to collaborate with us and to have a dynamic discussion on how operationally guidance might work and be implemented.

We also have an external privacy advisory committee that gives advice directly to the secretary and to the chief privacy officer. They have looked most recently at the information sharing issues that relate to intelligence information that we handle at the de-

partment and that we need to push out both to the private sector and state and local partners.

So we certainly are trying in as many venues and as many ways as possible to effectively push out privacy and privacy attentiveness within the department.

Mr. DENT. And my final question. Do any of the information sharing systems within the DHS Intelligence Enterprise require privacy impact assessment or PIA as required by the E-Government Act of 2002? And can you give us an example of PIAs that have been done with regards to the DHS Intelligence Enterprise?

Ms. COONEY. Yes. I am happy to do that. Most recently, we have worked on a privacy impact assessment that deals with our Homeland Security Information Network. We refer to it as HSIN. It is a network database that is managed by our Homeland Security operations center.

But, of course, much of the information that is within that database is brought in and analyzed by our intelligence analysis area as well as others. Much of it is information from citizens who happen to see suspicious activity and can call into the department. It includes information from our law enforcement components, our folks on the line every day protecting the borders.

We have recently worked on that privacy impact assessment. It is publicly available on our web site on the Privacy Office web site.

As I mentioned before, when these privacy impact assessments concern what might be considered national security operations, they don't necessarily require publication, but we work very hard at transparency of DHS operations. And so on that particular PIA, we worked diligently with HSOP and with I&A to fashion the PIA in a way that we could describe as robustly as possible exactly what information we are collecting and how we are handling it.

It is in the name of activity information rather than information about individuals. However, there is some information that comes into that database that concerns individuals. And to the extent that it is personally identifiable information, there are added safeguards and restrictions, roll-based access, in terms of who gets to see that information and when.

Mr. DENT. Thank you. I yield back.

Mr. SIMMONS. I thank the gentleman.

The gentlelady from Florida, Ms. Brown–Waite, is recognized.

Ms. BROWN-WAITE. Thank you very much, Mr. Chairman.

Ms. Cooney, you have a very, very impressive resume, and this question may have been asked before. I apologize if it was. Please don't hesitate to tell me.

But as I looked at your resume, your title is chief privacy officer, the acting chief privacy officer. Do you think that your duties are impaired any way by the title of acting, and do you have any idea when the acting with all the responsibilities will become the actual privacy officer, chief privacy officer?

Ms. COONEY. Thank you for your question.

Since taking this position, my philosophy has been that it is just business as usual within the Privacy Office and the department in terms of fully integrating privacy into our operations. So the title itself, I don't think, has made a significant difference for me in the

way in which I go about this job, nor in the way in which senior leadership has partnered with me to be effective in that job.

We cannot do this alone in the privacy office. This is an enterprise-wide value and initiative to protect privacy at the department. So I have not seen an impediment based on my acting position, and I am happy to continue to serve in this role as long as the secretary asks me to do so.

Ms. BROWN-WAITE. My next question is: Do you think that the Privacy Office has the adequate resources and funding to actually carry out the mission of the office?

Ms. COONEY. Well, I would first answer that by thanking members of Congress for your support in building our budget from the time that we were in our infancy when we had three FTEs and a budget of $750,000 to the 15 FTEs that we have now and about an equal number of very experienced privacy contractors who are embedded and made part of our privacy team, and the budget we have now of $4.3 million.

The exercise of pushing privacy out through the enterprise, of course, has also grown as the department and as we have multiplied our homeland security programs. We will need to continue to watch that as those programs grow, but we continue to leverage our ability to effectuate privacy by capitalizing on privacy officers that are in our component agencies, our major programs—U.S. VISIT, Citizen and Immigration Services, Transportation and Security Administration, and Cyber Security, as well as the more than 400 privacy professionals who I mentioned to you are embedded within the department.

Ms. BROWN-WAITE. What is the average longevity of the 16 full-time employees that you now have? Or did it just increase with last year's funding?

Ms. COONEY. We have gradually increased each year that we have been in operation. We had been at 12 FTEs, and we received four new ones in the 2006 budget. We have filled one of those. We are actively interviewing for two other of those spots, and the fourth position has been posted.

Under our former chief privacy officer, Nuala O'Connor Kelly, and together, we felt that that was imperative that whatever tools and resources Congress gave us, we would immediately use them. And we are actively doing that. So it has been incremental over the years.

Ms. BROWN-WAITE. Well, obviously, it takes a very special kind of person to fill this, and I would just encourage you don't fill it just for filling's sake. Go out there and get the best and the brightest.

Ms. COONEY. Thank you. We will do our very best to do that.

Ms. BROWN-WAITE. Thank you very much, and keep up the good job.

Ms. COONEY. Thank you.

Mr. SIMMONS. I thank the gentlelady for her comments.

Are there any additional comments or questions that members may wish to make?

Ms. Cooney, thank you very much for your testimony. It is great to have you here. You have responded very well. I think you shouldn't be acting anymore. I think you should be permanent. And

what we always say is, if there are any budgetary or legislative impediments to performing your duties that you will make the subcommittee aware of those. Thank you.

And now the chair will call the second panel.

Ms. COONEY. Thank you.

Mr. SIMMONS. The second panel consists of Mr. Keith Herath—I hope I am pronouncing your name correctly—chief privacy officer and associate general counsel at Nationwide Insurance Company, who is primarily responsible for creating and implementing privacy policy. Mr. Herath is currently serving a 2-year term on the DHS Data Privacy and Integrity Advisory Committee.

Mr. Jonathan Turley, Shapiro Profess of Public Interest Law at the George Washington University Law School. He is a nationally recognized legal scholar. In 1990, Professor Turley joined the George Washington law faculty, and in 1998 became the youngest chaired professor in the school's history.

And Lieutenant General Patrick Hughes, who is vice president of Homeland Security at L–3 Communications and has over 38 years of strategic planning and leadership experience. Prior to joining L–3 Communications, General Hughes was assistant secretary for information analysis at the U.S. Department of Homeland Security, a position he held from 2003 to 2005.

Thank you all for being here.

General Hughes, in particular, to you, welcome back. It is good to see you here.

And the chair now recognizes Mr. Herath to testify.

STATEMENT OF KIRK HERATH, CHIEF PRIVACY OFFICER, AVP-ASSOCIATE GENERAL COUNSEL, NATIONAWIDE INSURANCE COMPANIES

Mr. HERATH. Thank you. Good morning, Mr. Chairman, and members of the subcommittee. Thank you for the opportunity to speak with you today.

My name is Kirk Herath. I am the chief privacy officer, associate general counsel and assistant vice president for Nationwide Insurance Companies located in Columbus, Ohio. I am also currently serving as the president of the International Association of Privacy Professionals. In addition, I serve as a member of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee.

I would like it noted that the opinions expressed here today are mine alone and do not reflect those of any other person or organization.

Privacy is a vibrant and growing profession. Privacy is recognized by the private sector, and increasingly in the public sector and academia, as an important and integral part of an organization's success.

The job of a privacy professional demands mastery of a complex set of laws technology, security standards, and program management techniques. In many ways, the emergence and growth of the International Association of Privacy Professionals reflects the growing importance of privacy in public and private sectors.

Privacy protections within the government and marketplace require professionals to assess, create, monitor, and maintain policies

and practices. The IAPP was founded 5 short years ago, and in that time, it now has 2,200 members in over 23 countries.

Clearly, the profession of privacy has cemented its position as a critical resource in any organization that deals with data. Privacy professionals within DHS play an important role in furthering our nation's twin goal in protecting its citizens' security and their rights.

Most of us in the private sector discovered that the sheer scale of implementing privacy and safeguard requirements required a central office to coordinate the implementation of one corporate privacy policy that comply with a new set of emerging laws.

The federal government appears to be coming to the same conclusion. A central office is needed to coordinate privacy for a large government agency.

One can find many resources about how to create a privacy program. However, the steps in creating a privacy program can be summed up in the following: You first assess, you assess current processes, procedures, uses of data, et cetera. You then address, which is to identify and address gaps in your process and procedures. You monitor and audit to make sure that everything you put in place is working as it should, and then you repeat this process, because the environment is constantly changing.

There are many challenges with implementing privacy. With every assessment or audit, there are three competing factors vying for the most beneficial outcome. These include the business need for quick access to abundant amounts of personal information. Information is money. The business cannot succeed without person information. For DHS, information may lead to greater security.

Customer expectation is number two. The customer wants the product or service that they purchased or contracted for. The customer also has high expectations for how they want companies or organizations to manage and use their information.

And third, privacy regulations. Like all regulations, they serve a good purpose. However, they often conflict with organizational goals.

The job of a privacy officer is to help balance these three competing interests, because in the end, it rarely happens that each of the three competing interests is exactly equal. Generally, they are different.

Listing the challenges that arise when implementing privacy is easy. Resolving them takes time and resources and the power to effectuate the necessary change. It is a constant balancing act often with different outcomes each time an issue arises.

The DHS Privacy Office's mission is to minimize the impact on the individual's privacy, particularly the individual's personal information and dignity, while also achieving the mission of the Department of Homeland Security.

One wonders whether the DHS Privacy Office has the budget staff and institutional authority to adequately carry out its mission. In fact, the DHS Privacy Office has done a wonderful job working with the limited resources made available to it. They have done many of these assessments of existing programs and appear to be integrated in the planning and review processes for future

programs or programs under development. They have addressed most of the gaps discovered through their initial assessments.

Where they can probably use the most assistance and resources is with operating their ongoing monitoring and audit function. This function is in its infancy and is inadequately staffed. Even if it were adequately staffed, it is doubtful that the Privacy Office has the legal authority to conduct the type of deep analysis necessary to ensure ongoing adherence to privacy laws.

In sum, the Privacy Office is well organized and understands what it needs to do to carry out its objectives. It is highly motivated and experienced. Nevertheless, there are a few things Congress should consider to make it more successful.

I respectfully submit the following: Number one, strengthen the statutory authority of the Privacy Office. It should have a clear and direct reporting line to Congress. The DHS Privacy Office should have a larger budget to carry out its critical mission. Its current $4.3 million budget is insufficient in light of the DHS's overall budget.

Congress should consider adding chief privacy officers and privacy offices to all federal agencies or at least those that generally collect and process personal information on citizens.

Transparency in information processing is fundamental to the role that the Privacy Office plays. The Freedom of Information Act Office needs to stay connected to the Privacy Office, because this is the Privacy Office's single real connection to its customers, namely citizens.

DHS should quickly appoint an official replacement for Nuala O'Connor Kelly, who left many months ago. Not having an official replacement devalues the Privacy Office politically and organizationally.

In conclusion, I hope my testimony helps illustrate the large effort, cost and authority necessary for an organization to effectively implement a Privacy Office. For the DHS Privacy Office to carry out its statutorily defined requirements, it will need resources and the authority to implement a privacy program that balances the requirements of law and a responsibility of the government to protect its citizens.

Additionally, no Privacy Office can be successful without clear and strong support from the top. If support from leadership is absent, the privacy function will never be able to effectively carry out its mission. In fact, trying to perform a privacy function without senior leadership support may be worse than not doing anything with privacy, because it provides an illusion to privacy without the reality of having any in.

Thank you for inviting me to speak with you this morning. I would be happy to answer any questions that the committee may have.

[The statement of Mr. Herath follows:]

PREPARED STATEMENT OF KIRK M. HERATH

APRIL 6, 2006

Introduction

Mr. Chairman, members of the Subcommittee good morning. Thank you for opportunity to speak with you this morning.

My name is Kirk Herath, I am the Chief Privacy Officer, Associate Vice President, and Associate General Counsel for Nationwide Insurance Companies, located in Columbus, Ohio. I am also currently serving as President of the International Association of Privacy Professionals (IAPP), the world's largest association for the privacy field, representing over 2,000 privacy professionals in business, government, and academia from 23 countries. Additionally, I serve as a member of the Department of Homeland Security's (DHS) Data Privacy and Integrity Advisory Committee, which advises the Secretary of the Department of Homeland Security and the DHS Chief Privacy Officer on privacy and data integrity issues related to personal information.

I would like it noted that I am here today in a personal capacity as an expert in privacy and privacy compliance. I am not here today officially representing my employer, my professional association or the Data Privacy and Integrity Advisory Committee. Thus, the opinions expressed here are mine alone and do not reflect those of any other person or organization.

This morning, I will explain to the Committee how privacy has become imbedded into most private and a growing number of public organizations and how, in fact, it has become a legitimate profession and career path for thousands of knowledge workers. I also will attempt to describe for the Committee the very basic steps any organization needs to go through to address privacy and build a privacy infrastructure. Following this description, I will compare and contrast the role that the DHS Privacy Office plays to what any other privacy office would do, whether it is private or public sector, particularly the trade-offs and balancing that is required to be successful. Finally, I will also respectfully attempt to provide a brief set of recommendations for the Committee to consider if it desires to ensure more consistent privacy protections for DHS, or for any federal agency that collects and processes personal information.

The Profession and Business of Privacy

Before I describe how privacy programs should be organized and compare that to the DHS Privacy Office, I would like to discuss profession of privacy and the work of the IAPP. I believe that this will provide a good framework for the Subcommittee to see how Privacy is a vibrant and growing profession. In sum, privacy is recognized by the private sector, and increasingly in the public sector and academia, as an important and integral part of an organization's success. The growth of the IAPP reflects this view. The IAPP is a rapidly growing professional association that represents individual members working in the field of privacy. The organization works to define and promote this nascent profession through education, networking, and certification.

In many ways, the emergence and growth of the IAPP reflects the growing importance of privacy in public and private sectors. Privacy protections within the government and marketplace require professionals to assess, create, monitor, and maintain policies and practices. Put simply: privacy professionals are needed to give privacy protections viability within any organization.

The IAPP was founded five short years ago as an emerging network of privacy professionals recognized the need for a professional association. The organization has grown rapidly since those early days and now boasts over 2200 members in 23 countries. The IAPP's recent annual conference here in Washington was, to the best of my knowledge, one of the largest privacy conferences ever held, with over 800 attendees. Clearly, the market has placed a very high value on privacy and the robust, but responsible use of data.

When the IAPP was initially formed, the majority of our members shared a similar title: chief privacy officer, or CPO. Indeed, many—if not most—Fortune 500 companies have now appointed a chief privacy officer. But the majority of IAPP members are not CPOs. Rather, we have seen a robust hierarchy of professional roles in privacy emerge—in both the privacy and the public sectors. These privacy pros cover issues of compliance, product development, marketing, security, human resources, consumer response, and more. The management of privacy issues in large organizations now requires a broad and deep team of professionals with increasingly sophisticated skills. It is a hybrid profession encompassing a broad set of skills. Some organizations have even created job families for their privacy professionals. It is now a career track.

The job of a privacy professional demands mastery of a complex set of laws, technology, security standards, and program management techniques. In 2004, the IAPP introduced the first broad-based privacy certification to the US marketplace, the Certified Information Privacy Professional (CIPP). This credential is meant to serve as a demonstration of a candidate's knowledge of a broad range of fundamental pri-

vacy concepts. To date, over 800 people have taken the exam and over 600 CIPPs have been granted in the US.

In 2005, the IAPP extended the CIPP program to include issues of governmental privacy. The CIPP/G program covers issues specific to the public sector: such as the Privacy Act, eGovernment Act, Freedom of Information Act, Patriot Act, and more. To date, the IAPP has granted over 70 CIPP/Gs. The IAPP expects more growth in this sector, due to the growing importance of privacy in the public sector. This hearing reinforces that view.

Clearly, the profession of privacy has cemented its position as a critical resource in any organization that deals with data—whether that data is consumer or citizen data, or both. Privacy professionals within DHS and the few other government agencies that have privacy offices play an important role in further our nation's twin goal of protecting its citizen's security and their rights.

I encourage members of the committee to visit the IAPP's website, *www.privacyassociation.org,* to learn more about the profession of privacy. And, as a CIPP/G myself, I strongly recommend that the committee consider the value of such privacy certifications as a tool to ensure privacy issues are properly identified and addressed in the public and private sectors.

Operationalizing Privacy within an Organization—An Example

One of the reasons Chairman Simmons invited me today was to provide the Committee with a brief overview of the process private sector companies undergo to implement an effective privacy program. I believe that the steps taken by private sector companies take to protect the privacy of personal information can easily be extrapolated to the public sector. To the best of my knowledge, these were essentially the same steps that the DHS Privacy Office completed in order to provide the same privacy protection that individuals have come to expect from all entities that collect, use, and share their personal information.

I will use my own experience with Nationwide to describe for the Committee the basic steps necessary for any organization—either public or private—to implement and continue to manage its privacy responsibilities. Explaining how privacy has been adopted in the private sector will help illustrate the steps—including opportunities and challenges—necessary to effectively carry out a privacy program.

First, let me give you a brief overview of Nationwide. Nationwide is a fortune 100 company comprised of several dozen different companies and divisions that sell a variety of products—from auto, home, and commercial insurance to mortgages to financial products—such as annuities and investment funds, to retirement plans—such as 401k and 457 plans. Nationwide employees over 30,000 employees and has an exclusive sales force of just over 4,000 agents. It also sells its products and services through tens of thousands of independent agents, producers and brokers. Despite a complex organization, we have a legal duty to safeguard our customer information and protect their data wherever it is stored, accessed or shared. This can be a daunting task without a good plan and organization.

Nationwide began centrally managing privacy as Congress was putting the finishing touches on the Gramm-Leach-Bliley Act (GLBA) in late 1999. As you may know, GLBA requires financial institutions, including banks and insurance companies, to inform customers in an annual privacy statement how the company uses, protects, and shares customers nonpublic personal information. GLBA also requires that financial institutions safeguard customer information. It's not enough for a company just to tell a customer that it is "protecting your nonpublic personal information" or that "access to your information is limited to employees who have a business need-to-know your information." A company must have the processes and technological controls in place to veritably support the privacy statement.

Prior to GLBA, each entity of Nationwide managed compliance with state privacy laws—mainly some version of the 1982 Model National Association of Insurance Commissioners (NAIC) Privacy Act—independently in the 16 states where some version of this model had been enacted into law. To the extent possible, each company or division managed privacy practices differently. As you can imagine, this created a patchwork effect with respect to privacy. Each company and division adopted different privacy standards and practices. Even the philosophy of privacy varied between companies, with some companies following a very high standard for privacy and others following a standard that was the minimum necessary to comply with the law. Senior management had not articulated a uniform privacy policy and spread this policy throughout the organization, companies and divisions. In sum, there was no consistent guidance on privacy. To be fair, this situation existed because there was no single set of national privacy laws that applied equally to every entity, and there was no real enforcement mechanism.

For the private sector, this all changed when Congress enacted the Gramm-Leach-Bliley Act in November 1999. Among other requirements, the GLBA effectively forced companies to centralize privacy management and compliance. The sheer scale of implementing the privacy and safeguard requirements of GLBA required a centrally coordinated office to coordinate the implementation of one corporate privacy policy that complied with the new set of laws. I was assigned the role of advising Nationwide executive leadership on a privacy policy and compliance plan and then, with their agreement and approval with this privacy policy and plan, to implement GLBA requirements throughout all Nationwide companies and divisions.

GLBA and other federal and state privacy laws have had a positive effect on customers and citizens. A good example of this is that DHS probably would not have hired the first statutorily-required privacy officer in the federal government, Nuala O'Conner Kelly, if not directed to do so by law. Customers and citizens have come to expect that entities that use, share, or disclose their personal information should protect this information and should use, share, or disclose it appropriately. The federal government appears to be coming to the same conclusion: a central office is needed to coordinate privacy for any large government agency, perhaps one is even needed to coordinate "among" the federal agencies, but I will address that later.

The Four Basic Steps of a Privacy Program

One can find several books and a plethora of articles today about how to create a privacy program. Most of these are good descriptions that go into each area in great detail and are worthwhile reading. However, the steps in creating a privacy program can be summed up in the following manner. To implement a privacy program, any company or agency needs to follow a seemingly simple four step model:

1. Assess,
2. Address,
3. Monitor and Audit,
4. Repeat.

Step One—Assess

The goal in step one is to conduct dozens and dozens of assessments. The best way to carry out this task is to create a large cross-functional team. For example, in my case, I formed what we called a Virtual Privacy Team (VPT) that included about 40 people from across our corporation. Each Nationwide company or division had representation on the VPT. These team members in turn lead their own business unit or staff office privacy compliance team, which varied in size and scope, within each of the companies or divisions. By my estimation—by using this model, we were able to centrally manage and coordinate the activities of over 500 employees actively working on our corporate privacy implementation during 2000-2001, which was the high water compliance year of us, as we worked to comply with strict legal and regulatory time lines.

Basically, the objective in the first step in implementing privacy in an organization is to assess current processes, procedures, uses of data, etc. Any organization going through this process needs to conduct, among others, the following assessments:

1. Analysis of the legal requirements.
    a. What federal or state privacy laws exist that affect the organization?
    b. What were the specific requirements for each privacy law?
    c. How were companies and divisions complying with these patchwork of regulations?
2. Evaluation of existing privacy standards, practices, and philosophies.
3. Evaluation of information security practices.
    a. Does Nationwide have an information security policy?
    b. Does it meet the standards of the Safeguard Rule (the companion information security regulation within GLBA)?
    c. Collection of personal information.
    d. Which areas of Nationwide are collecting personal information?
    e. What type of information is being collected?
    f. Why is this type of information being collected (purpose)?
    g. Where is it stored?
    h. Is Nationwide only collecting personal information necessary to complete the customer's request?
4. Collection of Personal Information.
    a. Which areas of Nationwide are collecting personal information?
    b. What types of information is being collected?
    c. Why is this type of information being collected (purpose)?
    d. Where is it stored?

e. Is Nationwide only collecting personal information necessary to complete the customer's request?

5. Use of Personal Information.
   a. How is information being use?
   b. What is it being used to accomplish for the organization?
   c. Is there a legal or rational basis for each use of information?
6. Access to Personal Information.
   a. Who can access personal information?
   b. Does everyone with access have a business need-to-know the information?
   c. Is access monitored?
   d. Are employees technologically capable of accessing personal information that they should not be able to access?
7. Disclosure of Personal Information
   a. How is personal information shared within Nationwide?
   b. Are the principles of need-to-know enforced?
   c. Do these disclosures have a legal basis?
8. Disclosure of Personal Information with Third Parties.
   a. Does a contract exist with all third parties that receive Nationwide information?
   b. Have we conducted an information security audit to determine whether the third party is capable of adhering to the laws that require the information to be protected?
9. Data Integrity
   a. Is the data accurate and up-to-date?
   b. Is there a way for customers to access their data and valid correct errors?
10. Management
   a. What documentation or privacy procedures exist?
   b. Is it up-to-date, accurate, and sufficient for the company of division?
   c. Does it need to change to satisfy the new law?
   d. Can it be extrapolated to the rest of the organization as a best practice?
   e. Is there anyone responsible for complying with laws and regulations?

After going through the first assessment, which formed our legal analysis of privacy, the VPT in conjunction with a steering committee that I chaired drafted a privacy policy for Nationwide and a privacy statement detailing our privacy policy for our customers. The privacy policy was then adopted by a steering committee of senior Nationwide executives. This became the privacy philosophy that the VPT adhered to when implementing privacy across all Nationwide companies and divisions. It was the foundation upon which we have built our program over these past six years.

Step Two—Assess

Over an 18-month period, as these different assessments were completed, the VPT concurrently analyzed the results and determined how they fit with the overarching privacy policy. We then addressed the key question of whether the results of the assessment were sufficient or did they need modifications to match the newly drafted privacy policy? This is the hallmark of step two, which is identify and address gaps in your processes and procedures.

In step two, the VPT and small number of outside consultants conducted gap analyses between the legal requirements, the new Nationwide Privacy Policy and the results of the different assessments. For example, number nine in the assessment list, above, was Disclosure of Personal Information with Third Parties. To address this assessment, the VPT member worked with the team responsible for executing contracts in each company or division to evaluate the findings in the assessment against the legal requirements and Nationwide's Privacy Policy. In some cases, they discovered that they could not find a copy of a contract, or that a written contract didn't exist. Many contracts did not contain the new confidentiality, privacy, and information security, language required by the GLBA. These teams identified the gaps and developed a plan to address the gaps identified.

The VPT then created project plans to address the gaps. Let's use an assessment from earlier—Access to Personal Information. One of the items of the assessment was an illustration of how personal information flowed through a company or division. This assessment included where the personal information was stored and which associates could access it.

The privacy sub-team then documented the tasks necessary to address the gap between the assessment and both the legal requirements and Nationwide Privacy Policy. The next step was to develop a project plan to assign the activities for each task and to monitor the progress.

Step Three—Monitor and Audit

After the dozens and dozens of projects to address the identified gaps were finished, we created a privacy compliance program to audit the privacy procedures that the teams implemented. For practical reasons, this program was created and housed in the Office of Privacy, because it contained the evolving set of experienced professionals capable of carrying out these tasks.

There are several purposes to the audit phase of privacy implementation. One purpose is to confirm that the privacy processes are still operating. Sometimes, when the novelty of a project fades, employees inadvertently regress back to old practices. Also, employees often change jobs and the institutional memory leaves the unit. Monitoring through self-assessment or more formal audits keep compliance issues fresh and illustrate actual privacy practices to business leaders.

Another purpose of continuous monitoring or auditing is to determine whether a compliance process change is necessary as a result of a new business process. Business is a constantly changing environment. Audits help discover when new privacy processes are necessary to meet these new changes.

Finally, informal monitoring and audits prepare companies for formal market conduct audits by regulators. Regularly conducting internal audits allows business to understand and address privacy risks before a regulator conducts an audit. This reduces the risk of regulatory enforcement and fines.

Step Four—Repeat

Privacy implementation never ends. Thus, the four step process is really a continuous improvement loop. This has been extremely important over the past six years, as each year the private sector has been faced with an ever expanding array of legislative and regulatory requirements around privacy and information security. In addition to the changing legal landscape, a company is required to repeat the process to accommodate new business goals or changes to existing processes.

In summary, this may be an overly simplistic explanation of the complex process of implementing privacy throughout any organization—public or private. However, I believe that it correctly points out the nature of the process and is easy to understand. There is one other important item to note here. None of this is possible without a clear mandate and strong support from the top of the organization. If the privacy office lacks the support of the chief executive, whether this is a private or public organization, it will never be able to effectively carry out its mission. A privacy office without senior management support may be worse than not having a privacy office, because it merely provides an illusion of privacy without the reality.

The Challenges—Balancing Competing Interests

Earlier, I discuss the requirement for financial institutions to create a privacy statement, which describes how the company uses, protects, and shares customer information. It is difficult for a large company like Nationwide to make blanket promises to customers, because there are many competing priorities when it comes to privacy. This is no different for the DHS Privacy Office.

The challenges that arise while implementing privacy at Nationwide became apparent immediately. In business, information is money. At Nationwide, the more a division knows about an individual, the better the company can protect the financial needs of the individual. However, certain laws or contractual obligations between parties often make it difficult to "know" everything about a customer. It is equally true in both the private and public sectors.

Let me give you an example of how this can impact a company:

Susan works for a municipality and has a 457 deferred compensation plan with Nationwide that she obtained through her employer—a municipal government—whose relationship is with an independent producer under contract to Nationwide. Susan also has a Nationwide Insurance Agent through whom she purchased auto and homeowners insurance. Susan trusts her Agent to help her protect her financial assets—specifically, her house and her car. One day, Susan visits her agent and says that she has accepted a new job with a private company and is moving to a new city. Based on this scenario, one can see that Susan has at least three financial needs:

1. Change her auto insurance to a new state;
2. Change her homeowners insurance to the new state and residence;
3. Consider options for the assets in her 457 plan.

Today, the Agent can help Susan with the first two of her three financial needs. It would help Susan the most if the Agent could also look up the details of her 457 plan and provide this information to a licensed Nationwide broker to help Susan understand options for getting the most out of her 457 plan after she moves to a new job. But, for a variety of legal reasons, the outcomes of privacy implementation at Nationwide prevent this from occurring. The Agent does not have access to—nor

does he even have knowledge of—Susan's 457 plan information and, thus, he cannot help her consider options after she changes jobs.

I bring up this simple example to illustrate the challenges with implementing privacy. With every assessment, task to address a gap, or audit, there are three competing factors vying for the most beneficial outcome from their perspective. These include:

1. The business need for quick access to abundant amounts of personal information. Remember, information is money. The business cannot succeed without personal information.
2. The customer expectation. The customer wants the product or service that purchased or contracted for. The customer also has high expectations for how they want companies to manage and use their information. In short, they want it locked in a vault stronger than Fort Knox. But at the same time, they want Nationwide to be able to access it via phone, e-mail, Internet, or Agent 24 hours a day, seven days a week. They also expect to be provided additional products or services that can either save them or make them money. These are in and of themselves other competing interests for companies to manage.
3. The privacy regulations. Like all regulations, they serve a good purpose, in this case: protect individual investors or insured. But, they also come with unintended consequences, just like Susan's example from above.

As you can see, the job of a Privacy Officer is to help balance these three competing interests, like a carpenter of a three-legged stool. Picture a three-legged stool. The benefit of having three legs instead of four is that each leg can be a slightly different length, yet the stool will still function as a stool, even if it is a little lopsided. Because, in the end, it rarely happens that each leg of the stool—each of the three competing interests—is exactly equal. Generally, they are different. Sometimes, the privacy regulation is a bit longer, meaning the most important interest in a given business project. Other times, the interest of the customer or the business is given a slightly greater importance. But, the stool still functions as a stool.

This is no different for the DHS Office of Privacy. Ms. Cooney, her predecessor and those who will follow her, has also been asked to become a carpenter of a three-legged stool. But, in the DHS Privacy Office's case, the three competing interests are:

1. Government's responsibility for security, including responsibilities under the Homeland Security Act, the Aviation and Border Security Acts, and others
2. Individual privacy expectations;
3. The Privacy Office's responsibilities under Section 222 of the HAS, the Privacy Act, the Freedom of Information Act, and other competing and compatible privacy laws.

Listing the challenges that arise when implementing privacy is easy; resolving them takes time and resources and the power to effectuate the necessary change. It is a constant balancing act often with different outcomes each time an issue arises. It is hard to argue that the DHS Privacy Office is not faced with tremendous challenges in this area, as they balance the nation's collective security interests against the individual's interest in privacy.

A Very Brief Analysis of the DHS Privacy Office

Now, compare and contrast the process that I have just described to the DHS' Privacy Office: assess, address, audit, and repeat. All four steps must be tailored to government processes and then followed in the DHS for the Privacy Office to meet the requirements set forth by the Homeland Security Act, the Privacy Act, and several other laws regulating the government's use of personally identifiable data. Consider also the discussion about balancing important competing interests within an organization.

As you know, the Homeland Security Act (HSA) of 2002 authorized the formation of the Department of Homeland Security and the addition of a secretary to the president's cabinet to oversee the new department. Among other things, the Homeland Security Act also provides that the Secretary "shall appoint a senior official in the Department to assume primary responsibility for privacy policy, including:

(1) assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information;
(2) assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974;
(3) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government;

(4) conducting a privacy impact assessment of proposed rules of the Department or that of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected; and (5) preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of the Privacy Act of 1974, internal controls, and other matters."

To operationalize its legislative mandate, the DHS Privacy Office developed a Mission Statement that states the mission of the DHS privacy office is to minimize the impact on the individual's privacy, particularly the individual's personal information and dignity, while achieving the mission of the Department of Homeland Security." The mission goes on to state—and I am summarizing here—that the Privacy Office will achieve this goal through:

1. education and outreach efforts to infuse a culture of privacy across the department,
2. communicating with individuals impacted by DHS programs to learn more about the impact of DHS policies and programs, and,
3. Encouraging and demanding adherence to privacy laws.

Anyone who reads this Mission can see that the DHS Privacy Office is faced with the exactly same opportunities and challenges that any privacy office, including mine, faces every day—but on a much, much larger scale, and with a completely different risk dynamic. At Nationwide, my office is responsible for educating employees and establishing a culture of privacy, resolving the natural conflicts that occur with business interests in regard to this concept of privacy, and requiring adherence to privacy laws. There would appear to be little difference between my mission and the mission of the DHS Privacy Office.

Nevertheless, one wonders whether the *DHS Privacy Office has the budget, staff and institutional authority to adequately carry out its mission.* I will address some of these concerns in my recommendations and considerations below. In fact, the DHS Privacy Office has done a wonderful job working with the limited resources made available to it. They have done many of the assessments of existing DHS programs and appear to be integrated into the planning and review processes for future programs or programs under development. They have addressed most of the gaps discovered through their initial assessments. They also have a nascent employee privacy education component, although it lacks adequate funding. Where they could probably use the most assistance and resources is with operating their ongoing monitoring and audit function. This function is in its infancy and is inadequately staffed. Even if it were adequately staffed, it is doubtful that the Privacy Office has the legal authority to conduct the type of deep analysis necessary to ensure ongoing adherence to privacy laws. This incongruity is addressed further under my recommendations, below.

In sum, the Privacy Office is well organized and understands what it needs to do to carry out to meet its objectives. Its staff is highly motivated and experienced. However, they may lack support from the top and they clearly lack the financial resources necessary to effectively do the job Congress directed them to perform through Section 222 of the HSA.

Recommendations and Items for Consideration

While there are always risk assessments and balancing tests between privacy and other interests that must occur whether one is working in a public or private sector privacy capacity, there are still a few things that Congress should consider to make it more likely that our nation's privacy laws are not violated. Therefore, I respectfully submit the following for the Committee to consider as it defines its future agenda:

1. Strengthen the Statutory Authority of the DHS Privacy Office. The Privacy Office should have a clear and direct reporting line to Congress. If Congress is uncomfortable with Inspector General-like powers, then consider taking a half-measure and give the Privacy Office ombudsman-like power. Burying the office inside DHS means that it will never have the authority or respect it needs to carry out its mandate. The Privacy Office will rarely be able to act independently, and it will spend more time merely trying to survive politically than it will carrying out its mission to protect our citizens' privacy.
2. The DHS Privacy Office should have a larger budget to carry out its critical mission. The current $4.3 million budget does not on its face appear sufficient in light of DHS' overall budget to protect the privacy of all Americans. The difference between this year and last year's budget is only an increase of a few hundred dollars. I would doubt that any other area of DHS saw this paltry of an increase in its budget.

3. Congress should consider adding Chief Privacy Officers and Privacy Offices to all federal agencies, or at least those that generally collect and process personal information on citizens. Congress may even want to consider creating a Federal Data Commissioner, similar in authority and scope to those existing in the nations of the European Union. The Data Commissioner could either be the first among equals, or it could be the overarching policymaking body for enforcing all federal data processing. This body would have inspector general powers.
4. Transparency in information processing is fundamental to the role that the Privacy Office plays. The Freedom of Information Act Office needs to stay connected to the Privacy Office, because this is the Privacy Office's single real connection to its customers, namely U.S. citizens. One of the hallmarks of fair information practices is the ability of citizens or customers to know what information an entity has on them and have the ability to correct any erroneous information. This is simple due process and improves the integrity and accuracy of any organization's data. This role is naturally played the Privacy Office.
5. DHS should quickly appoint an official replacement for Nuala O'Connor Kelly, who left many months ago. The Acting Privacy Officer, Maureen Cooney, is doing a very capable job and should be seriously considered as the official replacement. However, the optics of not having an official replacement devalues the Privacy Office politically and organizationally. It indicates the job being capably performed by the staff may not be seen as worthy by senior department and administration officials as other areas in DHS and this undercuts the Privacy Office's authority.

Conclusion

I hope that my testimony helped illustrate the large effort, cost, and authority necessary for a corporation to effectively implement a privacy office. In order for the DHS Office of Privacy to effectively carryout its statute-defined requirements, it will need resources and the authority to implement a privacy program that balances the requirements of law, the responsibility of the government to protect its citizens, and the individual right of privacy.

Additionally, as I stated above, no privacy office can be successful without clear and strong support from the top. If support from the chief executive is absent, the privacy function will never be able to effectively carry out its mission. In fact, trying to perform a privacy function without senior management support may be worse than not doing anything with privacy, because it provides an illusion of privacy without the reality of having any.

Thank you for inviting me to speak with you this morning. I would be happy to answer any questions that you may have. I would also be more than happy to speak with you again or to work with you and your staff on any privacy issue.

Mr. SIMMONS. Thank you very much.

And now the chair recognizes Professor Turley.

We have your statement in the record this morning. If you can summarize in 5 minutes, that would be appreciated. And we look forward to hearing what you have to say.

STATEMENT OF JONATHAN TURLEY, SHAPIRO PROFESSOR OF PUBLIC INTEREST LAW, GEORGE WASHINGTON LAW SCHOOL

Mr. TURLEY. Thank you, Mr. Chairman. I will do my very best.

Mr. SIMMONS. If I could just say, I had a seminar at Yale that was 2 hours, but since I have come to Congress, my colleagues have not allowed me to take that amount of time.

Mr. TURLEY. A most enlightened institution for that reason.

Mr. Chairman, members of subcommittee, thank you very much for allowing me to speak on this important issue today of privacy and Homeland Security. And, of course, they are not separate issues. When we talk about Homeland Security, it is privacy that we are protecting. It is one of our core values. It defines us as a people.

Now, the DHS represents, for privacy advocates like myself, something of a concern just by its mere size and the myriad of functions that it has taken on. Due to its size and those functions,

it has a much greater impact on privacy. It affects the lives of Americans more than any other agency, because it is the agency of first contact for most Americans when it comes to airports and immigration and customs and disaster relief. So to the extent that DHS does not respect the privacy interest, it has the greatest impact upon citizens.

The other problem and concern for the DHS for many privacy advocates is that it is much like a governmental iceberg, that even though you see the DHS or at least its counterparts in your daily life, 90 percent of the agency remains below the surface, and so there is a lack of transparency. And privacy is often protected by the fact of transparency in government, the greater transparency, the greater protection of privacy because it tends to deter misconduct, and you don't have the abuses at all rather than having to chase them down through oversight committees.

Now, of course, privacy is protected in the Constitution. It is protected by various statutes, and for much of our history, it was protected by practical limitations. Probably the greatest protection of privacy was that the government could not engage in surveillance of a large number of people at one time.

In the last two decades, we have seen that technological barrier fall as we saw with DARPA and the TIA program. We now have the ability to follow Americans in real time. That is something the framers would never have anticipated, and it is why privacy is very much under threat.

The greatest concern for privacy is uncertainty, that is uncertainty is the scourge of privacy. Privacy is based upon an inception that your privacy will be recognized. To the extent that you are uncertain, you have a chilling effect, and that affects how people live their lives. And DHS recently was found to have one of the lowest privacy scores in a 2006 study.

I have gone through the myriad examples of threats to privacy that relate to DHS, but much of my testimony deals with the NSA operation. Now the problem with the NSA operation is really twofold.

One—and let me put this as simply as I can—it is based on a crime. Now, the overwhelming majority of experts in this field—Republicans and Democrats—are pretty uniform in this conclusion. It is inescapable.

There is an exclusivity provision in federal law. You cannot do what the president ordered his subordinates to do. If I thought that this was a close question, I think I have a reputation of going right down the middle on questions that are debatable. This is a crime. It was ordered 30 times by the president, and he stated that he will continue to order it.

It gives me no pleasure to say that. And I am not talking about his motivation. But often, people act for the best motivations with the worst possible means.

My testimony lays out why this is a criminal act, and that presents a serious problem for DHS. I do believe this committee has jurisdiction over this question. This committee has a liaison function with intelligence agencies. It governs intelligence information gathering that relate to DHS entities. It has a role in intel; it looks

at the role of intel in threat prioritization in its oversight function. It is the recipient of information.

After post–9/11, there is a mandate that agencies share information. The expectation is that Homeland Security is either the direct or indirect recipient of NSA information. That creates, not just the danger of DHS officials participating in a criminal enterprise, but it creates the specter of the fruit of the poisonous tree where activities of DHS may be undermined because of their reliance on unlawfully gathered information.

I know that my time is out, but I have listed towards the end of my testimony various proposals that can help protect privacy. But there is one that I just wish to emphasize. All of us, I believe, as Americans, have a faith in privacy. We know how important it is. I know the chairman has valued that. We have discussed that. But we cannot remain silent, because silence is a choice.

The NSA operation represents a serious threat to privacy and a serious threat to our constitutional values. And I hope that this committee will assert its authority—I know the chairman has attempted to do so—but will be vigorous in asserting its authority to hold hearings on the NSA operation and not to be deterred by any past refusals.

Thank you so much, sir.

[The statement of Mr. Turley follows:]

PREPARED STATEMENT OF PROFESSOR JONATHAN TURLEY

Chairman Simmons, Representative Lofgren, members of the Subcommittee, thank you for allowing me to appear today to testify on the important issues of privacy and homeland security.

I come to this subject with prior work as both an academic and a litigator in the areas of national security and constitutional law. As an academic, I have written extensively on electronic surveillance as well as constitutional and national security issues. I also teach constitutional law, constitutional criminal procedure and other subjects that relate to this area. As a litigator, I have handled a variety of national security cases, including espionage and terrorism cases. I am appearing today, however, in my academic capacity to address important issues related to domestic surveillance and homeland security.

I. GENERAL PRIVACY CONCERNS RAISED BY POST 9-11 SURVEILLANCE AND ENFORCEMENT.

The Department of Homeland Security (DHS) is the agency with the greatest ability to erode privacy since it has the dominant role, with the Federal Bureau of Investigation (FBI), in domestic enforcement activities. Due to its size and diverse functions, the DHS has a much greater impact on privacy than any other agency. The DHS affects the lives of Americans to a far greater extent than most agencies because it has a far greater number of contacts with citizens in their everyday lives from airport security to disaster relief to immigration to customs. The DHS is not just a massive agency, it is a massive consumer of information from other agencies, state governments, private contractors, and private citizens. While the FBI is subject to criminal procedures and routine court tests, DHS is like a government iceberg with ninety percent of its work below the visible surface. This general lack of transparency makes it easier for abuses to occur by reducing the risk of public disclosure and review.

At risk is something that defines and distinguishes this country. Privacy is one of the touchstones of the American culture and jurisprudence. Indeed, it is a right that is the foundation for other rights that range from freedom of speech to freedom of association to freedom of religion. The very sanctity of a family depends on the guarantee of privacy and related protections from government interference.

Privacy is protected by the Constitution, including but not limited to the protections afforded by the Fourth Amendment. It is also protected in various statutes, such as the Privacy Act of 1974; E-Government Act of 2002, and the Federal Information Security Management Act of 2002 (FISMA). Further protections can be

found in the substantive and procedural requirements of surveillance laws such as Title III and the Foreign Intelligence Surveillance Act (FISA).

Finally, there have long been practical protections of privacy. Until recent technological advances, there were practical barriers for the government to be able to conduct widespread surveillance on citizens. However, it is now possible to track citizens in real time with the use of advanced computers as recently made clear by the disturbing Terrorism Information Awareness (TIA) project of Defense Advanced Research Projects Agency (DARPA). These new technological advances constitute an unprecedented threat to privacy. Agencies like DHS often naturally gravitate to the accumulation of greater and greater information. Technology now allows these agencies to satiate that desire to a degree that would have been unthinkable only a couple of decades ago.

Despite these protections, privacy remains the most fragile and perishable of our fundamental rights. When pitted against claims of national security, privacy is often treated as an abstraction and government officials offer little more than rhetorical acknowledgement of privacy concerns in their programs and policies. The resulting uncertainty is the very scourge of privacy. Privacy depends on a certain expectation of citizens that they are not being watched or intercepted. When uncertain of the government's effect that inhibits the exercise of free speech and other rights.

The uncertainty over privacy is clear in recent polls and studies. Notably, the DHS receives one of the lowest scores on the privacy question. The 2006 Privacy Trust Study of the Ponemon Institute gave the DHS only a 17 percent score, down by 10 percent from the previous year.

This freefall is more than a public relations problem. Our constitutional test for privacy under the Fourth Amendment is based on "the reasonable expectation of privacy" under the *Katz* doctrine. To the extent that a citizen has a reasonable expectation of privacy, the government is usually required to satisfy a higher burden, including the use of a warrant for searches. The *Katz* test has now created a certain perverse incentive for government. As agencies like DHS reduce that expectation of privacy in the public, it actually increases the ability of the government to act without protections like warrants. The result is a downward spiral as reduced expectations of privacy lead to increased government authority which lead to further reduced expectations.

Privacy concerns after 9-11 have grown with each year in the war on terror. There is a pervasive view that the Administration is wielding unchecked and, in some cases, unlawful authority in the war on terror. In areas that range from enemy combatant detentions to warrantless domestic surveillance programs to data mining of private records, the chilling effect for privacy and civil liberties has become positively glacial for many citizens, particularly citizens of the Muslim faith or Middle Eastern descent.

Just in the last few months, Congress has faced a remarkably wide range of issues that directly threaten privacy rights and civil liberties. It is regrettably a long and lengthening list. Today, in the interests of time, I wanted to focus on a few of the most recent controversies to show how privacy rights and civil liberties are eroded by the aggregation of otherwise disparate and insular programs. While these examples may appear unrelated, they each impact privacy rights and civil liberties in significant ways. The point that I wish to convey is that privacy is being undermined in a myriad of ways and that any effort to protect this right will have to be equally comprehensive.

a. The Failure to Comply with Privacy Standards, including the Use of Reseller Information That Lack Fair Information Practices. As shown recently by the GAO, the DHS is using an increasing amount of data from information resellers that lack critical protections and fair information practices. The recent misuse of 100 million personal records in alleged violation of the Privacy Act typifies this concern.

b. Over-classification and Reclassification Efforts. The Administration has led a serious rollback in the efforts to gain greater transparency in government by over-classifying and reclassifying basic documents and information. Agencies like DHS can prevent disclosure of misconduct or negligence by using classification rules to avoid review.

c. Registered Traveler Programs. The DHS continues to encourage the creation of registered traveler programs that would assemble a databank of prescreened passengers. Whether run privately or governmentally, these programs offer illusory security but present serious threats to civil liberties.

d. Failure to inform Congress of Surveillance Programs like the NSA operation. One of the greatest protections of civil liberties is the separation of powers doctrine and its inherent system of checks and balances. The failure to inform the members of Congress, particularly the full committee membership

of the intelligence committee, of ongoing intelligence activities negates any meaningful oversight functions.

e. New Threats Against Whistleblowers. Legislation to increase penalties for federal whistleblowers is a startling reaction to the disclosure of unlawful activity. This is exemplified by the proposed increase in penalties for officials seeking to disclose unlawful activity under the NSA domestic surveillance program. Likewise, the continued refusal of Congress to pass a federal shield law for journalists can only be seen as an intentional deterrent for whistleblowers. When an official at DHS is aware of an unlawful program, the media may be the only effective way to stop the illegality.

These are a few of the most recent examples of how privacy rights and civil liberties protections are being pummeled across a long spectrum of insular governmental policies and programs. If Congress truly wants to protect privacy, it must deter threats by increasing both the likelihood of disclosure of unlawful conduct and the penalties for such conduct. This requires greater transparency in agencies like the DHS, better oversight in Congress, and fuller protection for those who seek to disclose misconduct.

II. THE NSA DOMESTIC SURVEILLANCE PROGRAM

The recent NSA operation brings together many of the most dangerous elements discussed above: lack of congressional oversight, the violation of federal law, the pursuit of whistleblowers, and finally the absence of any meaningful action from Congress. In terms of privacy rights, the NSA operation also presents the most serious attack on the guarantees that are essential for the exercise of the full panoply of rights in the United States.

The disclosure of the National Security Agency's (NSA) domestic spying operation on December 16, 2005 has created a constitutional crisis of immense proportions for our country. Once a few threshold, and frankly meritless arguments of legality are stripped away, we are left with a claim of presidential authority to violate or circumvent federal law whenever a president deems it to be in the nation's security interests. As I made clear in a January hearing, these claims lack any limiting principle in a system based on shared and limited government. It is antithetical to the very premise of our constitutional system and values.

This is, of course, not the first time that President Bush or his advisers have claimed presidential authority to trump federal law. In its infamous August 1, 2002 "Torture Memo," the Justice Department wrote that President Bush's declaration of a war on terrorism could "render moot federal law barring torture." The Justice Department argued that the enforcement of a statute against the President's wishes on torture "would represent an unconstitutional infringement of the president's authority to conduct war."

The President also assumed unlimited powers in his enemy combatant policy, where he claimed the right to unilaterally strip a citizen of his constitutional rights (including his access to counsel and the courts) and hold him indefinitely.

On December 30, 2005, President Bush again claimed authority to trump federal law in signing Title X of the FY 2006 Department of Defense Appropriations Act. That bill included language outlawing "cruel, inhumane or degrading treatment" of detainees, such as "waterboarding", the pouring of water over the face of a bound prisoner to induce a choking or drowning reflex. In a signing statement, President Bush reserved the right to violate the federal law when he considered it to be in the nation's interest.

The NSA operation, however, is far more serious because the President is claiming not just the authority to engage in surveillance directly prohibited under federal law, but to do so domestically where constitutional protections are most stringent. The scope of this claimed authority is candidly explained in the Attorney General's recent whitepaper, "Legal Authorities Supporting the Activities of the National Security Agency Described by the President." As I noted in the prior hearing, it is a document remarkable not only in its sweeping claims of authority but its conspicuous lack of legal authority to support those claims. It is also remarkably close to the arguments contained in the discredited Torture Memo.

The vast majority of experts in this field have concluded that the NSA program is unlawful. Even stalwart Republican members and commentators have rejected its legality. It is an inescapable conclusion. Under Section 1809, FISA states that it is only unlawful to conduct "electronic surveillance under color of law except as authorized by statute." The court in *United States v. Andonian,* 735 F.Supp. 1469 (C.D. Cal. 1990), noted that Congress enacted FISA to "sew up the perceived loopholes through which the President had been able to avoid the warrant requirement."

FISA does allow for exceptions to be utilized in exigent or emergency situations. Under Section 1802, the Attorney General may authorize warrantless surveillance

for a year with a certification that the interception is exclusively between foreign powers or entirely on foreign property and that "there is no substantial likelihood that the surveillance will acquire the contents of any communications to which a United States person is a party."

No such certification is known to have occurred in this operation. Nor was there an authorization under Section 1805(f) for warrantless surveillance up to 72 hours under emergency conditions. Finally, there was no claim of conducting warrantless surveillance for 15 calendar days after a declaration of war, under Section 1811.

The NSA operation was never approved by Congress. Moreover, the Administration's attempts to use the Authorization for Use of Military Force, Pub. L. 107–40, 115 Stat. 224 (2001), as such authorization is beyond incredible, it is unfathomable.With no exceptions under the Act, the NSA operation clearly conducted interceptions covered by the Act without securing legal authority in violation of Section 1809.

The NSA operation is based on a federal crime ordered by the President not once but at least 30 times. Indeed, in his latest State of the Union Address, President Bush pledged to continue to order this unlawful surveillance. A violation of Section 1809 is "punishable by a fine of not more than $10,000 or imprisonment for not more than five years, or both." Likewise, an institutional defendant can face even larger fines and, under Section 1810, citizens can sue officials civilly with daily damages for such operations.

The DHS is likely a recipient—directly or indirectly—of the information gathered under this unlawful program. In my view, government officials participating in this program are participating in an ongoing criminal enterprise. The DHS officials have an independent obligation to determine if this program is lawful and to refuse to participate on any level with the program if it is viewed as unlawful. This includes the receipt or use of intelligence. Moreover, to the extent that federal courts determine that this operation is unlawful, the incorporation of the intelligence in DHS investigations or enforcement may ultimately result in undermining those activities. Under a classic "fruit of the poisonous tree" theory, the use of this tainted intelligence can taint any information gathered as a result of its use.

Putting aside the questions of criminality, the NSA operation jeopardizes basic privacy guarantees. First, it shows an unchecked and unilateral exercise of presidential authority. Second, the conspicuous absence of congressional oversight has destroyed any faith in a legislative check on such authority. Finally, it created uncertainty for citizens as to their guarantees of privacy and civil liberties under this program or other undisclosed programs.

III. WHAT CAN BE DONE?

Just as there are a myriad of threats to privacy, there are a myriad of possible measures to protect privacy interests. The most significant protections often come in the form of protecting those who would reveal violations while deterring those who would commit the violations. Such reforms include the following:

a. Investigation of the NSA domestic surveillance program with public hearings.

b. Strengthening of whistleblower protections, particularly for employees at defense, intelligence, and homeland security agencies.

c. Strengthening laws on data mining and data sharing by agencies, including meaningful deterrents for agencies like DHS that violate the Privacy Act and other statutory protections.

d. Reverse the trend toward reclassification and over-classification of documents that decreases the transparency of government by enacting new avenues to challenges overbroad assertions of classified status.

e. The Congress should prohibit not simply a government-run registered traveler system but a private-run system. The DHS support for a pilot program in Orlando should be ended by barring the expenditure of any federal funds and prohibiting the incorporation of such a program into TSA airport security systems.

f. Congress should require compliance with conferral rules on all intelligence operations (other than covert activities) so that all members of the intelligence committees are informed of operations like NSA's domestic surveillance program.

g. A new system of privacy officers should be established so that every major office in agencies like DHS have a privacy officer who will be responsible for training, enforcing, and certifying compliance with federal privacy laws.

h. Enhancing the authority and funding for the DHS Privacy Officer. While Congress created this position in the Homeland Security Act of 2002, there is a widespread view that the privacy officer needs greater authority and access as well as more resources to police the programs of this massive agency. The

slow response of the DHS to establish this office indicates a lack of internal support of the model of an independent internal watchdog office. For this reason, changes should include a reporting requirement not only to the DHS but directly to Congress.

i. Congress should pass a federal shield law for journalists, as has virtually every state. Increasing legal threats for journalists, including contempt rulings, presents an obvious deterrent to any whistleblower seeking to disclose unlawful conduct.

j. Congress should require an annual report, with regular public hearings, on privacy matters to identify emerging threats to privacy and possible legislative solutions.

IV. CONCLUSION

These threats to privacy rights and civil liberties have created not just a constitutional crisis but a test for every citizen. Our legal legacy was secured at great cost but it can be lost by the simple failure to act. The President is right: these are dangerous times for our constitutional system. However, it is often the case that our greatest threats come from within. Indeed, Justice Brandeis warned the nation to remain alert to the encroachments of men of zeal in such times:

> Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasions of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachments by men of zeal, well-meaning but without understanding.

Citizens, let alone congressional members, cannot engage in the dangerous delusion that they can remain silent and thus remain uncommitted in this crisis. Remaining silent is a choice; it is a choice that will be weighed not just by politics but by history.

Thank you for the opportunity to speak with you today and I would be happy to answer any questions that you might have at this time.

Mr. SIMMONS. And thank you very much for that testimony. We very much appreciate that.

General Hughes, welcome back, and we look forward to your testimony.

LIEUTENANT GENERAL PATRICK HUGHES, USA (RET.), VICE PRESIDENT OF HOMELAND SECURITY, L–3 COMMUNICATIONS

General HUGHES. Well, thank you. As you said, my testimony is contained in my written input. I appreciate the chance to appear before you today.

I would like to express my views in a very simple form rapidly. I believe in protected rights of all persons in the United States expressed in law, including, certainly, the right to privacy.

Within the law, I think we are compelled under the conditions we now live in to collect information, analyze it, and produce utility information to perform the mission of protecting our nation and our citizens and residents.

In the process of acquiring and providing information for this utility, we must discover and preclude terrorism. We simply cannot afford to have terrorist acts of the kind that we know could occur here in the United States.

I also am mindful that much of the work of the Department of Homeland Security is focused on other crimes, crimes that are not terrorist in nature but are associated perhaps and are crimes of national security implications.

So much of what they do and what we expect from them as citizens has to do with criminal acts under the law as currently constituted.

The use of this acquired information is important. It must be used legally to discover these acts or this plan and conspiracy

ahead of time in an attempt to preclude it. And that is really a very difficult goal under the complicated conditions that we now heard about from testimony this morning and that you know so very well, because you have lived there.

I don't think I am qualified to offer exact recommendations within constitutional law or within civil law and criminal law in this country, but I am a person who has practiced the effort to do this work here in the United States and overseas, and we must find some balance between protecting the rights of our citizens and our residents and countering the planned and indeed engaged acts of terrorists and criminals which do threaten our security, and in some cases, perhaps, our existence as we know it.

Thank you very much.

[The statement of General Hughes follows:]

PREPARED STATEMENT OF PATRICK M. HUGHES

APRIL 6, 2006

Representative Simmons, Representative Lofgren, Members of the Sub-Committee on Intelligence, Information Sharing and Terrorism Risk Assessment:

Thank you for the invitation to appear before you on the subject of "Protection of Privacy in the DHS Intelligence Enterprise." I am appearing today as a private United States citizen, although it is noteworthy that from November 2003 until March 2005, during the early formative and developmental stages of the Department of Homeland Security, I was the Assistant Secretary for Information Analysis in the Information Analysis and Infrastructure Protection Directorate of DHS. Since then I have continued my interest and work in matters dealing with homeland security, homeland defense and intelligence related to homeland security on both professional and personal levels. Prior to this period I served for more than 35 years in the US Army and from 1999 until 2003 as a private consultant to both government and industry.

Because of this background I was asked to come here to give my views on issues that relate to the protection of privacy and really the protection and assurance of legal and procedural rights of Americans in the context of intelligence gathering and production of information that can be acted upon by those who work to protect the lives and property of our citizens. This "operationalization" of intelligence—especially where it concerns persons who are residents of the US, including those who have full rights of citizenship, is vital to understanding my views. We have all learned, through bitter experience that we must seek to interdict, to preclude, to stop—impending acts of terrorism, before they occur, because that is the right thing to do. It is an imperative of all who serve our nation. In this modern era of the potential for the application of weapons with mass effects, we simply cannot afford to allow the commission of terrorism because we cannot bear the price and we cannot afford the consequences.

Indeed, the toll that crime with homeland security implications takes on our social order each day, and the results of catastrophic disasters—which we have recently suffered through on a scale not experienced before—also affect my view of what we should protect and what we should abrogate when human beings become involved in these events. As we look to the future—in my view—we can anticipate the worsening of these conditions.

My views have been formed in the crucible of combating the Viet Cong Infrastructure in Vietnam; in seeking to discover acts of espionage and subterfuge during the Cold war; in ferreting out the meaning of North Korean activities; in engaging in the smaller but vexing conflicts of recent years, including the hunt for War criminals and insurgent groups in Bosnia, our attempts to decipher the tribal groups of Somalia, and our best efforts to break the erosive conditions found in places like Panama and Haiti. My views, like yours, have been formed in the crucible of 9-11 and in the conditions and events of the post-9-11 period in which many terrorist attacks and crimes with homeland security impact have occurred albeit primarily overseas. Here too—we must anticipate the future. New threats are on the horizon.

My views are simple—yet found in the very complex context of today's problems and circumstances.

My view is that we must engage in the collection of necessary information about persons of concern in order to discover conspiracy and intent that should be—that must be—interdicted in order to forestall an unacceptable condition, under the law.

If we fail to interdict we must act in a similar fashion to understand that which we failed to stop and to know with certainty who or what was responsible for the event—so that we can learn and so that we can attribute both blame and appropriate action in light of that blame.

My view is that we should not violate the rights of American citizens in engaging in such activities, but rather that we should seek a legal finding of necessity under the law as rapidly as possible—before we abrogate any rights for the greater good.

My view is that we must create a mechanism that provides for very rapid response (minutes to hours) to the legal tests of suspicion and probable cause to engage in both information collection and operational action—before the passage of time and the changing of circumstances results in the loss of our opportunity to act to prevent a catastrophe.

My view is that we must provide for a degree of information collection, analysis, storage and production necessary to support analysis and operational decisions. Without this functional ability we cannot do the job. This capability—of necessity—must include intelligence, law enforcement, judicial organizations, the military and elements of governance and must be empowered through a form of secure interoperability that protects the security of the information and the rights of the persons involved.

My view is that the government should have the right to compel any person—no matter who they are or what their legal status is—to provide dependable assured identification to appropriate authorities in appropriate conditions, like travel via mass transportation conveyances. Similarly we should have the right to compel the full disclosure of materials and items that are being transferred within, through and across our borders, on one's person, in luggage, and in cargo—no matter what the nature of those materials and items are.

We should have a viable mechanism that requires—not requests—that information be provided when citizen concern about activities they note reaches a level of compelling reaction. In this age we cannot sit idly by and not report that which seems to us to be suspicious or illegal, especially in the context of homeland security and homeland defense. Conversely we should not tolerate reports of a frivolous nature, or those based solely on contentious relationships and interpersonal disagreements.

Finally, we should protect large gatherings and public venues with appropriate sensory technologies and dependable observation. Surely the answer, in the aftermath of a future terrorist event, cannot be that we failed to secure a specific place or condition because of privacy concerns.

In many cases this set of personal beliefs and views on my part—my "opinions" if you will—are hardly new or revolutionary. They are—in my view—basic and evolutionary. They form the foundation for a set of laws and procedures that will protect the rights of our residents, our citizens and will help to protect and secure our Republic. I do not advocate excessive restriction nor do I advocate trampling on the rights of our people. Rather I counsel that we should find a set of laws and procedures that meet our needs—in the context of demonstrated threats and future conditions we can anticipate—and put those laws and procedures into force.

I know this is difficult to do. I also recognize the highly politicized environment in which we are interacting today. As a fellow citizen I simply hope for some balance between doing that which is right and necessary to protect our people and property on our own soil, and not doing that which violates the expectation of privacy and personal freedom that each person is entitled to under the law.

My goal is to secure a peaceful and safe progressive existence for our nation.

Mr. SIMMONS. I thank all three witnesses for their excellent testimony.

And I think, General Hughes, you stated very explicitly the conundrum that we face as Americans on the one hand, providing for common defense is an essential responsibility of the federal government. The Preamble to the Constitution also says that we must establish justice. The First and Fourth Amendment rights are clear to all of us. And so in a situation where we are involved with threats, yes, we want to collect actionable intelligence, but at the same time, we don't want to violate the rights of innocent citizens. And so this is the challenge of the balancing act.

Now, General Hughes, you served as the heart of I&A, Intelligence and Analysis in the Department of Homeland Security. Is that correct? That is my recollection. Different name.

General HUGHES. The same office but a different name.

Mr. SIMMONS. Yes.

General HUGHES. The office has been enhanced by greater independence.

Mr. SIMMONS. It would seem to me that in your capacity as head of that, the Intelligence and Analysis Office, you would receive intelligence products from other agencies—the CIA, the National Security Agency, Defense Intelligence Agency, NRO, et cetera, et cetera. You would receive those products. Presumably, you would receive them in a timely fashion.

If you looked at a particular intelligence product, would you know how the information was collected that went into that product?

General HUGHES. Usually, I would know how the information was collected. In many cases, that collection mechanism would be classified in order to protect its viability. But generally speaking—in fact, sitting here trying to think about an exception to that, I can't think of one. So generally, I would know even in the most sensitive cases how it was collected.

Mr. SIMMONS. And would you make a reasonable assumption that it was collected in accordance with the law?

General HUGHES. Yes, I would. I do think the use of the term law is important to me, and I would certainly defer to a more expert person, but the term law must be accompanied, I think, by the term interpretation and procedure. Many of the activities carried out by the government and by law enforcement organizations and intelligence organizations are found in the larger construct of the law that are devolved, some would say evolved, into procedure, policy and activity that can be interpreted differently by different persons. That has been a problem as long as our republic has been in existence, I think.

I think we all seek to do the right thing and we seek to do it legally. There are occasions, I think, when different interpretations are very valuable, because they point out the tensions between what one group or one administration or one organization might view as being correct to do and what another person or group might do as being incorrect. But the law itself is generally a larger body of knowledge that is interpreted by others, and policy and procedures put into effect on that basis. That makes it—I will use this term—problematic.

Mr. SIMMONS. As a military officer and as a federal official sworn by your oath of office to uphold the constitutional laws of the United States of America, if, in your capacity as head of a INA or its predecessor, it came to your attention that there might be a privacy issue, a violation of privacy involving some of the information in your possession, would you report that, or would you just keep it to yourself?

General HUGHES. Well, in fact, that very event happened, especially as we formed the Department of Homeland Security. There were questions of the right to privacy by citizens and the right to protection under the privacy laws of the information that we held

in our files. And you had to take each case on its own merits and determine within the procedure and policy at the time in the context of law how you would handle that information.

In some cases, the information was easy to expunge. It was very rapidly obvious in the eyes of persons with good judgment, our legal authorities and our privacy office that it should be expunged, and it was.

In other cases where there is a belief that a conspiracy exists and a person is a participant in it to conduct an act of terrorism or another crime of homeland security implications, the deliberate decision had to be made to retain that information and use it, and I think that, personally, in my own view, it is true but difficult to deal with that some of the information from some of the people concern citizens and residents of the United States.

I mean, I think every day you read about these events in the newspaper, and they seem to me to be covered adequately by law. It is against the law to plan to commit a crime at some point, and certainly to commit a crime. And it is especially against the law in the context of protecting the citizens' rights in this era we now live in of the potential for mass effects from such activities. I am not saying that the law needs to be changed, I am saying that we need to understand this in the context in which we are dealing with it.

Mr. SIMMONS. I hear your testimony to be that, for you, this was a serious issue and something that you and your office took seriously.

General HUGHES. And I had the direct legal counsel available in my office at all times and a direct connection to the Privacy Office, and I can assure you, and I would certainly be happy to do so under oath, that we not only took it seriously, we practiced it seriously.

Mr. SIMMONS. I thank you. My time is expired.

The distinguished ranking member of the full committee, Mr. Thompson, from Mississippi.

Mr. THOMPSON. Thank you very much, Mr. Chairman.

I am not sure if I am—I am a little troubled by what you said, Mr. Hughes. Was this information gained that you considered gained legally or illegally?

General HUGHES. I certainly might hope that in every case, it was gained legally, but once again, the interpretation of the law and the interpretation of policy and procedure to some degree has to rest in the eyes of the beholder until a determination is made by legally constituted authority. In searching my memory here this morning, I can't recall a single case where I ever believed it was gained illegally. However, I think once again one has to understand the modern environment in order to deal with this question.

Mr. THOMPSON. We understand the environment.

General HUGHES. Okay.

Mr. THOMPSON. Believe me. The question, though, is, notwithstanding the environment, there are some privacy considerations that have to be maintained.

General HUGHES. And I believe they were.

Mr. THOMPSON. Well, I guess I will—Mr. Turley, under the present scenario of wiretapping private citizens and not going

through any procedure, is it your belief that that process at this point is in fact illegal?

Mr. TURLEY. I absolutely believe that. And I don't have a scintilla of doubt. And if you look back at pass testimony I have given to both the House and Senate—I have been called by Democrats and Republicans, and I have always expressed when I considered something to be a close call.

This is not a close call. This here is an exclusivity provision under federal law. You have to do domestic surveillance no matter how you may frame it. This has always been viewed as domestic surveillance what was being done by the NSA. And you have to do it under either FISA or Title 3. You have to do it under that type of statutory authority. This was created to go around that. It was a direct violation of the exclusivity provision. And until the NSA operation, I don't remember hearing anyone having any doubt about any of those questions.

And that means that we have a very serious issue, because the president stood in front of Congress during the State of Union and said that not only had he ordered this 30 times, but he would continue to do so until, basically, someone stopped him.

And what was most astonishing is that members stood up and gave him a standing ovation. It was one of the most bizarre things I have ever seen as an academic. Members of Congress who pass these laws had a president who told them that he was not going to comply with those laws, and they give him a standing ovation.

Now, the framers—I have to tell you, we all sort of speak for the framers as if we are in some type of carni show.

[Laughter.]

But I think it is safe to say that the framers did not think it was going to happen this way, that they believed that Congress would have an institutional interest that it would protect, that regardless of their affiliation to the president, that they would fight to protect the legislative authority of this body. This is the most central and direct threat to the legislative branch's inherent authority that I have certainly seen in my lifetime.

Mr. THOMPSON. Mr. Herath, you mentioned some things that we could do to strengthen the Privacy Office. I talked about some things like subpoena power, initiate investigations, and I would think that in order to do your job, you need the tools necessary. Where do you come down on that issue?

Mr. HERATH. Well, Mr. Thompson, I agree that the subpoena power and investigatory power in a formal sense is necessary. That probably was part and parcel of my recommendation of the statutory authority.

I think, however, and I am speaking on behalf of the Privacy Office. I am not speaking on behalf of the Privacy Office. I am speaking on behalf of me. But I think that would probably be the last thing you would want to do as a privacy official. The first step, as Ms. Cooney described, you try do it, you know, informally through relationships.

If you have created a culture that is receptive to your privacy requests, I would say the vast majority, if not 99 percent, of your request are going to be complied with. However, I think that there does need to be, for those special occasions where you simply in

many cases know that whoever it is you are asking is not forthcoming, I think you do need to have sort of that final hammer with the subpoena.

Mr. THOMPSON. Or if that person that is withholding the information knows that you have subpoena authority.

Mr. HERATH. Correct.

Mr. THOMPSON. And, you know, it is just a matter of time that they will pull that trigger.

Mr. HERATH. Well, yes, I often say, you know, you have got to have skin in the game. If there is no formal ramification for withholding evidence, then there is a greater chance that will be withheld.

Mr. THOMPSON. Thank you.

I yield back, Mr. Chairman.

Mr. SIMMONS. I thank the gentleman. Would the gentleman like to go a second round?

Mr. TURLEY. One more.

Mr. SIMMONS. Okay.

Mr. Turley, thank you for your testimony. I was looking on page five, where you made the statement, "The NSA operation was never approved by Congress." And again, while the jurisdiction for this program resides with the House and Senate Intelligence Committees, in my opinion, I have always been troubled by the discussion of this program.

The ranking member of the House Intelligence Committee has said publicly that the NSA program was essential to targeting al-Qa'ida, and she made the statement as the ranking Democrat on the House Intelligence Committee, "I have been briefed since 2003 on a highly classified NSA foreign collection program that targeted al-Qa'ida. I believe the program is essential to U.S. national security and that its disclosure has damaged critical intelligence capabilities."

As somebody who served many years ago on this Senate Intelligence Committee, I was always puzzled by why senior members of these oversight committees did not, on the one hand, place the program into the law or alternatively legislate the program out of the law, or I should say legislate it to cease. I don't believe either one of those actions took place.

And I have also been concerned that through the routine authorization and appropriation process of the Congress over the years essentially dollars were authorized and appropriated for the National Security Agency to continue to perform that program. Now that takes me back to the mid–1980s when there was a covert action directed against Nicaragua. It involved the Contras and the Sandanistas, and, in fact, the Boland Amendment did explicitly terminate that program in 1984.

Do you have any thoughts, or do any of the members have any thoughts as to what might have been done back in 2003 that would have perhaps better dealt with this issue.

Mr. TURLEY. I suppose my first answer is I believe that the ranking Democratic member on the committee also mentioned that she didn't feel that she was able, because of the restrictions, to seek out advice of experts as to whether this was lawful under FISA, and that it was not until this matter became public that she concluded

that, indeed, there were legal issues. She was looking at it purely from an operational standpoint.

The second response is that I am still not sure why this operation was not disclosed to the full membership of those committees. My understanding is that it is only covert operations that are retrained to the smaller group. This would not constitute, as far as I know, that type of a covert operation. The surveillance program has generally been viewed as something that goes to the membership.

The third answer is that an appropriation of money has never been considered by the courts as any form of authorization. Under 1809, the authorization would have to be a specific authorization to give essentially a third track if you are not going to put it under FISA or Title 3.

And then, finally, my last response is, I am not too sure that you could put what was the NSA operation in the federal law without it being struck down. I mean, I think there is serious constitutional questions.

But I also believe, as someone who has practiced—I have been in the FISA court as a young intern at NSA, and I have been counsel in FISA cases, and I still don't understand why there was a need to go outside of FISA. FISA is the most user-friendly law ever created for a president. And so I still am not convinced about the need to circumvent the law.

Mr. SIMMONS. I appreciate that response.

I vaguely recall the Senate Resolution 400 required that the committee be kept fully and currently informed. That certainly applied to the Senate, maybe not to the House.

My recollection is that there were various compartments that involved covert action and other activities, but that in my experience, when a controversial program was briefed to the committees and to the leadership, if it existed for more than a year, it was handled within the oversight process. So perhaps this is an issue for oversight of those committees.

And I recognize the gentleman from Mississippi.

Mr. THOMPSON. Thank you very much, Mr. Chairman.

I would like to respectfully disagree on some of the jurisdictional issues that have come before us today. I think all of us, including yourself, want to give the tools necessary for law enforcement to do the job, but in collecting data, we want to make sure that those privacy and civil liberties issues are protected.

And if, in fact, the information gained is then transmitted, that is gained illegally and transmitted to any organization, and they began the process. That pause in intelligence creates a real problem, whether it is DHS. If I am a citizen, and I am all of a sudden on some kind of list that was, for whatever reason, put on that list through intelligence illegally gained, you know, I have a problem.

And I think all of us want to create a process that protect the rights of citizens, protect the individual liberties, but also keep America strong. I agree with Mr. Hughes, these are difficult times, but we have to make more than just an average effort to protect the rights of citizens. It has to be an enhanced effort, a work in progress.

There is legislation on the books that talks about sharing intelligence, talks about a number of things that I think gives us significant jurisdiction authority to look at these things. Facts about it, we passed the law requiring the sharing of information between agencies because it was not taking place. I want us to be cognizant of that.

The other issue is, and I will sort of make closing comments at this point if you like rather than giving questions. You know to the extent that we can strengthen whistle blower protections for citizens who have concerns and employees. We need to put that into place. We need to dispense laws on data mining and data sharing by agencies. You just can't go get the information and throw it out there for review without the protection of citizens.

I have talked about the subpoena power that we all kind of agree that you really can't do your job effectively unless you have that.

I must also say, Mr. Chairman, I am concerned that because we don't have it, the Privacy Office is using the leadership or the secretary or some friendly persuasion rather than having the inherent authority in that office to get it done. Whether they have to exercise it or not, we need to have it in place. This is a critical issue for all of us.

One of the strengths of our country and many of the things our founding fathers put together was the interest in seeking certain freedoms, and I would not want us under the color of intelligence or any other statute limit many of those freedoms for the citizens who operate within the law.

The law should protect them, and I look forward to continuing the discussion along this line, Mr. Chairman, and coming up with, not only a robust system that protects us all, but also, on the other hand, a system that protects the individual rights and liberties of American citizens.

And I yield back.

Mr. SIMMONS. I thank the gentleman for his comments, and thank him very much for his participation in this hearing this morning.

I think these issues are incredibly important, and I think they are also incredibly difficult. I am haunted by what I read in the 9/11 Commission report. I am reminded constantly that 12 of my constituents died on that day. And I recall regularly that my daughter was living in New York City a few blocks from the World Trade Center in an area that she could not return to because of the damage and destruction that two of her roommates and best friends from childhood were killed on that day. And I struggle with the balance between liberty and security.

Could we have listened to the phone conversation of Mohammad Atta? Could we have prevented that if we had done things differently? And as we work to bring about the changes to how we provide our Homeland Security for the safety of our citizens, are we protecting the liberties that make this country what it is and what we want it to be, not just for ourselves but for our children and future generations?

This is a solemn responsibility and a difficult challenge where, I believe, all of us have to work together to come up with a solution. And we won't solve it today or tomorrow. We will solve it

through a process of discussion and debate and hearing just as we have today.

I thank the panel for coming, and I thank the ranking member. The hearing is adjourned.

[Whereupon, at 10:49 a.m., the subcommittee was adjourned.]

PROTECTION OF PRIVACY IN THE DHS INTELLIGENCE ENTERPRISE PART II

Wednesday, May 10, 2006

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND ERRORISM RISK ASSESSMENT,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The subcommittee met, pursuant to call, at 4:03 p.m., in Room 311, Cannon House Office Building, Hon. Rob Simmons [chairman of the subcommittee] presiding.

Present: Representatives Simmons and Lofgren.

Mr. SIMMONS. [Presiding.] The Homeland Security Committee, and Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment will come to order.

We are meeting today at the request of the minority members of the subcommittee under House Rule 11 to receive testimony from a witness of the minority's choosing for one additional day on the subject of protection of privacy in the Department of Homeland Security intelligence enterprise.

The majority extended invitations to every witness that the minority requested, and I personally called the primary witness, Dean Parker, to secure her testimony today.

Unfortunately, none of the minority witnesses were able to attend. But, as I have expressed to my friend and colleague from California, I will continue in this effort.

Ms. LOFGREN. Mr. Chairman, I appreciate that offer of collaboration.

And as we discussed briefly early today, Dean Parker has not been able to attend. And I think, since she doesn't have current knowledge, we will continue to pursue the other three witnesses which you have written to. And I look forward to working with you in securing their attendance and learning what we can.

So, at this point, I would concur that this hearing ought to be called to a halt—or gavelled to a halt. And we will see either those three witnesses or their representatives who can speak knowledgeably for them at a future date.

And I thank you for your courtesy.

Mr. SIMMONS. I thank the ranking member for her comments. I concur in her assessment of the situation.

Having no witnesses, the subcommittee stands adjourned.

[Whereupon, at 4:04 p.m., the subcommittee was adjourned.]

○