TURNING SPY SATELLITES ON THE HOMELAND: THE PRIVACY AND CIVIL LIBERTIES IMPLICATIONS OF THE NATIONAL APPLICATIONS OFFICE

FULL HEARING

OF THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

SEPTEMBER 6, 2007

Serial No. 110–68

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
48–963 PDF WASHINGTON : 2009

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

BENNIE G. THOMPSON, Mississippi, *Chairman*

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
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
AL GREEN, Texas
ED PERLMUTTER, Colorado
VACANCY

PETER T. KING, New York
LAMAR SMITH, Texas
CHRISTOPHER SHAYS, Connecticut
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
BOBBY JINDAL, Louisiana
DAVID G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
MARSHA BLACKBURN, Tennessee
GUS M. BILIRAKIS, Florida
DAVID DAVIS, Tennessee

JESSICA HERRERA-FLANIGAN, *Staff Director & General Counsel*
ROSALINE COHEN, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

CONTENTS

TURNING SPY SATELLITES ON THE HOMELAND: THE PRIVACY AND CIVIL LIBERTIES IMPLICATIONS OF THE NATIONAL APPLICATIONS OFFICE

Thursday, September 6, 2007

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The committee met, pursuant to call, at 10:00 a.m., in Room 311, Cannon House Office Building, Hon. Bennie G. Thompson [chairman of the committee] presiding.

Present: Representatives Thompson, Harman, Jackson Lee, Christensen, Etheridge, Cuellar, Carney, Green, Perlmutter, King, Lungren, Reichert, Dent, and Broun.

Chairman THOMPSON. The Committee on Homeland Security will come to order.

The committee is meeting today to receive testimony on "Turning Spy Satellites on the Homeland: The Privacy and Civil Liberties Implication of the National Applications Office."

The Department chose Congress' August recess as a time to announce, with great fanfare, the creation of a new National Applications Office, referred to as the NAO, to facilitate the use of spy satellites to protect the homeland.

For the first time in our Nation's history, the Department plans to provide satellite imagery to State and local law enforcement officers to help them secure their communities. While I am all for information sharing with our first preventers, it has to happen the right way. Whether the National Applications Office is the right way remains to be seen.

What was perhaps most disturbing about the Department's announcement, moreover, is that it wasn't an announcement at all. This authorizing committee did not learn about the National Applications Office from you, Mr. Allen, but from the Wall Street Journal. There was no briefing, no hearing, no phone call from anyone on your staff to inform any member of this committee of why, how, or when satellite imagery would be shared with police and sheriffs' offices nationwide.

Apparently, we weren't the only ones left in the dark. Despite my repeated requests that the Department take privacy and civil liberties seriously, the privacy officer and civil rights and civil liberties officer were not brought into the National Applications Office development process until this spring, more than a year and a half after the National Applications Office started coming together. This

is unacceptable. The rigorous privacy and civil liberties protection must be baked into from the beginning, and your Department's experts on these topics were shut out.

Furthermore, the National Applications Office will be up and running in less than 4 weeks. How the working group responsible for developing the rules for State and local use of spy satellite imagery will complete their work in this time is beyond me. Indeed, they only recently began their work.

We are here today to help to ensure that privacy and civil liberties at the Department do not remain the afterthoughts that they have apparently been.

I want to know from our Department witnesses the scope of the program, its legal basis, and specifically how constitutional protections will be incorporated. I note, however, we will be doing it with one hand tied behind our back.

Last week, we invited the Department's Office of General Counsel to send an attorney to explain all this. What we got instead was a letter from the Department's Acting General Counsel stating, I do not feel that it would be useful for me to participate as a witness.

We frankly don't need the Acting General Counsel's advice on determining who will be a useful witness and who will not. I had a reason and a purpose for asking him to testify, and his absence creates a new question that I will seek to have answered later.

I firmly agree that America must use the tools at its disposal to prevent another terrorist attack on our soil, but we must do so within the confines of the law. Sharing spy satellite information with our State and local law enforcement simply goes to far more noncontroversial applications. As Kate Martin of the Center for National Security Studies has aptly stated, this potentially gives rise to a Big Brother in the Sky. Like Ms. Martin, I am not convinced that the potential impact of all this has been fully considered or that adequate protections are in place.

I look forward to hearing from our witnesses on how the Department plans to address these concerns, and from our panel of civil rights and civil liberty experts on the consequences of failure to get it right. We welcome our panel of witnesses.

[The statement of Mr. Thompson follows:]

PREPARED STATEMENT OF THE HONORABLE BENNIE G. THOMPSON, CHAIRMAN, COMMITTEE ON HOMELAND SECURITY

The Department chose Congress' August recess as the time to announce—with great fanfare—the creation of a new National Applications Office (NAO) to facilitate the use of spy satellites to protect the homeland.

For the first time in our nation's history, the Department plans to provide satellite imagery to state and local law enforcement officers to help them secure their communities.

While I'm all for information sharing with our first preventers, it has to happen the right way. Whether the NAO is the 'right way' remains to be seen. What was perhaps most disturbing about the Department's 'announcement', moreover, is that it wasn't an announcement at all.

This authorizing Committee did not learn about the NAO from you, Mr. Allen, but from the Wall Street Journal. There was no briefing, no hearing, and no phone call from anyone on your staff to inform any Member of this Committee of why, how, or when satellite imagery would be shared with police and sheriffs' officers nationwide.

Apparently we weren't the only ones left in the dark.

Despite my repeated requests that the Department take privacy and civil liberties seriously, the Privacy Officer and Civil Rights and Civil Liberties Officer were not brought into the NAO development process until this spring—more than a year and a half after the NAO started coming together.

This is unacceptable. Rigorous privacy and civil liberties protections must be 'baked in' from the beginning, and your Department's experts on these topics were shut out.

Furthermore, the NAO will be up and running in less than four weeks. How the working group responsible for developing the rules for state and local use of spy satellite imagery will complete their work in time is beyond me. Indeed, they only recently began their work!

We're here today to help and to ensure that privacy and civil liberties at the Department do not remain the afterthought that they have apparently been. I want to know from our Department witnesses the scope of the program, its legal basis, and specifically how Constitutional protections will be incorporated.

I note, however, that we'll be doing so with one hand tied behind our back. Last week, we invited the Department's Office of General Counsel to send an attorney to explain all this.

What we got instead is a letter from Gus Coldebella, the Department's Acting General Counsel, stating, 'I do not feel that it would be useful for me to participate as a witness,' I frankly don't need the Acting General Counsel's advice on determining who will be a useful witness and who will not. I had a reason and a purpose for asking Mr. Coldebella to testify, and his absence creates new questions that I will seek to have answered.

I firmly agree that America must use the tools at its disposal to prevent another terrorist attack on our soil—but we must do so within the confines of the law. Sharing spy satellite information with state and local law enforcement simply goes far beyond more non-controversial applications. As Kate Martin of the Center for National Security Studies has so aptly stated, it potentially gives rise to a 'Big Brother in the Sky.' Like Ms. Martin, I am not convinced that the potential impact of all this has been fully considered or that adequate protections are in place.

I look forward to hearing from our witnesses on how the Department plans to address these concerns and from our panel of civil rights and civil liberties experts on the consequences of failure to 'get it right.'

Mr. THOMPSON. I now yield to the ranking member for his statement.

Mr. KING. Thank you, Chairman Thompson. I want to welcome the witnesses. I look forward to their testimony.

I also share Chairman Thompson's concern and frustration that this committee was not made aware of this program at an early date, early time. Not for any reasons of turf or ego, but because if we are to be an effective oversight committee, if there is to be an effective relationship between the committee and the Department, it is essential that we be brought in at the start, not find out about it from press reports after the fact.

I have great regard for Mr. Allen. I am confident this will not be repeated in the future. I just want to emphasize that I fully agree with the chairman on this that this was not handled properly. And, again, we are not just talking about questions of technicalities or procedure, we are talking about the effectiveness and the legality of the program itself.

Now, having said that, from the information we have gotten over the past several weeks, including a briefing this morning, I at this stage do not see constitutional issues. Having said that, there is still no reason why—and the reason I say that, I don't see a fourth amendment issue here. But, again, as the testimony comes out today and as we hear especially from the second panel of witnesses, there may be issues raised that cause concern.

And also, it is my understanding that for the most part, if not entirely, what is going to be done under this program in a comprehensive, coordinated, cohesive way is what has been done in an

ad hoc way in a variety of ways over the past 30 years. So this certainly appears to be a step in the right direction, and it is unfortunate we have what may well be a needless controversy because we were not brought in early on.

I also must say to Chairman Thompson, though, that I am disappointed that we could not accommodate the requests of the DNI to have the Deputy Director of National Intelligence for Collection and also the DNI Civil Liberties Protection Officer testifying with the governmental witnesses. And, again, this is not just a matter of protocol, but I just thought it would add, if we are concerned about civil liberties, if we are concerned about civil rights, if we are concerned about what protections are in place, I believe they should have been allowed to testify at the government panel. And by putting them and offering them to testify at the second panel in an adversarial role, to me, defeats the purpose of what we are trying to do here as a committee. So, again, Mr. Chairman, I am disappointed in your decision not to give them the opportunity to testify at the government panel.

Having said that, I am sure this panel will give us the much needed information we need. I also look forward to the testimony of members on the second panel.

And I think it is important to keep in mind that we are talking about here confronting an enemy which is attempting to destroy us. It is essential that we do have effective surveillance. It is essential that we use all the necessary tools. From what I have learned so far, I believe sufficient protections are in place. But, again, we could avoid a lot of this issue if we had been brought in early on. And certainly not just Chairman Thompson and myself, but certainly people such as Chairperson Harman who has such a long experience in this and is Chair of the relevant committee, and as Chairman Conyers of the oversight committee. This would be a lot further along I think standing together in a much more bipartisan way if it had been done that way from the start.

So with that, I yield back the balance of my time the balance of my time. I thank the chairman for calling this hearing, and I look forward to the testimony.

Chairman THOMPSON. Thank you very much, Mr. King. Let me indicate that we invited DNI to participate on the second panel. They refused, as you know. But we are also opened to holding additional hearings on this matter going forward.

We thought it important, since Mr. Allen's shop is responsible for this particular program, that they be given exclusive panel presentation for this hearing, and for that reason we made that decision. But other members of the committee are reminded that, under the committee rules, opening statements may be submitted for the record.

I welcome the first panel of witnesses.

Our first witness, Charlie Allen, is the Department's Chief Intelligence Officer. Mr. Allen leads the Department's intelligence work through the Office of Intelligence and Analysis and focuses on improving the analysis and sharing of terrorist threat information.

Our second witness, Mr. Dan Sutherland, is the Department's Officer for Civil Rights and Civil Liberties. Mr. Sutherland pro-

vides advice to the Secretary and senior department officers on a full range of civil rights and civil liberties issues.

Our third witness, Hugo Teufel, is the Department's Privacy Officer. Mr. Teufel is primarily responsible for privacy policy at the Department. That includes assuring that the technologies used by the Department to protect the United States sustain and do not erode privacy protections related to the use, collection, and disclosure of personal information.

Without objection, the witnesses' full statement will be inserted in the record. I now ask each witness to summarize his statement for 5 minutes, beginning with Mr. Allen.

STATEMENT OF CHARLES ALLEN, CHIEF INTELLIGENCE OFFICER, OFFICE OF INTELLIGENCE AND ANALYSIS, DEPARTMENT OF HOMELAND SECURITY

Mr. ALLEN. Chairman Thompson, Ranking Member King, members of the committee, thank you for the opportunity to speak about the National Applications Office.

I would like to point out that the National Technical Means, such as overhead imagery from satellites, have been used for decades lawfully and appropriately to support a variety of domestic uses by the U.S. Government's scientific, security, and law enforcement agencies. The National Applications Office, when operational, will facilitate the use of remote sensing capabilities to support a variety of customers, many of whom have previously relied on ad hoc processes to access these intelligence capabilities.

The National Applications Office will provide not only a well ordered transparent process for its customers, but also ensure that full protection of civil rights, civil liberties and privacy are applied to the use of those remote sensing capabilities. In doing so, it will build on the outstanding work of the Civil Applications Committee, known as the CAC, which was established in 1975 to advance the use of the capabilities of the intelligence community for civil, nondefense, national security uses.

My staff and I have worked closely with the CAC to ensure that the standup of the National Applications Office, with the broadened mandate to include homeland security and law enforcement communities, will still support civil and scientific need for geospatial imagery at a robust level. Let me give you some background on the standup of the NAO, the National Applications Office.

In April 2005, the Director of National Intelligence, the DNI, and the Director of the U.S. Geological Survey commissioned an independent study group to review the current and future role of the CAC and to study whether the intelligence community was employing National Technical Means effectively for homeland security as well as law enforcement purposes. The study group, led by Mr. Keith Hall, former Director of the National Reconnaissance Office, concluded that, unlike civil users, many homeland security and law enforcement agencies lacked a Federal advocate for the use of National Technical Means. The study group's bottom line was, and I quote, "an urgent need for action, because opportunities to better protect the Nation are being missed."

They recommended unanimously that the DNI establish a new program to employ effectively the intelligence community's national

technical capabilities not only for civil purposes but also for homeland security and law enforcement.

The study group also recommended that the program be established within the Department of Homeland Security. In response to the study group's recommendation, the Director of National Intelligence designated the Secretary of Homeland Security as executive agent in late spring 2007 to establish the program in the form of a National Applications Office. A National Applications Executive Committee, cochaired by the DNI and the DHS, will be established to provide senior interagency oversight and direction.

In the past, with the CAC's assistance, scientists have used historical and current satellite imagery to study issues, such as environmental damage, land use management, and for similar purposes research. Similarly, some homeland security and law enforcement users also in the past routinely accessed imagery and other technical intelligence directly from the intelligence community, especially in response to national disasters such as hurricanes and forest fires.

The Department of Homeland Security/U.S. Secret Service has used overhead imagery to identify areas of vulnerability based on topography and to build large maps to support its security planning.

DHS and Federal law enforcement agencies have used imagery to identify potential vulnerabilities of facilities used for high-profile events such as the Super Bowl.

These are all valid, useful, lawful uses of National Technical Means that enhance our ability to protect our Nation, whether the threats are manmade or naturally occurring.

The objective of the NAO is to bring all these requirements for imagery support under one oversight body where they are not only prioritized but reviewed to determine whether the requirements are appropriate and lawful.

In short, the NAO's mission is to serve the right customers with the right product at the right time. On a day-to-day basis, the NAO will work with civil applications, homeland security, and, on a case-by-base basis, law enforcement customers to articulate their requirements to determine how our satellite imagery systems may be able to satisfy them, and submit any validator request to the National Geospatial Intelligence Agency for collection tasking.

The National Applications Office will also be able to access through the National Geospatial Intelligence Agency commercially available imagery to meet many of the customer needs.

Allow me to state categorically that the National Applications Office will have no relationship or interaction with either the FISA or the terrorist surveillance programs.

Now, let me talk about privacy and civil liberties. I am very pleased today to have with me my colleagues, Dan Sutherland and Hugo Teufel, who will speak in more detail about how NAO protects privacy and civil liberties. Since its inception, we have considered privacy and civil liberties to be at the forefront of the planning of the office.

The independent study group in 2005 articulated the need to protect privacy and civil liberties as a guiding principle. In my view, the NAO will strengthen privacy and civil liberties. The NAO will

be subject to direct oversight by privacy and civil liberties offices within both the Department of Homeland Security and the Office of the Director of National Intelligence. In addition, the National Applications Office will have its own legal adviser. At the executive level, the DNI's Civil Liberties Protection Officer and its Office of General Counsel, as well as DHS's Chief Privacy Officer and Officer for Civil Rights and Civil Liberties, will serve as advisers to the National Applications Executive Committee, which conducts the oversight and guidance. As evidenced today, the Congress will provide additional oversight of the NAO.

Together, these oversight mechanisms will ensure that the NAO will protect privacy, civil rights, and civil liberties under the highest standards while serving the strength and the security of this Nation. I assure you and the American people that the appropriate use of National Technical Means capabilities will make the Nation safer while maintaining strong protections of privacy and civil liberties. The National Applications Office will continue longstanding practices of employing these capabilities with full regard for the privacy and civil liberties of all Americans.

The rules for lawful and appropriate use for such capabilities have not changed. Under all conditions, especially in our increasingly uncertain homeland security environment in which we face a sustained and heightened threat, it is essential that our government use all of its capabilities to ensure the safety and well-being of its citizens. The NAO brings a critical and sensitive national capability to bear. It does so with the full respect for law and the rights our citizens cherish. I request your support for this vital national program.

Thank you very much.

[The statement of Mr. Allen follows:]

PREPARED STATEMENT OF THE HONORABLE CHARLES E. ALLEN, CHIEF INTELLIGENCE, OFFICE OF INTELLIGENCE AND ANALYSIS,

Chairman Thompson, Ranking Member King, Members of the Committee, thank you for the opportunity to speak with you about the National Applications Office (NAO). National Technical Means (NTM)—such as overhead imagery from satellites—have been used for decades, lawfully and appropriately, to support a variety of domestic uses by the US government's scientific, law enforcement and security agencies. The NAO, when operational, will facilitate the use of remote sensing capabilities to support a wide variety of customers, many of whom previously have relied on *ad hoc* processes to access these intelligence capabilities. The NAO will provide not only a well-ordered, transparent process for its customers but also will ensure that full protection of civil rights, civil liberties and privacy are applied to the use of these remote sensing capabilities.

Once initially operational this fall, the NAO will facilitate the use of NTM for civil applications and homeland security purposes. A third domain, law enforcement, will be a part of the NAO, but will not be operational on October 1 to allow additional time to closely examine any unique aspects of law enforcement requirements in light of privacy and civil liberties. In doing so, it will build on the outstanding work of the Civil Applications Committee, known as the "CAC," which was established in 1975 to advance the use of the capabilities of the Intelligence Community for civil, non-defense uses. My staff and I have worked closely with the CAC to ensure that the stand-up of the NAO—with a broadened mandate to include the homeland security and law enforcement communities—will still support civil and scientific need for geospatial imagery, at an even more robust level.

Background of the National Applications Office

From its inception, the CAC has helped civil and scientific users understand how NTM can assist their missions and how to gain access to information normally in the hands of the intelligence agencies. With the CAC's assistance, for example, scientists have used historical and current satellite imagery to study issues such as environmental damage, land use management, and for similar purposes of research. The CAC also has used imagery to study glaciers and examine the effects of global climate change.

Similarly, some homeland security and law enforcement users in the past routinely accessed imagery and other technical intelligence directly from the Intelligence Community, especially in response to natural disasters such as hurricanes and forest fires. The Department of Homeland Security (DHS), for example, used overhead imagery in 2005 to examine areas damaged by Hurricanes Katrina and Rita to determine areas most in need of assistance. The DHS US Secret Service has used overhead imagery to identify areas of vulnerability based on topography and to build large maps to support its security planning. DHS and Federal law enforcement agencies have used imagery to identify potential vulnerabilities of facilities used for high-profile events such as the Super Bowl. These are *all* valid, lawful uses of NTM that enhance our ability to protect our nation—whether the threats are man-made or naturally occurring. The objective of the NAO is to bring all of these requirements for imagery support under one oversight body, where they are not only prioritized but also reviewed to determine whether requirements are appropriate and lawful. Allow me to state categorically, the NAO will have no relationship or interaction with either the FISA or the Terrorist Surveillance Programs.

Let me provide background on the decision to establish the NAO. The Director of National Intelligence (DNI) and the Director of the U.S. Geological Survey commissioned an independent study group in early 2005 to review the current and future role of the CAC and to study whether the Intelligence Community was employing NTM capabilities effectively for homeland security and law enforcement purposes. The study group, led by Mr. Keith Hall, formerly Director of the National Reconnaissance Office, concluded that, unlike civil users, many homeland security and law enforcement agencies lacked a federal advocate for the use of NTM. In addition, the study group determined that many agencies, especially at the state and local level, did not know what remote sensing capabilities the Intelligence Community possessed that might be useful to them or how to request NTM in support of their missions. The study group's bottom line was that there was "an urgent need for action because opportunities to better protect the nation are being missed." It recommended unanimously that the DNI establish a new program to employ effectively the Intelligence Community's NTM capabilities not only for civil purposes, but also for homeland security and law enforcement uses as well.

In response to the study group's recommendations, the DNI designated the Secretary of Homeland Security as Executive Agent in late spring 2007 to establish the new program in the form of the NAO. As it becomes initially operational this fall, the NAO will work with the Intelligence Community to improve access to NTM for domestic users in the homeland security and civil applications communities at all levels of government, who, heretofore, have not had a structured process to request such intelligence. DHS, as executive agent, will operate the NAO. A National Applications Executive Committee, co-chaired by the DNI and DHS, will be established to provide senior interagency oversight and guidance. "This interagency forum will ensure the NAO adequately serves those government customers who have lawful and appropriate requirements for geospatial intelligence, to include classified satellite imagery and derived products.

Day to Day Activities

On a day-to-day basis, the NAO will work with civil applications, homeland security, and in the future on a case-by-case basis, law enforcement customers, to articulate their requirements, determine how our satellite imagery systems may be able to satisfy them, and submit any validated requests to the National Geospatial Intelligence Agency (NGA) for review, approval and collection tasking. The NAO also will be able to access, through NGA, commercially available imagery to meet many customer needs.

The NAO will be advised and supported by three working groups representing customer domains: civil applications, homeland security, and law enforcement. It should be noted that the law enforcement working group will be stood up over the next year, after closely examining any unique aspects of law enforcement requirements in light of privacy and civil liberties. All three domain working groups will

include representatives from the DHS Privacy Office and the DHS Office for Civil Rights and Civil Liberties as well as an attorney assigned directly to the NAO.

In addition to its day-to-day business of helping its customers gain access to NTM, the NAO will help customers take advantage of educational opportunities to learn about the Intelligence Community remote sensing capabilities, including their benefits and limitations. The NAO also will serve as an advocate in Intelligence Community discussions about future technology investments that might benefit the civil applications, homeland security, and law enforcement domains.

Privacy and Civil Liberties

Since its inception, we have considered privacy and civil liberties to be at the forefront of the planning for the NAO. The independent study group in 2005 clearly articulated the need to protect privacy and civil liberties as a guiding principle in its findings. In my view, the NAO—when operational—will *strengthen* privacy and civil liberties. The NAO will be subject to direct oversight by privacy and civil liberties offices within both the Department of Homeland Security and the Office of the Director of National Intelligence. In addition, the NAO will have it own legal advisor. At the executive level, the DNI's Civil Liberties Protection Officer and its Office of General Counsel, as well as DHS's Chief Privacy Officer and Officer for Civil Rights and Civil Liberties Officer, will serve as advisors to the National Applications Executive Committee, which will provide executive oversight and guidance for the NAO. The President's Privacy and Civil Liberties Oversight Board will have oversight of the use of NTM for combating terrorism.

In addition, all requests from the NAO for the use of classified satellite imagery will continue to abide by current NGA processes and be vetted by NGA attorneys and policy staff to determine legal appropriateness before collection tasking occurs. This review provides a supplemental level of oversight in addition to the strong protections already embedded in the NAO. In this way, both DHS and NGA will ensure adherence to applicable law and regulation, and intelligence oversight rules. DHS and NGA are bound by intelligence oversight rules, explained in Executive Order 12333, that protect the privacy and civil liberties of US persons. Further, DHS and NGA are required to report any violations of law or other questionable activities to the Intelligence Oversight Board of the President's Foreign Intelligence Advisory Board including violations of E.O.)333. Finally, both DHS and NGA are subject to oversight by the House and Senate intelligence committees.

Conclusion

I assure you and the American people that the appropriate use of these NTM capabilities will make the nation safer while maintaining the privacy and civil liberties of Americans. The NAO will continue long-standing practices of employing these capabilities with full regard and protection for the privacy and civil liberties of Americans. The rules for lawful and appropriate use of such capabilities have not changed.

Under all conditions, and especially in our increasingly uncertain homeland security environment in which we face a sustained and heightened threat, it is essential that our government use all its capabilities to assure the safety and well-being of its citizens. The NAO brings a critical and sensitive national capability to bear. It does so with full respect for the law and the rights our citizens cherish. I request your support for this vital national program.

Chairman THOMPSON. Thank you, Mr. Allen, for your testimony.

I now recognize Mr. Sutherland to summarize his statement for 5 minutes.

STATEMENT OF DANIEL W. SUTHERLAND, OFFICER, CIVIL RIGHTS AND CIVIL LIBERTIES, DEPARTMENT OF HOMELAND SECURITY

Mr. SUTHERLAND. Thank you, Chairman Thompson, ranking Member King, and distinguished members of the committee. Thank you for giving me the opportunity to speak to you today about the civil rights and civil liberties implications of the new National Applications Office.

We believe that the work of the new NAO will reach its highest level of effectiveness when it is carried out in a way that respects America's rich constitutional history. So I want to begin by assuring you that our office, the Office for Civil Rights and Civil Liberties, is working very closely with Assistant Secretary Allen and his staff and our colleagues in the Privacy Office to assure that the new NAO meets that highest level of effectiveness. In addition, we look forward to continuing to work with the Director of National Intelligence's Civil Liberties Protection Officer and the Privacy and Civil Liberties Oversight Board as well as this committee on this issues. There are a complex range of people who are working on these issues, and we have a good working relationship that we look forward to building on.

Just briefly, let me touch on the mission of our office generally. In accordance with 6 USC, Section 345, the mission of the Office for Civil Rights and Civil Liberties is to assist the dedicated men and women of the Department of Homeland Security to secure our country while preserving our freedoms and our way of life.

We have worked on issues, almost all the issues that have faced the homeland security effort from the Hurricane Katrina recovery, to the operation of watch list immigration policy, to the training of our workforce. Of course, we collaborate extensively with our colleagues in the Privacy Office as well. So, just a general layout of our office.

Let me talk about how it relates to the National Applications Office and our work here. I want to highlight quickly four reasons why we think that the protection of civil liberties should become a core responsibility, a part of the basic infrastructure of the NAO.

The first reason is because the people who lead the program have made it clear that they are committed to protecting civil liberties. You just heard Assistant Secretary Allen's testimony. But, in addition, our office was written into the planning for the NAO and our important role was made clear in the NAO's concept of operations, and in recent weeks we have been working very closely with the NAO, the larger Intelligence and Analysis Directorate within which it operates, and a variety of these other agencies. And we have established a solid working relationship with the NGA where these applications will come from.

So the first reason that we believe that there is a protection of civil liberties is that it is being built into the infrastructure as we begin to operate the program.

The second reason why we are optimistic is that we have a solid track record of working with our colleagues in Intelligence and Analysis on projects such as this. For example, our offices have worked together on many initiatives relating to radicalization and engagement with American Arab, Muslim, Sikh, and South Asian communities, an extremism that our country is facing. We described some of that work in previous meetings with staff members here and in testimony in front of this committee.

We are also heavily involved in the Department's information sharing environment efforts which are led by INA, and this year we have begun working on fusion centers and helping in terms of training and other work that INA is doing in terms of fusion centers.

So there are numerous other projects that I could specify. Those are just a few. We have an increasing and deep working relationship with our colleagues in Intelligence and Analysis, and so we believe that that is a strong track record we can build on.

Third, the NAO is creating important procedural safeguards to protect civil liberties. Just as Felix Frankfurter once wrote, the history of liberty has largely been the history of the observance of procedural safeguards. In other words, if parameters are established, if ground rules are laid out, the chances that violations will occur are much less likely, and that if those violations occur, they will be limited in scope and effect.

So, Charlie has already referenced several of the safeguards. Let me just mention them again.

First, we are working with the NAO to implement the Con Ops for the office. The Con Ops integrates in the protection the role of the Civil Rights and Civil Liberties Office as well as the Privacy Office.

Secondly, we are working on the standard operating procedures, and will make recommendations related to the extent and process for our review of any NAO requests. We have already begun working with and are assured that we are going to be involved in a variety of different legal and policy working groups that are associated with this.

And, finally, we will serve as formal advisers to the National Applications Executive Committee which will be established in the upcoming weeks.

So all of these procedural steps will help ensure that privacy and civil liberties issues are fully considered in the ongoing work of the NAO.

So fourth and finally, maybe most importantly, we will provide training on these issues. We have already been asked to provide training on basic civil liberties protections to the staff of the NAO in the upcoming weeks, and we expect to accomplish that initial training here in this month. And we believe that our training efforts should extend beyond DHS employees in the sense of customer education on civil liberties as one means of warding off potential misuse.

I want to thank you for inviting me to share our thoughts on the National Applications Office, and I look forward to working with this committee to provide oversight of this important program. Thank you.

[The statement of Mr. Sutherland follows:]

PREPARED STATEMENT DANIEL W. SUTHERLAND

Introduction

Chairman Thompson, Ranking Member King and distinguished Members of this Committee: Thank you for providing me the opportunity to testify today on the National Applications Office (NAO) and the civil rights and civil liberties implications of its work. The work undertaken by the new NAO within our Department will be an asset to the country's homeland security effort, and NAO will reach its highest level of success when accomplished in ways that respect America's rich Constitutional history. I want to begin by assuring the Committee that the Office for Civil Rights and Civil Liberties is engaged with Assistant Secretary Allen and his staff and our colleagues in the Privacy Office to ensure that the NAO reaches the highest level of effectiveness. In addition, I look forward to continuing to work with our colleagues in the Office of the Director of National Intelligence's Civil Liberties Protec-

tion Officer, the Privacy and Civil Liberties Oversight Board and this Committee to provide strong oversight of the NAO.

The Mission of the Office for Civil Rights and Civil Liberties

In accordance with 6 U.S.C. §345, the mission of the Office for Civil Rights and Civil Liberties is to assist the dedicated men and women of the Department of Homeland Security (DHS) to secure our country while preserving our freedoms and our way of life. We assist our colleagues in four ways:

- We provide proactive advice on a wide range of issues, helping the Department to shape policy in ways that are mindful of civil rights and civil liberties;
- We investigate and facilitate the resolution of complaints filed by the public regarding Departmental policies or actions taken by Departmental personnel;
- We provide leadership to the Department's equal employment opportunity programs, seeking to make this Department the model Federal agency; and,
- We serve as an information and communications channel with the public regarding these issues.

In essence, we provide advice to our colleagues on issues at the intersection of homeland security and civil rights and civil liberties. We therefore have the opportunity to work closely with every DHS component, both in Washington, D.C., and in many field offices across the country. Our Office has been involved in nearly all aspects of the critical issues facing the homeland security effort—from the Hurricane Katrina recovery, to the operation of watch lists, to immigration policy, to the training of our workforce.

Because our Office is small, we realize that we must, to use a sports analogy, "punch above our weight." One way we have accomplished this is by creating the "Civil Liberties Institute," a program to provide high-quality training on a wide range of topics.

Through the "Civil Liberties Institute," we have developed:

- a training video that emphasizes elements of the National Detention Standards;
- a multi-hour instructional video on how to screen people with disabilities at airports;
- educational materials on how to screen those who wear religious head coverings;
- an intensive training DVD for DHS personnel who interact with Arab Americans, Muslim Americans, and people from the broader Arab and Muslim world; and,
- "Guidance Regarding the Use of Race for Law Enforcement Officers," a tutorial on the Department of Justice's Guidance and the DHS policy.

These materials are available to DHS law enforcement employees in DVD, CD–ROM, or via on-line web-based training formats.

Of course, we collaborate extensively with our colleagues in the Privacy Office. We work closely with colleagues from the Office of the Director of National Intelligence (DNI), the Privacy and Civil Liberties Oversight Board (PCLOB), and others across the government.

The work of the Office for Civil Rights and Civil Liberties has been supported by other DHS elements because we provide constructive advice that allows the men and women of the Department to fulfill their mission at the highest level of effectiveness. Our work has also been welcomed by colleagues outside of government, as demonstrated by our frequent collaborations with leading civil rights, civil liberties, immigration, and community organizations. Our Office plays a unique role within DHS, and, we hope, a valuable one, and we will continue to assist our colleagues to tackle complex issues in innovative and constructive ways.

The Office for Civil Rights and Civil Liberties' Role in the National Applications Office

Having laid out the role of our Office, let me address the specific topic of the National Applications Office. I would like to highlight four reasons why the protection of civil liberties will become a core responsibility—part of the basic infrastructure—of the National Applications Office.

First, the people who lead the program have made it clear that they are committed to protecting civil liberties. The Office for Civil Rights and Civil Liberties was written into the planning for the NAO and our important role is made clear in the NAO Concept of Operations (CONOPS). In recent weeks, we have been working very closely with the NAO, the DHS Office of Intelligence and Analysis (I&A) within which the NAO functions, the DHS Privacy Office, the DNI, the PCLOB, and the National Geospatial-Intelligence Agency (NGA). The Office for Civil Rights and Civil Liberties has established a solid working relationship with our colleagues in each of these organizations. The commitment to establishing safeguards to protect,

and indeed enhance, our civil liberties has been front and center of all of these discussions. We believe that a great foundation has been laid for working together over the upcoming weeks, months and years.

Second, we have a solid track record of working with our colleagues in I&A on complex projects such as this. Our offices have worked together on many initiatives related to extremism and radicalization. Assistant Secretary Allen and his colleagues at I&A are great supporters of our work to engage with the American Arab, Muslim, Sikh and South Asian communities, the fruits of which we have described in prior meetings with your staffs and in testimony before this Committee. We are heavily involved in the Department's Information Sharing Environment efforts led by I&A, and we are also taking a leadership role with respect to government-wide efforts lead by the Program Manager for the Information Sharing Environment at DNI. This year we have begun to partner with I&A to train personnel and develop sound civil rights and civil liberties policies and procedures for State and local fusion centers. There are numerous other projects for which our offices consult each other on a regular basis. This strong track record reassures us that we will be in a good position to advise the NAO for the long term.

Third, the NAO is creating important procedural safeguards to protect civil liberties. Justice Felix Frankfurter once wrote, "The history of liberty has largely been the history of the observance of procedural safeguards."[1] That is, if parameters are established, if ground rules are laid out, the chances that violations will occur are much less likely and are much more likely to be limited in scope and effect. There are several significant safeguards that are being built into the NAO's infrastructure. First, we are working with NAO to implement the CONOPS for the office. The CONOPS includes a prominent role for our Office and the Privacy Office to provide support and guidance to the NAO, and will allow us to be embedded into the work of the NAO. Similarly, we will review the Standard Operating Procedures (SOP) and make recommendations related to the extent and process for our review of NAO requests for NGA Products and Services. We have already been assured that we will be part of the Policy and Legal Working Group, co-chaired by DNI and DHS, which we and the Privacy Office will participate in along with all relevant NAO sub-working groups. In addition, together with the Privacy Office and DNI's Civil Liberties Protection Officer, we will serve as formal advisors to the National Applications Executive Committee, which will be established in the upcoming weeks. All of these procedural steps will help ensure that privacy and civil liberties issues are fully considered in the on-going work of the NAO.

Fourth and finally, we will provide training on these issues. We and the Privacy Office have already been asked to lead a training session on civil liberties and privacy protections to the new staff of the NAO. We expect that this training, which is anticipated to be scheduled for later this month, will only be the first of many such efforts. We believe that our training efforts should extend beyond DHS employees. For example, we will lead an effort for "customer education" on civil liberties as one means of warding off potential misuse.

Civil Liberties and the Domestic Use of Geospatial Imagery and Derived Products and Services

As we undertake our work, we will assist the NAO effort by keeping a watchful eye on several key potential civil liberties issues. We will carefully watch:

- The expansion of customers and increased use of geospatial imagery and derived products and services to ensure that the increased volume does not lead to mistakes. As the NAO customer base increases, it will likely receive many more new project requirements, potentially posing an increased risk that improper requests will be approved in error, with a concurrent increased risk to civil liberties. We will help our colleagues at NAO to ensure that quantity does not result in sacrifices of quality.
- NGA provides a legal and policy review of all Federal requests for domestic geospatial intelligence (GEOINT). NGA has a long-established process to review domestic requests to ensure compliance with the law and Intelligence Oversight rules. That process employs the Proper Use Memorandum (PUM). A PUM is a memorandum between the requesting agency and NGA outlining the parameters of permissible requests. A PUM includes the requesting agency's authorized mission permitting use of such information, a description of the intended use of the domestic imagery, who will exploit the domestic imagery, who will receive the domestic imagery and derived products, storage and protection of the imagery, and certification by an appropriate official of the lawfulness and validity of the request. We will work with the NAO to ensure that the NAO's-

[1] *McNabb* v. *United States,* 318 U.S. 332, 347 (1943).

sponsored PUMs submitted to NGA contain the appropriate parameters and authorities. We will also work with NAO to ensure that requests received and information provided fit within the contours of these PUMs.

• The NAO will review all State and local law enforcement requests for the use of NGA products and services. NAO will forward their vetted requests to NGA for legal and policy review and final approval. Domestic requests for NGA products and services will only be approved if they comply with applicable legal requirements, including, but not limited to, Executive Order 12333, and would not result in an unreasonable search under the Fourth Amendment. Our Office will monitor proposed efforts by law enforcement users involving novel uses of geospatial imagery and derived products and services or those which approach the limits of existing civil liberties standards in this area. We will address those issues in the planning phase and as they arise in the future.

• As geospatial imagery and derived products and services are added to other data to form products for dissemination throughout the information sharing environment, civil liberties and civil rights concerns may arise. As these products are developed, we anticipate that there may be potential concerns related to access to those products, retention of images or data, and the reliability of the data and use of data. We will address those issues in the planning phase and as they arise in the future.

Conclusion

The Office for Civil Rights and Civil Liberties will work with the NAO to establish a firm and certain foundation that provides strong adherence to civil rights and civil liberties. We will closely monitor and address the areas I have mentioned and other issues that may arise. Building upon our success in civil rights and civil liberties compliance and training, and our track record of close cooperation with DHS components, we will work with the DHS Privacy Office, I&A, the Civil Liberties Protection Officer at DNI and the Privacy and Civil Liberties Oversight Board to protect and preserve civil liberties as NAO begins operations to help the government ensure the safety and well-being of our citizens.

I thank you for inviting me to share our thoughts on the National Applications Office today, and I look forward to working with this Committee to provide oversight of this important program.

Chairman THOMPSON. Thank you, Mr. Sutherland, for your testimony.

I now recognize Mr. Teufel to summarize his statement for 5 minutes.

STATEMENT OF HUGO TEUFEL, CHIEF PRIVACY OFFICER, DEPARTMENT OF HOMELAND SECURITY

Mr. TEUFEL. Thank you very much, Chairman Thompson, Ranking Member King, members of the committee, Mr. Perlmutter from my home State of Colorado.

I want to thank you for the opportunity to discuss the Privacy Office's efforts to protect privacy within the National Applications Office of the Department of Homeland Security, and I will be brief in my remarks.

I want to assure the committee that the Privacy Office is engaged with the Assistant Secretary and his staff, and our colleagues in the Office of Civil Rights and Civil Liberties and with the Office of the Director of National Intelligence's Civil Liberties Protection Office to ensure that the NAO will operate transparently and in full compliance with all statutory and policy requirements, including privacy.

As the NAO develops, we will continue to identify privacy risks and fashion protections to mitigate or eliminate those risks. The NAO prioritizes the protection of privacy and civil liberties. All activities of the NAO fall under existing legal authorities, including Executive Order 12333 and the Privacy Act.

I want to stress, as the program stands today, there has been no collection, use, or maintenance of records about individuals as covered under the Privacy Act. Moreover, the Privacy Impact Assessment, PIA, of the NAO undertaken by my office and Mr. Allen's staff identified that the necessary safeguards were in place on the processes of the NAO providing appropriate privacy protections. Of course, we will continue to work with the NAO to see that NAO continues to establish and maintain privacy protections throughout the development and implementation of this new effort, and we will be vigilant in our oversight responsibilities to ensure continued compliance with privacy law and Federal policies regarding the collection, use, maintenance, and dissemination of records.

Two other things I want to add. First is, the Civil Applications Committee is not something that was new to me. I served as the Department of the Interior's Associate Solicitor for General Law from June of 2001, July of 2001, until January of 2004. And as one of a handful of attorneys within the Solicitor's Office with SCI access, the CAC was one of my clients.

Other than the use of National Technical Means for map making and environmental uses, there was an ad hoc approach to the use of NTM, with NGA attorney and programmatic oversight, but not much else. So I can tell you that with the movement of the CAC and these responsibilities over to the NAO, there is far greater and layered oversight than existed previously.

Two, I want to stress to you, since I became the privacy officer at the Department, my office has increased focus on intelligence and the intelligence community. We have been working with INA and our colleagues over at CRCL since the beginning on intelligence issues. And, I want to note that as a matter of policy, not as a matter of law because Section 208 of the E-Government Act exempts the intelligence community, we notwithstanding that exemption as a matter of policy since the beginning of the Department, have as a matter of policy that we will conduct privacy impact assessments on activities of intelligence and analysis, and we did so in this case.

Additionally, throughout my office everyone involved in any way with INA or the intelligence communities is undergoing intelligence training on law and policy. I, myself, have been through the Army JAG School's intelligence law course at Charlottesville and, in completion of my master's program at the Naval War College, am currently enrolled in an intelligence and homeland security course.

So we take this very seriously, and we want to better understand the intelligence community so that we can do a better job of overseeing what it is that Intelligence and Analysis does generally and with respect to NAO.

With that, I am concluded. Thank you very much.

[The statement of Mr. Teufel follows:]

PREPARED STATEMENT OF HUGO TEUFEL, III

Introduction

Chairman Thompson, Ranking Member King, and Members of the Committee, I thank you for the opportunity to discuss the Privacy Office's efforts to protect privacy within the National Applications Office (NAO) of the Department of Homeland Security (DHS).

I want to begin by assuring the Committee that the Privacy Office is engaged with Assistant Secretary Allen and his staff, our colleagues in the Office for Civil Rights and Civil Liberties, and with the Office of the Director of National Intelligence's (ODNI) Civil Liberties Protection Office to ensure the NAO will operate transparently and in full compliance with all statutory and policy requirements, including privacy. As the NAO develops, we will continue to identify privacy risks and fashion protections to mitigate or eliminate those risks. The NAO prioritizes the protection of privacy and civil liberties. All activities of the NAO fall under existing legal authorities, including Executive Order 12333 and the Privacy Act. I want to stress, as the program stands today, there has been no collection, use or maintenance of records about individuals as covered under the Privacy Act. Moreover, the Privacy Impact Assessment (PIA) of the NAO undertaken by my office and Mr. Allen's staff identified that the necessary safeguards where in place on the processes of the NAO providing appropriate privacy protections. Of course, we will continue to work with the NAO to see NAO continues to establish and maintain privacy protections throughout the development and implementation of this new effort, and we will be vigilant in our oversight responsibilities to ensure continued compliance with privacy law and Federal policies regarding the collection, use, maintenance, and dissemination of records.

The Privacy Office Interaction with Intelligence and Analysis

The Privacy Office believes it is never too early for a component or program to engage our office. Programs operate effectively and privacy interests are best served when privacy protections are considered in the earliest stages of program or system development. We call our efforts to embed privacy into Departmental programs in the earliest stages "operationalizing privacy." Frequent privacy training—at the time of hire and annually thereafter—active involvement in the technology investment review process, and issuance of our Privacy Technology Implementation Guide are just a few examples of the tools the Privacy Office uses to encourage operationalizing privacy within the Department. The Government Accountability Office (GAO) acknowledged our gains in this important goal during its recent review of our office. Still, in an organization as large as DHS, one of our biggest challenges is keeping abreast of individual programs in their very earliest moments of conception. We rely very heavily on components to seize upon the lessons of our outreach and notify us of their future plans, even if the contemplated use of PII is remote.

My staff became part of the NAO's Policy and Legal Working Group in November 2006. The purpose of this working group was, and is, to advise the Director of the NAO and the implementation planning team on issues related to the formation and anticipated operation of this new Departmental initiative. The Privacy Office's role in the group is to ensure strict compliance with all applicable privacy law and policies.

The most significant result of this initial, but limited, interaction was the issuance of the NAO Concept of Operations (CONOPS). The CONOPS commits the NAO staff to conduct their authorized functions effectively while ensuring that their activities affecting U.S. Persons are conducted in a manner that protects privacy and constitutional rights. The CONOPS further commits the Privacy Office, along with the Office for Civil Rights and Civil Liberties, to provide support and guidance to the NAO, and recommend steps to reconcile the need to use domestic information with the keystone requirement of protecting the privacy and civil liberties of U.S. persons. DHS will also assure any future updates to the NAO CONOPS are reviewed by the Privacy Office in accordance with Privacy Office guidance. The governance structure calls for the DHS' Director of Operations Coordination to review the program annually, including its compliance with privacy requirements, and includes our offices and our colleagues at the ODNI Civil Liberties Protection Office as advisors to the National Applications Executive Committee.

The Privacy Office became more involved with NAO during the iterative PIA process. I&A and the Privacy Office worked together for several months to draft a PIA cataloging and documenting both potential privacy risks and the steps the Department will take to mitigate these risks.

The NAO Privacy Impact Assessment

The *E-Government Act of 2002* requires agencies to conduct a PIA when developing or procuring IT systems or projects that collect, maintain, or disseminate information in an identifiable form or about members of the public. The Department has pioneered the use of PIAs beyond what the E-Government Act requires in two ways which are relevant to our work with the NAO.

First, the Privacy Office recognized that privacy can be impacted by offices, such as the NAO, policies, and rules of the Department, in addition to information technology. Therefore, as a matter of policy the Privacy Office conducts PIAs to examine

these offices, policies, and rules, as well, even though it is not required to under the E-Government Act. These PIAs examine the application of the Fair Information Practice Principles (FIPPs) to the policy or, in this case, the office. The eight FIPPs are rooted in the tenets of the Privacy Act and govern the appropriate use of personally identifiable information (PII) at the Department.[1] They are:

1. *Transparency:* DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system whose existence and purpose is a secret.
2. *Individual Participation:* DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.
3. *Purpose Specification:* DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used and shared.
4. *Data Minimization:* DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).
5. *Use Limitation:* DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department is limited to purposes compatible with the purpose for which the PII was collected.
6. *Data Quality and Integrity:* DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.
7. *Security:* DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
8. *Accountability and Auditing:* DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Second, as a matter of policy, the Privacy Office conducts PIAs on national security systems, which are exempted from the requirement under Title II of the E-Government Act (Section 202(i)); although, consistent with the need to protect the processes associated with national security, the Privacy Office refrains from publishing these PIAs on our public facing website, www.dhs.gov/privacy.

This broad use of the PIA beyond the strict requirements of the E-Government Act is consistent with the Privacy Officer's authority under Section 222 of the *Homeland Security Act of 2002* to assure that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information. We have found that PIAs are an invaluable tool for programs to understand how their use of information impacts privacy. In addition, PIAs enhance the confidence the public has in the steps DHS takes to protect privacy. Thus, I was pleased to see GAO report that our office had made significant progress in both the number and quality of PIAs issued by the office.

On June 15, 2007, the Department issued a PIA for the NAO. I&A shared it with various Congressional Committees, and I know this Committee has now seen it as well. The document is For Official Use Only and, therefore, was not made public—and I am limited in what I can say about it here. Nonetheless, the PIA examined the application of the FIPPs to the NAO as it is presently planned. At this time, privacy concerns are nominal because the NAO does not presently anticipate routinely using or maintaining PII. Should this change, all notice, comment and oversight requirements imposed by the Privacy Act, the Privacy Office, and, I'll add, the DHS Office for Civil Rights and Civil Liberties, will be strictly followed. This PIA, like every other issued by the Department, will be updated as often as is required.

[1] The Department's PIA Guidance defines PII as "any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department." Section 208 of the E-Gov Act requires agencies to conduct a PIA for systems which collect, maintain, or disseminate information in an identifiable form, which is defined as "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means." (P.L. 107–347)

In fact, we anticipate issuing a new version of the PIA soon incorporating additional views; when the revision is complete, we will of course share it with this Committee.

Finally, I want to note that in order to improve our ability to conduct privacy oversight for I&A, Privacy Office staff, including the Chief Privacy Officer, are undergoing training on intelligence law and the intelligence community, to better understand that community's mission and legal constraints. The Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, the "Church Committee," and the report of the Rockefeller Commission, are all required reading in our office. We are mindful of the abuses of the past and we are determined that those abuses not be repeated at our Department.

The Privacy Office and Office for Civil Rights and Civil Liberties and ODNI's Civil Liberties Protection Office

I am particularly pleased to be appearing today with the Officer for Civil Rights and Civil Liberties, Dan Sutherland. His office and mine share a statutory obligation to work together to ensure programs, policies and procedures involving civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner.

Both Mr. Sutherland and I have strived to give maximum effect to this statutory obligation. In addition to our frequent consultation, our staffs have instituted biweekly calls to ensure the close level of cooperation contemplated by the Homeland Security Act. The NAO is another opportunity for our offices to work together and coordinate our policies relating to privacy and civil rights and civil liberties.

Our office has developed a very close working relationship, as well, with our colleagues at the ODNI's Civil Liberties and Protection Office, which is charged with ensuring appropriate protections for privacy and civil liberties are incorporated in the policies and procedures of elements of the intelligence community within the National Intelligence Program, including DHS. I am pleased to be appearing today with Mr. Joel, who heads the ODNI's Civil Liberties Protection Office.

Our combined efforts on training and oversight will be critical to the success of the NAO.

Conclusion

The Privacy Office is committed to ensuring the NAO will be a success, both in terms of forwarding the critical missions of the Department and the United States Government to ensure the safety and well-being of our citizens, and equally in preserving the privacy protections the American public has a right to expect. I believe the NAO will not only preserve, but strengthen, these privacy protections.

This will require close cooperation between my office, the Office for Civil Rights and Civil Liberties, Assistant Secretary Allen and his staff, the Privacy and Civil Liberties Oversight Board, and the Office of the Director of National Intelligence. Together we will provide guidance, train staff and program participants, facilitate outreach with the privacy and civil liberties advocacy community, and exercise our oversight role zealously. We will continue to monitor the evolution and operation of the NAO to ensure the use of PII is done so in accordance with all applicable laws and policies. We will update the PIA as necessary, and will, of course, be happy to report our findings back to this Committee at any time.

I thank the Committee for this opportunity to testify about the NAO and its privacy compliance documentation, as well as the Privacy Office's role in moving the program forward successfully. I look forward to answering your questions.

Chairman THOMPSON. Thank you very much. I would like to thank the witnesses for their testimony. I remind each member that he or she will have 5 minutes to question the panel. I will now recognize myself for questions.

Mr. Allen, one of the concerns that I think you heard earlier this morning is that, at present, we have not or you have not developed the written policies for the implementation of this new program. And you further indicated that if that was not the case by October 1, you would in fact delay the rollout of this program. Is that still your opinion?

Mr. ALLEN. Mr. Chairman, what I indicated is that we have been working on issues and the concept of operations. That has been finished and submitted, I believe, to Capitol Hill, including your office. We are working on guidelines, we are working on standard operating procedures.

Chairman THOMPSON. Excuse me. I am not certain if we have that.

Mr. ALLEN. If you don't, I was informed that you do, but I will verify that and get back to you, Mr. Chairman. But we do have a concept of operations. We are finishing guidelines and standard operating procedures, and looking at how to staff and stand up the organization. We think we can certainly meet the requirement that you all indicated that you wanted to have, a greater framework to understand the legal basis, which I think Mr. Teufel just spoke to at least in part, because we are not asking for new authorities or new forms of legislation, because this operates under the National Security Act of 1947, the Executive Order 12333, the Homeland Security Act of 2002, and, as Mr. Teufel said, under the Privacy Act we meet all those standards. We will give you that framework and the guidelines that we have developed, Mr. Chairman.

Chairman THOMPSON. Thank you. I want you to understand that if the authorizing committee asked you today for the written protocol by which you will operate this program, we do not have it in a form that you can present it to us. Am I correct?

Mr. ALLEN. I think we can provide that to you in short order, because we do have the concept of operations, we do have the privacy impact assessment. We operate, as you know, and we do have guidelines and SOPs. We can provide you with significant data.

Chairman THOMPSON. I think it is important for you to provide this committee with all of the information that you propose to operate this program going forward. Do you have a timetable under which we can expect receipt of this information?

Mr. ALLEN. We will provide you the concept of operations today. I thought your committee had it; and, if it doesn't, I apologize.

Chairman THOMPSON. Now, just to talk about a few items associated with this rollout. Is it your understanding that the Privacy and Civil Liberties Oversight Board participated in the development of this National Applications Office?

Mr. ALLEN. The Privacy and Civil Liberties Officer——

Chairman THOMPSON. Not office. The board.

Mr. ALLEN. The White House board. It is aware and has been informed of this particular National Applications Office and the fact it is to be stood up. Yes.

Chairman THOMPSON. Well, if you will provide this committee with any communication associated with that board's notification and participation in the development of this project, in addition to the earlier requests, then I will be satisfied. There is some question as to whether they really know, Mr. Allen, and I want you to understand that.

Mr. ALLEN. Thank you. We will take that for the record and get back to you.

Chairman THOMPSON. Mr. Sutherland, since this program is about to be rolled out October 1, can you provide this committee with when you first participated in the review?

Mr. SUTHERLAND. Yes, sir. Our office was drawn in in late July.

Chairman THOMPSON. Of this year?

Mr. SUTHERLAND. Of this year, yes, sir. Our colleagues at the DNI, the Civil Liberties Protection Office, were drawn in in the fall of last year. Our colleagues at the Privacy Office I know can speak

to this more, but were more clearly involved as the spring came along, and we were drawn in the last few weeks.

Chairman THOMPSON. Is your involvement at this point—just explain your involvement.

Mr. SUTHERLAND. Yes, sir. We have been extremely integrally involved over the past few weeks. We are working on helping to develop the standard operating procedures for the NAO. We are beginning to work on some of the legal and policy working groups that are going to be stood up as the executive committee begins. And so we have been working, getting briefings on the intricacies of the program both at NGA and at NAO, so we have a full understanding of the program and how it works.

Chairman THOMPSON. Thank you very much. I think my concern is that, for the most part, the program was developed and presented to you before you were involved in it.

Mr. SUTHERLAND. I am sorry, sir. Again?

Chairman THOMPSON. If the program was introduced in August and you first saw it in July, for all intents and purposes it was complete.

Mr. SUTHERLAND. If I could use a football analogy. We were brought in in the pre-season. The regular season is going to kick off October 1. We do believe, and Assistant Secretary Allen has said, we should have been brought in earlier. But we do have colleagues in the privacy and civil liberties community who were working on these issues earlier. But there is no doubt we should have been brought in earlier, but we are at a stage now where we feel comfortable we are able to make a large impact and really benefit the NAO with our expertise.

Chairman THOMPSON. Thank you very much.

I yield to the ranking member for questions.

Mr. KING. Thank you, Mr. Chairman.

First of all, thank you for your testimony. It is my understanding that the conversation between you, Mr. Allen, and the concept of operations and privacy impact assessment were given to staff of the committee on August 17. I think this is the document we are talking about. But, in any event, I have it here.

I have listened carefully to your testimony and I would like to know, is there anything that is going to be done under this program which has not been done ad hoc up until now or could have been done ad hoc up until now?

Mr. ALLEN. Congressman King, there is nothing new in the sense we have done this in the past for homeland security when we have had hurricanes, disasters. The Civil Applications Committee is well established, and it still has to go through the whole review of NGA attorneys before any of its requests are acted upon.

As far as law enforcement, we haven't begun that. We are going to stand up a working group between ourselves, DHS attorneys, DNI, and Department of Justice.

So there is nothing new. It will be a broader customer base, I believe, once we are able to tell the nondefense community more about what might be available to support them for homeland security affairs. But the science applications will continue, and we hope to make them stronger than they are today.

Mr. KING. Now, has this been shared with law enforcement before?

Mr. ALLEN. There is a Legal Law Enforcement Working Group that is standing up of Justice, the Director of National Intelligence, and the Department of Homeland Security. They are aware of it and they are looking at applications. As you know, we have on an ad hoc basis the National geospatial Intelligence Agency under the egress of both the DCI and now the DNI and has supported the Secret Service, supported the FBI in certain applications. But those have been for national security events where geospatial imagery can be of assistance in helping protect major events.

Mr. KING. My understanding was, when we had the D.C. snipers 5 years ago, wasn't this program used then?

Mr. ALLEN. Yes. Congressman King, I was requested by the Director of Central Intelligence, George Tenet at the time, acting on a request from Director Mueller, to image the interchanges between Pennsylvania and North Carolina, because of the killings that could occur and had occurred along the interstate, because the Bureau wanted the National Geospatial Intelligence Agency to outline the sites, places where snipers might hide. It was used, and Director Mueller, as I recall, was very gratified.

Mr. KING. I am trying to determine whether constitutional issues may arise here. Is there any thermal imaging involved in this program?

Mr. ALLEN. As far as——

Mr. KING. As far as being able to penetrate residences.

Mr. ALLEN. No. We will not penetrate residences. This is not going to penetrate buildings. There can be some infrared collection of space to look at forest fires, hot spots. We have used this to support the National Fire Service for decades. This was used long before the proposal was made to establish a National Applications Office.

Mr. KING. If I could ask then, Mr. Sutherland and Mr. Teufel, both of you, is there any Supreme Court case on point involving a fourth amendment issue which would pertain to anything which would come under this program?

Mr. SUTHERLAND. We are——

Mr. TEUFEL. Coordinating.

Mr. SUTHERLAND. —coordinating our thoughts on the Supreme Court litigation. There is Supreme Court litigation that sets the parameters under which we will evaluate the program. There was the Supreme Court case a few years ago on thermal imaging that you are talking about. But, to date, we have seen nothing that implicates that litigation. I mean, that litigation and those decisions lay the contours, the parameters under which we will evaluate the specific requests that are made.

Mr. TEUFEL. There is the CAC's decision about the language with reasonable expectations of privacy, and there is well established case law on when law enforcement can fly over in air space and take pictures. But understand that, while we are both lawyers, we are not practicing as lawyers currently in our positions.

Mr. KING. I guess I am getting at, there has been talk about spies in the sky and spying and snooping and everything else. But I am just wondering if there is anything under this program which

has not been done for at least 30 years under both Democrat and Republican administrations, for instance, whether it is in organizations, whether it is hurricanes, which as I see it is what you are going to continue doing but now it is going to be more consolidated and more coordinated.

Mr. ALLEN. Yes, Congressman King. We use it for border security. We are trying to determine how best to employ its capabilities. For border security, for seaport security, critical infrastructure it is very helpful, and for national security events it has been used rather prolifically in the past, as well as natural disasters, including fighting fires and earthquakes. And, of course, it was used immediately after September 11. Within a half an hour, using a sensitive capability, we could see the extent of damage in New York City.

Mr. KING. Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you very much.

Ms. Harman has agreed to start our questioning after we recess and come back. The plans will be, after the two votes, about 5 minutes after the last vote, to reconvene. So we will recess the committee.

[Recess.]

Chairman THOMPSON. We would like to reconvene the recessed hearing. The next questioner will be Ms. Harman from California for 5 minutes.

Ms. HARMAN. Thank you, Mr. Chairman.

Welcome to our witnesses. I have worked with each of you over some period of time and I appreciate your service, and I surely am grateful you are in the positions you have.

Having said that, I am about to deliver as sober a message as I know how to deliver. Number one, I represent satellite central. My district in California is where most of our defense satellites are designed and built. I know a lot about satellites. I spent 8 years serving on the House Intelligence Committee, 4 years as Ranking Member, and I know their capabilities and I know that their capabilities are evolving and it is very serious business to use satellite feed for domestic purposes. And it not only serious right now, but 6 months from now the capabilities will evolve further, and we will be able to do more and more. And obviously I am not going to discuss that in a public setting. That is my first point.

My second point is, Charlie Allen, you said this is nothing new, it is just a broader customer base. Well, that is new, a broader customer base. Requests from customers to use materials that are ever more sensitive, for purposes that we may not even understand yet, is new. That is not old. That is new. And sharing information with this broader customer base provides all kinds of issues about privacy and civil liberties of Americans that weren't there before and that is new. That is my second point.

My third point is I have listened up and, as best as I can tell, our two privacy and civil liberties witnesses were not cut into this until this year, July of this year. This program may have been shared with others last year. I know that the origins of it were 2005. And I am surely not saying that it is a bad idea to have a program, but privacy and civil liberties concerns apparently were an afterthought. And I understand that we have in this committee some kind of a privacy document which those who have read it—

and I am not one of those—think is not an adequate document. So that is my third point.

My fourth point is that just telling us that Executive Order 12333, the 1947 National Security Act, the Homeland Security Act of 2002, and the Privacy Act cover this program is not telling me anything. I am a trained lawyer, as some of you are, and some of our other members are, and I want to see the legal document that puts the clear, bright legal framework around this program and is speaking for me. I do not think it should proceed. I oppose the idea that it would become operational until we have that framework and have a chance to review it. I am not talking about delaying unnecessarily. But I am saying that the right way to do this is for Congress—which passes the laws of the United States and protects the Constitution, to review carefully the legal framework for what I consider to be a new program before it is rolled out.

And finally, we are dealing in a context here. And the context is—and I speak as someone truly aggrieved that this administration, post 9/11, rolled out the terrorist surveillance program, decided unilaterally; it would not comply with FISA, something I didn't learn until years afterwards, and has been making security policy in the executive branch without full regard for the laws that Congress has passed. I think that is unacceptable. And that is my context.

So what I worry about is that even if this program is well-designed and executed carefully by all of you, and I take you as a man of good faith, that someone, somewhere else in the administration, could hijack it and use it for other means. I worry about it in this administration and I worry about it in the next administration.

And to remind people who may have a short view of this, there will be another administration. The President may be of a different party, and I think some folks who just say the executive branch should have all the power it needs are forgetting that they may be giving power to a new Democratic administration and they may rue the day that they did that.

So my time is almost out. My lecture has abated. But I have just one question. Has anyone focused on Posse Comitatus and do you know that this program, as you conceive it, will comply with the Posse Comitatus Act?

Mr. TEUFEL. Ma'am, again while I am an attorney, I am not a practicing attorney. Neither is Dan. My understanding is that the lawyers have looked at the Posse Comitatus issue and that it is nonviolated. Again I am speaking as a nonpracticing lawyer here.

Ms. HARMAN. My time has expired, Mr. Chairman, I made my point clear. But I would like to see that answer amplified by someone——

Mr. TEUFEL. Yes, ma'am.

Chairman THOMPSON. Well, I think, Mr. Allen, can you provide the committee with a response to Ms. Harman's question?

Mr. ALLEN. We will certainly respond to that question and also give her the assurances of the legal framework and also how the various concept of operations, guidelines, privacy impact statement—which I think you already have—and the processes by which we will operate. I understand the concerns, but we believe

VerDate Nov 24 2008 09:52 Aug 21, 2009 Jkt 000000 PO 00000 Frm 00027 Fmt 6633 Sfmt 6601 H:\DOCS\110-HRGS\110-68\48963.TXT HSEC PsN: DIANE

that we are ready to operate this particular program starting on 1 October. Otherwise, it will—under ad hoc basis, I think you would want more layered oversight than what we currently have.

Chairman THOMPSON. Thank you very much. Ms. Harman, do you want to make a comment?

Ms. HARMAN. My comment is, Mr. Chairman, that with respect, I don't find that answer satisfactory. I think this committee should insist on reviewing the legal underpinnings of the program and satisfying ourselves that this is being done properly. And I say this on a bipartisan basis, this is the leverage we have. We let this thing go, it may be another blank check to the Executive, it may morph into things that will terrify you if you really understand the capabilities of satellites, and I for one would strongly oppose letting this proceed without doing that careful review as quickly as possible.

Chairman THOMPSON. Thank you very much. And I want Mr. Allen to understand that I made the request; Ms. Harman has made the request again. There is still significant discomfort on the committee that we don't have enough written policies by which this program is scheduled to begin October 1. And that is an absolute unreadiness that I hope you hear from us in this hearing. And we will before the end of the day provide a written letter expressing similar unreadiness on the committee's part.

We are now yielding 5 minutes to the gentleman from Pennsylvania, Mr. Dent.

Mr. DENT. Thank you, Mr. Chairman. And I know Ranking Member King talked about Supreme Court decisions. I would like to follow up on what he talked about. As you gentlemen know, some courts have ruled that the heat signatures emanating from a public residence are protected by the fourth amendment. And in Virginia, as an example, courts have held that utilizing forward-looking infrared radar to detect the excessive heat detected by marijuana-growing operations as the basis for establishing probable cause to search that particular home is improper.

I know that you are not dealing with infrared or heat sensors. Given that example, what kind of safeguards will the NAO have in place to ensure that law enforcement agencies requesting technical assistance in surveillance are complying with the existing State and Federal court decisions regarding the fourth amendment—particularly State court decisions which I think is more operable here.

Mr. Sutherland?

Mr. SUTHERLAND. Thank you. Just to understand the process I think will help. A request comes in for someone to use one of the products or services of the NGA. It will now come into the NAO. Within the NAO, located within the Department of Homeland Security Intelligence and Analysis Directorate, there will be attorneys who review it. There will be a privacy officer and an officer for civil rights and civil liberties who will have oversight of that. So there will be that filter.

The case law that you are referring to will be a significant part of that filter, as well as other case law in other areas. It wouldn't necessarily raise a fourth amendment issue; it could raise other issues. If our internal analysis decides that that is a request that

does meet the proper use, we would then forward it to the NGA, and the NGA has another distinct and robust set of measurements and analysis that they do and have been doing for many, many years.

So what Assistant Secretary Allen is saying is that by bringing the NAO to DHS, which DHS has the unique capabilities of a privacy officer and an officer for civil rights and civil liberties, you are adding additional layers of review onto that analysis of whether that is a proper use of the system. So NGA is a robust way to look through the issues and our Department will have that as well.

Mr. TEUFEL. I would like to expand on that. NGA has the proper use memorandum, PUM, process. When a request comes into NGA, as we understand it, NGA conducts a legal and policy review and establishes controls on the information that will be collected. And if a request is approved, the PUM will specify what can be collected, who can receive the raw data, how it is to be stored, how it can be used and who will receive the final product. So at the NAO, the collection manager will review existing PUMs and say, okay, I have a current request; does it fall under an existing PUM? If not, a new PUM is requested and, as I understand it, NGA has denied PUMs in the past for various reasons. If it falls under a PUM, then the collection manager will go to NGA under the PUM and make the request.

Mr. ALLEN. I would like to add to what Mr. Teufel said, is that the Civil Applications committee falls directly under the same rules and restrictions, even though it has operated for 30 years, and on occasion they have redirected some of the civil application committee requests to make sure they are in accordance with the proper use of that request.

Mr. TEUFEL. When I was at Interior, we did not review CAC requests the way we at DHS will review NAO and CAC requests. It is far more robust oversight than existed previously.

Mr. DENT. I guess my next series of questions—and I will try to be quick—will be directed to Secretary Allen. I guess the main question I have: Is there a risk of overloading our intelligence communities with requests from various civil authorities, and what happens if the NAO receives too many applications for assistance, and how do we process these things timely?

Mr. ALLEN. That is a great question because the process we have today is ad hoc. If there is competition, NGA has to make that decision sort of as the requirements flow in. Now we have a more ordered process to look at the needs of the customers. And then one of the good things, this is a clearinghouse. The NAO is a clearinghouse and sets—not only looks at the needs, but establishes priorities so we don't overburden these classified capabilities that are used almost entirely for foreign collection.

Mr. DENT. How long do you think—how much time would it take between the time of the request being submitted to the actual time of return of the requested information to the civil authority? Do you have any idea?

Mr. ALLEN. If it is a research type of effort that the Civil Applications Committee—it could take days, weeks or months. If it is in extremis, as we did when the World Trade Center was struck by airplanes, that was in extremis and was done in matter of a few

minutes. But as a general rule, it is going to take—it is a very deliberate, considered type of action. It can take days, certainly weeks and months if it is a research type project.

Mr. DENT. Thank you, gentlemen. I yield back.

Chairman THOMPSON. Thank you very much. We now yield 5 minutes to the gentleman from Texas, Mr. Green.

Mr. GREEN. Thank you, Mr. Chairman. I thank you and the Ranking Member for your opening comments. I thought they were very insightful.

I would also like to thank these fine men for the service they are rendering to their country.

Friends, if I may, I would like to share with you briefly this thought. This country was founded, in part, because of the unfetterred access that the king's men had to our property, to our papers; and it was that unfetterred access that caused people to venture across the ocean and come here so that they could establish a system that would give them the kind of privacy that we enjoy to this day.

The Founding Fathers were really brilliant men and—well, of course, there were some women involved—who understood the need and necessity for a fourth amendment. The Supreme Court has held in Kyllo versus the U.S. that thermal imagery is subject to the fourth amendment. The fourth amendment really is kind of the cornerstone, if you will, of the home being the castle. If we allow the unfetterred access by way of satellite technology, which is unchartered space for us, we really don't know exactly where this will end. We know where we are. And if we allow it based upon custom and tradition, meaning we have always done what we are doing, we allow it based upon the notion that we have in-house people who will review this and our in-house people will tell us whether we are making mistakes or not, I think we are making a mistake.

It is not a question of whether it has been done before. The question is whether what was done before was constitutional. The question is whether what will be done is constitutional. So we are at a point where, in my opinion, we have to ask ourselves, do we have the kinds of checks and balances that the Constitution envisions, not the kinds of checks and balances that the executive branch envisions?

We just found that Dr. King's wife, Mrs. King, was being surveilled unconstitutionally by the executive branch. We have discovered that a Congressperson had his papers taken from his office unconstitutionally. The question is: Is this constitutional and are there checks and balances as envisioned by the executive branch? To have the NGA under the executive branch—and let me pause for a second and get this on the record—is the NGA under the executive branch? Does everybody agree that it is?

Mr. ALLEN. Yes.

Mr. GREEN. All right. If the NGA is under the executive branch, it is not comparable even to the FISA courts. It is at best an executive remedy. The constitution requires a broader remedy that envisions the judiciary being a part of something as pervasive as what we are capable of doing with the satellites. My question is: Why don't we have the NGA or something comparable to the NGA under

another branch of government? This is kind of the clearinghouse; do you agree?

Mr. ALLEN. I believe, sir, you are talking about the National Applications Office.

Mr. GREEN. No. The National Applications Office, as I understand it, it will go to the NGA and the NGA will review and approve the collections of information. Is this not true?

Mr. ALLEN. That is not exactly the way it will work. Because the National Application's Office, working with both civil agencies, science agencies, as well as the Homeland Security and potentially law enforcement——

Mr. GREEN. If I may, sir, please. Let me abridge your comments. Will not the National Applications Office receive the request?

Mr. ALLEN. They will receive the request and it will prioritize it.

Mr. GREEN. If I may, please. Will not the National Applications Office then take the request to the NGA?

Mr. ALLEN. After explicit, significant legal review.

Mr. GREEN. Yes, but they take it to the NGA. And will not the NGA then give a yea or nay?

Mr. ALLEN. Another review, yes. If there is a difference, it will be resolved between the two organizations.

Mr. GREEN. A rose by any name—that which we call a rose by any name still smells just as sweet. Call it NGA, call it National Application; either office is under the auspices of the executive, true?

Mr. ALLEN. Both offices will fall under the executive branch.

Mr. GREEN. That creates a great amount of consternation in the minds of constitutional scholars. I believe it does. Why not have NGA—or if we want to talk about the National Applications Office, why not have this under the auspices of the judiciary, something comparable to FISA? Probably I shouldn't say comparable to FISA, but something—something comparable to what FISA was envisioned to be. Why not have it on the judiciary? The President appoints these FISA judges. Why can't we have some other entity outside of the executive to perform these as a clearinghouse?

Mr. ALLEN. I believe that no other element can really understand the customers or——

Mr. GREEN. I beg to differ.

Mr. ALLEN. —or priorities.

Mr. GREEN. I beg to differ. If you are saying there are not other people that have the intelligence and intellect to understand the Constitution of the United States of America, then we need to do away with the Supreme Court.

Mr. ALLEN. That is not what I said. You didn't let me answer.

Mr. GREEN. Let me give you more time.

Mr. ALLEN. There are limits to physics. What we have is an application for civil and homeland security purposes. And the National Applications Office is going to bring into order and focus already existing processes. It will have a broader customer set, as Congresswoman Harman noted, but it will all be done in accordance with the Constitution, in accordance with the laws, and there will be checks and balances.

Mr. GREEN. If I may, please, sir. I have to intercede because I have little time. It will be done according to the executive branch's

interpretation. And that, many times, will conflict with the Constitution, which is why you have another branch to give another opinion that can supersede the executive branch's interpretation. Listen, I am imploring, I beseech you, I beg that you please give some consideration to the notion that we need a third branch of government or another branch of government involved.

Thank you, Mr. Chairman. I yield back the balance of my time.

Chairman THOMPSON. Thank you, gentlemen. The time has expired. Mr. Allen, I hope you get the understanding that the committee desperately needs the guidelines under which this program is expected to be implemented. And the discomfort you continue to hear is the lack of information that we have, and I think you will hear it throughout the hearing.

I yield 5 minutes to the gentleman from California. Mr. Lungren.

Mr. LUNGREN. Thank you, Mr. Chairman. This is a most interesting hearing and I appreciate what the gentlemen at the table are attempting to do, and I appreciate what members of this committee are attempting to do. But let us see if we can clarify this a little bit.

On the fourth amendment questions. In Florida v. Riley, the United States Supreme Court said that surveillance by helicopter at 400 feet did not implicate the fourth amendment because anybody could be flying over at—a plane could fly over and observe things.

In the Dow chemical v. U.S. case, where it was a business that they were talking about, aerial photography over chemical company complex, they found it was not a fourth amendment search. But Justice Burger, Chief Justice, said this: It may well be, as the government concedes, that surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally prescribed absent a warrant, but the photographs here are not so revealing of intimate details as to raise constitutional concerns.

It appears that the courts have viewed even sophisticated aerial photography from satellites is not implicating the fourth amendment because you are using enhanced techniques, but you are basically doing what you could do if you were flying a bit lower, and protecting yourself by being at a higher level. But—wait a second. The question that comes up is with thermal imagery, because in the Kyllo case that the gentleman suggested, in an opinion written by Justice Scalia, they talked about—this is a law enforcement case using thermal imagery in a law enforcement investigation against a home. And we were talking about the right of privacy really implicating itself when you are talking about a home.

So I guess my question is this: Are all three of you agreeing that this program does not send it to thermal imaging of homes? Would that be correct?

Mr. ALLEN. That is my view. As I said, we can use infrared in a broad sense to look at forest fires and hot spots, but not homes. There is a huge difference.

Mr. LUNGREN. You are using infrared and those sorts of things to look at hot spots. The idea of thermal imaging to penetrate a house is to see—in cases we had in California when you are dealing with marijuana, you were trying to find out whether marijuana

grows there. The courts basically said, absent a warrant, you couldn't do that. You could actually get a warrant to find out the electrical bills of a company and look at it that way, but still you had to have some basis to get it. But the idea was that somehow that imagery allowed you to penetrate the walls and see people.

That is different than finding hot spots to locate the presence of fires or look at agricultural grows and those sorts of things. And that is all that I want to make sure we are doing. Because when I saw the article that appeared in the New York Times, and they are talking about spy satellites being used domestically, the idea was we were violating the fourth amendment. But if what you are telling us is what you had done before, where we use sophisticated technology, we enhance the view that we get from satellites so that we can see what can be seen by the eye if you were there at a lower elevation, that is one thing. And that doesn't bother me because that passes the test. I mean, it passes the Supreme Court test in every single situation. But the specter has been raised by the headlines to suggest that you are going to spy on people in their homes, violating my-home-is-my-castle doctrine which underlies, really, the basis of the privacy protections in the Constitution.

I think that is where you have members very concerned. And if you could be very explicit in your rules that that is not what you are doing, I think you resolve a lot of the problems we have here. And the American public then realizes we are not talking about looking into your bathroom, we are not talking about looking into your bedroom. We are talking about things that are otherwise visible if you were there in closer proximity. That is all I am trying to get from you.

Is that your understanding and will that be incorporated in the documents that you have that we will be able to review?

Mr. ALLEN. That is well understood, and we can demonstrate that that is the case, that we are not here, it does not penetrate buildings, it does not penetrate homes. This is to be used in a much broader sense as you have described. And the differentiation is very significant. I will let Mr. Teufel——

Mr. LUNGREN. Is there anything I said that you disagree with?

Mr. TEUFEL. No, absolutely not. If the national technical means were to be used in that fashion and there were not a warrant, as required under the fourth amendment of the United States Constitution, my colleague, Dan Sutherland, and I would be racing over to see Charlie Allen to talk to him about the improper unconstitutional use.

Mr. LUNGREN. That is incorporated in the principles that you have in the documents that you are bringing forward; is that correct?

Mr. TEUFEL. And it is also part of NGA's PUM process. And NGA would not allow such an inappropriate, improper use of the satellites.

Mr. LUNGREN. But it is part and parcel of the documentation that you have that regulates this program and that we are going to have a chance to look at; is that correct?

Mr. TEUFEL. The Constitution of the United States, sir.

Mr. LUNGREN. I am talking about the principles laid out in the way you are going to operate.

Mr. SUTHERLAND. If I can say, the concept of operations incorporates that. Yes, we are working on standard operating procedures for—they are in draft form, yes. And the executive committee, as it forms, and the working groups that come from it will incorporate all of this. So the answer is absolutely yes.

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

Chairman THOMPSON. Thank you. But the point, for the committee's sake at this point, is that at present there is no such approved document that guarantees just what Mr. Lungren said, other than the Constitution of the United States?

Mr. SUTHERLAND. Chairman Thompson, right now there is a concept of operations document that is set final, and I believe it has been provided to staff. But this is what Secretary Allen was saying earlier. He will make sure that is in everybody's hands by the end of the day. But in the upcoming weeks, we have a standard operating procedures document and other documents like that. And as I think we have been saying, we clearly need to be working with the committee, as we form those, in giving you visibility on this to give everybody the level of comfort that they need to have.

Mr. ALLEN. That is correct. We provided, I believe, the concept of operation on the 17th of August. As you know, we also worked with the Intelligence Committees to ensure they had no concerns, and briefed them as well as the appropriators. So you need to have more materials to satisfy your needs.

Chairman THOMPSON. Excuse me. You briefed the appropriators but not the authorizers. I think that is the point. And whatever documents we have received, we got them from the appropriators. We did not get them from the Department.

Mr. ALLEN. We did brief the HIPC, which authorizes my budget, since it falls under the national intelligence program. We did not brief you from an oversight perspective, and I have apologized for that.

Chairman THOMPSON. Well, the standard operating procedures are yet to be received by this committee. And I think until we receive those documents by which this program is to go forward, it is not in the best interest of any of us for that October 1 to come with you implementing that program.

I yield 5 minutes to the gentleman from Colorado, Mr. Perlmutter.

Mr. PERLMUTTER. Thanks, Mr. Chairman. I really don't have that many questions. It is more of a statement, and I apologize for missing a number of the questions that you have been asked. You three gentlemen come to this committee—and I think the committee and I know I hold all of you in high regard. And the real disappointment has been we feel like you have gotten the cart before the horse, that this thing really has—is a fait accompli—and some of the others may have said this-before you really took time, in our opinion, to look at the privacy issues that come with this.

And, Mr. Teufel, it is a big difference between going from the Interior Department and the U.S. Geologic Survey to the Intelligence Department of Homeland Security. There is a major shift in em-

phasis just by going from one place to the other. And if it is only that, these protocols and procedures have to be in place.

And the fact that we are the last people to hear about it, as some of you in the Privacy Department of the Homeland Security were, that is the problem. And and some of these things, as Mr. Lungren has said, and I think Mr. King too, have been going on a long time, whether it is for Hurricane Katrina or maybe a national security event.

So we need to know, though—and there may be instances, Mr. Allen, where you might want to be able to view into a home with infrared. But obviously if that is the case, we want to have some procedures that comply with the Constitution.

And it isn't just the courts that set those parameters as to what the first amendment means or the third amendment. I mean, everybody talks about the fourth amendment, the warrantless,—the need for warrant. But the third amendment says you are not going to have government in your house, period, except during times of war.

And my comment—and I guess how in the future, Mr. Allen, can—as you develop new programs, can you include the privacy side of the Department earlier on and contact us earlier on? I am on the Intelligence Committee of this committee and really hadn't heard anything about it until we got the papers a few days ago.

Mr. ALLEN. And I appreciate, Congressman, your concerns. And as I said, the legal framework, the guidelines, the procedures, the protocols, we have a good number of them in place and I think they will meet your needs and requirements. One of the things that came very late, of course, was the Director of National Intelligence letter of designation which put into motion full planning back in June. We only received the actual letter of designation that the Secretary of Homeland Security will be the executive agent in June. So we had done some preliminary planning, but now we are doing it full bore.

So part of it is catching up with the fact that now we are working with the Civil Applications Committee, the Department of Interior, the U.S. Geologic Survey and others. We had set a tentative date to begin operation around 1 October. We advised the appropriators of this and they have provided us with reprogramming so we can spend some dollars to get ready for this.

But I understand your concerns, procedures, protocols, guidelines. We certainly will give you the legal framework which we have outlined already. But this has been probably one of the most reviewed programs, certainly, in the executive branch. That has been my experience. But I understand your concern.

Mr. PERLMUTTER. Thanks, Mr. Chair.

Chairman THOMPSON. Thank you very much.

We now yield 5 minutes to the gentleman from Washington, Mr. Reichert.

Mr. REICHERT. Thank you, Mr. Chairman. Thank you all for being here. It is good to see all three of you again.

I just want to follow up on some of the same discussion and conversation you have heard here this morning already. First, Mr. Allen. Was it an oversight on your part not to include the civil

rights and civil liberties and chief privacy officer until later on in the process, or was that——

Mr. ALLEN. We had the DNI's civil rights and civil liberties officer involved in November of 2006 when we started talking about the fact that this could come to Homeland Security with a letter of designation which we didn't have at the time, and Mr. Teufel, I believe, had an officer with that working group. We got the letter of designation and, of course, the civil rights, civil liberties, and Mr. Teufel did a privacy impact statement this spring and early summer. So I think we have worked very much, as these gentlemen have stated, in close cooperation and collaboration with both officers.

Mr. REICHERT. Mr. Sutherland testified that he came into the process in July. Do you agree, Mr. Allen, he should have been brought into the process earlier?

Mr. ALLEN. In retrospect I think that would have been the case. But we have worked cooperatively on all issues with Mr. Sutherland.

Mr. TEUFEL. Sir, if I may. I had the opportunity to speak with Alex Joel, who is the civil liberties protection officer over at ODNI. I know what my office's timeline was and I wasn't quite sure what his was. Alex Joel became aware of this process back in October of 2006. And in November of 2006, a member of my staff participated in a working group or the entity that was brought together to look at this. And both Alex and my staff were aware that at the very beginning, back in November or shortly after November 2006, put into the documents is the privacy officer and the civil rights and civil liberties officer must be working—we must be working with them on this to ensure that we protect privacy and civil liberties.

Now, my office got more heavily involved with the NAO in spring of 2007, and for a period of time—I want to say between 1 and 2 to 3 months—my office worked with the NAO and INA to put together this privacy impact assessment.

Mr. REICHERT. Would you disagree with the member of the second panel that has provided testimony that you were marginalized in this process?

Mr. TEUFEL. I haven't seen that testimony.

Mr. REICHERT. Do you feel you were marginalized in this process?

Mr. TEUFEL. No, not at all. Since I have been in the office, I have done a great deal working with Charlie and folks on his staff to get the privacy office more deeply involved with the things that INA is doing so that we can be there early and often to make sure the privacy protections are in place.

Can we do better? We can always do better. But I have got a very good close working relationship with Charlie Allen and his staff, as does Dan. Dan and I worked together very closely, as we do with our colleague over at ODNI, Alex Joel. So I would disagree that my office—and, for that matter, Dan's office—has been marginalized.

Mr. REICHERT. Can you explain to me, then, what the process is when you do witness a violation? What happens?

Mr. SUTHERLAND. Congressman, we deal with issues that cover the whole gamut of the Department of Homeland Security and the homeland security efforts. So we deal with them essentially the same. We go to the people responsible for the program and explain our views on why they might shape the policy in a different way. If we are—Hugo and I both talked about this publicly. If we feel that there are major concerns, I report directly to Secretary Chertoff. I have great relationships with Assistant Secretary Allen and his peers in the Department, and we talk regularly. So we would go directly to senior officials and raise these issues.

Mr. REICHERT. Your investigative policy would be put forward, you would investigate the issue and come out with a finding?

Mr. TEUFEL. Sure, if necessary. If there is a problem, typically it is resolved at the staff level. If it were to get to me, and, I assume probably also with Dan, I am going to make a phone call to the principal or that principal's chief of staff within the Department to say, hey, we have got an issue here we need to address. Around the same time, I am going to be in contact with the general counsel's office to let them know there may be a legal issue that needs to be addressed. If it doesn't get resolved then—and it has never been the case that we haven't resolved an issue when we have been speaking with the component head—then I am going to the Secretary and the Deputy Secretary with my concerns.

Mr. REICHERT. If I may, Mr. Chairman, one last question, a simple question. Does moving the Civil Applications Committee from the Department of the Interior to the National Applications Office within Homeland Security create new risks to the privacy and civil liberties of U.S. citizens?

Mr. ALLEN. I will let my colleague speak. But we are going to continue the same processes, only with greater layers of review from the Civil Applications Committee. My commitment to the CAC, as it is known and been known for many years, is to give it robust support so that it—scientific research, particularly on things like climate change and environmental damage can be continued. They have done some great work. The CAC needs stronger support, and I intend to give them that and I will let my colleagues talk about the civil rights/civil liberties aspects.

Mr. SUTHERLAND. Congressman, we believe there are additional layers of review and analysis that are brought to bear with this new structure. That did not exist before. Protections, procedural protections that are in place. Certainly when you expand the customer base, there are going to be novel—I presume there will be novel requests for use of the technology. That is the reason why it is great to have the increased scrutiny that the NAO brings.

The Department of Homeland Security is unique in the Federal Government in that we have a chief privacy officer who sits in the position, and with the authorities that Hugo does, and officer for civil rights and civil liberties. We are a unique department in that sense and that is one of the values of having the National Applications Office within this Department.

Mr. REICHERT. If I may just comment quickly, Mr. Chairman. I appreciate your testimony and I do share the same concerns that the rest of the members of the committee have shared with you, but I do have a great amount of faith in your abilities to protect

our Constitution. But I do think that the oversight, as Mr. Allen and others have said, and the access to that report would be a great asset for us.

I have personal experience in asking for assistance from the Secret Service and the FBI—in some of this technology that you talk about—back in the mid-1980s and it was denied to local law enforcement, the sheriff's office that I happened to be the sheriff of back in Seattle. So I know there is some oversight there. At least back then. And I am certain that Congress was made aware of the technology when it existed back in the middle 1980s.

And I appreciate your testimony. Thank you.

Mr. TEUFEL. If the fourth amendment required a warrant before, the fourth amendment requires a warrant today. And if there are any violations of intelligence law or policy, they have to be reported to the President's Foreign Intelligence Advisory Board and potentially to the Attorney General. So I just wanted to advise you all of that.

Chairman THOMPSON. Thank you.

I yield 5 minutes to the gentleman from North Carolina, Mr. Etheridge.

Mr. ETHERIDGE. Thank you, Mr. Chairman.

Let me thank each of you for being here and also for your service. And I will say from the outset, so you know where I am coming from, I agree with Ms. Harman. I think that we have got work to be done in this area.

I hope you understand why this committee is so sensitive to this, of what is going on. When you read it in the paper first, it puts us in a defensive mode to start with.

So that sort of leads me to my question. I served in the State legislature one time with what I thought was an outstanding legislature, but also a great attorney, and I remember one comment he always made. When he was a trial attorney, he always wanted to depend on people trusting him. But when he got to the General Assembly, he always wanted to know about the law. He was concerned about what the underpinnings of the law are.

I think we are here in an area where where a high level of trust you can delegate to people you trust. But what happens to those people who follow when you don't have firm, hard guidelines with underpinnings of the law? Let us talk beyond that. Because I think it is critical and we are getting on an area where Mr. Allen said earlier, we are talking about an expanded customer base. We are in a new area. This hasn't been there before.

So my question is this, I guess. What has sparked the need to expand the access to spy satellite imagery? And I guess my big question ought to be why was the former system so inadequate?

Mr. ALLEN. The former system was—I don't know that it was totally inadequate. It did excellent work. All that the commission—and we had distinguished Americans serve on it and studied it and recommended unanimously that there probably were some opportunities that were being missed to help protect the homeland, to provide greater security on things like ports and borders and infrastructures; that we should address those kinds of requirements.

What it recognized was that these are capabilities that probably could be used with great care—because it emphasized civil rights

and civil liberties and privacy in this report back to the Director of National Intelligence—was that there could be greater opportunities to help keep the country safer and more secure. That is the reason that the report—the study was conducted. The DNI did not designate the Secretary of Homeland Security until June of this year, just 3 months ago, a couple of months ago, as the executive agent. We are now working hard to get the protocols in place.

Mr. ETHERIDGE. Let me follow that. Can you provide examples of requests you would feel exceed the existing legal limits? And secondly, are you aware of any such potential abuses of the spy satellite imagery that occurred in the wake of Hurricane Katrina; because you talked about having to use it for that, to help with that?

Mr. ALLEN. I will let my colleagues speak about any violations. I was not at Homeland Security when it was used in Katrina and Rita, but it was used. It was very valuable. The National Spatial Intelligence Agency did good things to bring capabilities in a hurry to help save lives and to prevent further damage to our country, particularly down in Louisiana and Mississippi. It was of great use. The Secretary of Homeland Security deeply appreciated that capability. But I know of no violations of any law during that. Now, as far as what might be violations of the law, I leave it to my colleagues to discuss.

Mr. SUTHERLAND. One can always imagine hypotheticals that would violate the law. You pointed out it would be difficult to imagine a fourth-amendment issue in this context, but we will certainly be looking at it. And the advantage, as I said before, of having the NAO within DHS is you add a layer of several additional attorneys, and then those with specialties in the area of privacy and civil liberties more generally, who are going to be reviewing these. So one can imagine hypotheticals. That is our responsibility, is to look at the—when we have an increased customer base, hopefully you will have increased quantity of requests for this outstanding technology. Our job is to make sure that increased quantity does not sacrifice quality, and we will be able to do that in a number of different ways.

Mr. ETHERIDGE. Mr. Chairman, it seems to me in closing that the request that each member has made, I think thus far—and I echo that—that we spend more time with you, and getting your hands on the documentation so that we can feel comfortable; and hopefully in the future others can feel comfortable and the American people can feel comfortable that we really are working to protect them, as I know you are, but also protecting our civil liberties as well as theirs.

Mr. ALLEN. Thank you, Congressman. We will do that.

Chairman THOMPSON. Thank you very much.

Yield 5 minutes to the gentleman from Georgia, Mr. Broun.

Mr. BROUN. Thank you, Mr. Chairman. I believe in my heart you are honorable folks and I believe, as you state very fervently, that there are protections within your agency. That doesn't satisfy me. Frankly, I don't believe this horse is dead yet, so I will beat it more.

I agree with Ms. Harman that I think you have a real Posse Comitatus problem here and also I know that technology is expanding tremendously—minute by minute almost. And I have a tremen-

dous distrust of government. And I am not assured by you gentlemen that there are sufficient checks and balances put in place, because what I hear from you-all is that the agency can police itself and there is no outside policing of the agency by some separate entity of government.

As Mr. Green was talking about, I believe very firmly that there needs to be some outside review, there needs to be some way of going to check the agency itself. We are talking about a new agency. We are talking about new technology. We are talking about advancing technology. And I believe that every person on this committee wants to make sure that this Nation stays safe and secure. But I for one am not willing to give up my liberties and my constitutionally protected God-given rights to your agency or any other. And I hope you see from all of us that there is a tremendous concern here.

I am new on this committee and I am just trying to get ahold of things that are going on. And it just deeply concerns me as a new Member of Congress about what you are telling me, because I don't see any outside review. I don't see any sort of effort on your part of looking beyond the agency itself.

So please reassure me, how—when there are other people sitting in your seats, how in the future, as new technologies develop, how as we advance a year, 5, 10 years from now, that there won't be intrusions into people's privacy and their private lives so that we can protect our homeland, that we can protect the national interest, but that individuals, law-abiding citizens aren't under danger. And I don't see that. Frankly, I don't see that and I don't hear that from this testimony today.

So if you-all could assure me, I would feel a whole lot more comfortable and hopefully the other members of this committee will, too.

Mr. ALLEN. I think we have gone through the layers of review. And this is an office within a Department, and there are layers of review there. There is another whole agency within the intelligence community called the National Geospatial Intelligence Agency which has also significant reviews and they only—they only do this where there is a proper use memorandum. There are—and there is significant review of them.

There is also the Director of National Intelligence who has his own civil rights/civil liberties officer. And the DNI is, you know, responsible to ensure that all of his activities are under his—he designated this to the Secretary, or done legally and properly. There is the President's Foreign Intelligence Advisory Board, PFIAB, and under it is the Intelligence Oversight Committee which also looks for any violations of intelligence law, of intelligence operations and activities. So there is huge review. And it is beyond just this office, which I will be the operations manager within the Department. But I will let my colleagues talk about proper use. And, of course, probably the most significant review is here today, the Congress of the United States.

Mr. SUTHERLAND. I think Secretary Allen said it well. I think Mr. Toefel and I both have been getting briefings on the capabilities of the system, and I think the technology, which the Secretary could speak about much more articulately than I can. The tech-

nology and what the purpose of the imagery is, is not concerning just the capabilities of the system. And I don't know if you have been able to talk about that a little bit more.

Mr. ALLEN. The capabilities, I know and I deeply respect Congresswoman Harman. There are limits of physics. We are talking about space systems. We are not talking about, as Congressman Lungren pointed out, airborne or other kinds of manned or unmanned aircraft. We are talking about systems today, a great deal of the requirements probably as they come in from these civil users, non-Defense users under the National Applications Office, a lot of them could be satisfied by commercial imagery. Commercial imagery is a growing industry, and commercial industry has capabilities that are reaching and approximating those of classified imagery satellites. And there are many waiting to be launched around the world.

So I agree with you, we are in a different era where technology is driving us into a world of deeper concern. And no one has more concern I think than I do, given my career with intelligence and with the Central Intelligence Agency.

But from my perspective, there is significant oversight throughout these processes. And these systems are not directed at individuals, because these systems are not capable of that from space. And we are talking about a space-based system here.

Mr. TOEFEL. I just want to add, sir, I share your distrust of government. That is why I took the job that I hold presently. And I know that the Founders had a profound distrust of government. And so when they crafted the Constitution of the United States, they made it a limiting document, limiting what we all can do, we who work in the Federal Government. And so I am very focused on that because we all have sworn an oath to protect and defend the Constitution. And so I want to tell you that, that the Constitution means a great deal to me.

There are a number of agencies that are involved in oversight here, far more than existed previously. A number more people who are going to be looking at this thing, including career employees, career employees in my office who in our close work with INA are becoming more and more involved at an earlier and earlier level with intelligence and analysis activities. And they have various protections under the law that, if necessary, to protect their country and the Constitution, they can and doubtless will exercise.

Chairman THOMPSON. I can appreciate that. But I have asked Ms. Harman and Mr. Carney to expand on this whole issue from the Committee's perspective in their chairmanship. There are some real concerns that we have going forward with this program that I have heard from everyone. And some of the things that are being said, I am not comfortable with. The technology can do a lot of things, and people saying that it can't causes me real concern. But those two individuals kind of take the leadership.

Mr. Carney is chairman of the subcommittee for the full committee, and I will yield 5 minutes to him.

Mr. CARNEY. Thank you, Mr. Chairman. I do have a number of questions, but first I will yield 30 seconds to my colleague from Texas, Mr. Green.

Mr. GREEN. Thank you, Mr. Chairman. And thank you for yielding.

Two things. One, the Constitution, the Fourth Amendment contemplates privacy in the home. But it really concerns privacy, and the home is not the only place where the Fourth Amendment contemplates privacy.

The second point: If you have an issue that you deem to be important enough to take to a court to receive a proper warrant, what court would you take it to?

Mr. SUTHERLAND. I assume, sir, that it would be taken by the prosecuting attorney in whatever jurisdiction which they are seeking to use that information.

Mr. GREEN. I ask this question, Mr. Chairman, because it may be necessary for us to deal with jurisdictional questions in terms of the judiciary as it relates to the issue of what court they would eventually go to, assuming they had a legitimate question they wanted to bring up.

Finally, I would make this comment. I respect you, sir, and have great appreciation for what you are saying. But J. Edgar Hoover, who was the head of the FBI, a great patriot, spied on Dr. King. The FBI spied on Mrs. King after his death. It was all unlawful. So, we cannot assume that the Executive is going to be judicious when it comes to the Fourth Amendment.

Mr. TOEFEL. You are right, sir. So let me point out that, under the 9/11 Commission Report bill——

Chairman THOMPSON. The gentleman yielded back his time. It did not require an answer.

Mr. CARNEY. If Professor Toefel would like to answer, that would be fine.

Mr. TOEFEL. I just wanted to point out that, under the 9/11 Commission Report bill that was enacted, the Privacy and Civil Liberties Oversight Board has far greater independence. And that is the first entity with independence that I would point you to, greater independence than my office or Dan's office.

And then the second office that I would point you to is the various Offices of Inspector General at DHS, at whatever requesting agency, and over at DOD. And the inspector generals have great independence and can look into allegations of impropriety, unconstitutional, unlawful activity whether at DHS and the NAO or over at NGA.

So I wanted to call that to the committee's attention.

Mr. CARNEY. Thank you for that.

With my background, I have a little more faith in our systems and their capabilities than Mr. Allen is letting on, I think, here. Can somebody describe the steps and the process, how this actually works? You get a request from law enforcement agency X. Then what happens?

Mr. ALLEN. You could get a request from the Federal Bureau of Investigation. Today it goes directly to the National Geospacial Intelligence Agency. Under our proposed system, it would go to the National Applications Office, where it would be looked at to see if it is lawful and meets the needs for what for the request, that it is prioritized, and then sent over to the GNGA where it is looked at again for its proper use, under the Proper Use Memorandum

which the Bureau would have submitted. And then, if it is proper and lawful, it will then be put into the system to get access to conduct, collect that imagery. The NRO would do that. The NRO simply operates the satellites. And then the material would come back and then be geospacially looked at and read out by analysts. The U.S. Geological Survey has its own analysts, and they do a great job. Some of the material is read out immediately by the National Geospacial Intelligence Agency.

So it works very well today, but I think it could work better under this National Applications Office, certainly a broader set of customers.

Mr. CARNEY. How long does this take, this process?

Mr. ALLEN. We are getting into classified areas when we talk about capabilities of our satellites.

Mr. CARNEY. No. How long does the process take?

Mr. ALLEN. The process can be very quick. It can be a matter of hours, or it can take a significant longer period of time if it is a routine, a nonemergency type of request. I mean, I am restricted on speaking specifics about our classified satellites and their capabilities.

Mr. CARNEY. That, I understand. But I am just talking about just the process here. We are talking about novel issues sometimes. I think that was Mr. Sutherland's term.

Mr. ALLEN. If it is a novel issue, I am sure it would be given a lot of scrutiny and would take significant layers of review before. And if it was decided not proper, the requesting agency or department would be told it was improper.

Mr. CARNEY. Are we talking days, weeks, hours?

Mr. ALLEN. It depends on the urgency. Because—I think you all do not have a clear idea of what the NAO is. It is a clearinghouse that looks at needs and/or requirements from non-Defense users, potentially, and then to help look at those; if they are competing priorities, to help make recommendations to the NGA on which takes precedence. So we view this generally as sort of a nonurgent, nonemergency process. But if a hurricane hits Louisiana or Mississippi, we obviously are going to give it high attention. And NGA will turn it around in a very quick period, certainly overnight.

Mr. CARNEY. But for law enforcement applications, how does that work?

Mr. ALLEN. We are only now forming a legal working group under DHS, DNI, and the Department of Justice to look at how law enforcement uses might be employed. But it would be on a case-by-base basis. So this is downstream. This is not my highest priority. My highest priority is to make sure that homeland security, along with civil applications, gets full support.

Mr. CARNEY. Well, there are criminal applications in Homeland Security. For example, legal immigration, et cetera. The concept of operations and the SOPs, two different things obviously. The Con Ops have been done for a few weeks now. Is that correct?

Mr. ALLEN. We provided it I believe to your staff on 17 August, is what I was told by my own staff.

Mr. CARNEY. And the SOPs should be done, when?

Mr. ALLEN. We are working on the SOPs. Some of the guidelines are done at this stage. Others are yet to be completed. But we are moving ahead.

Mr. CARNEY. Will the SOPs be completed by the October time frame?

Mr. ALLEN. I believe, as we understand how to use—for example, if we ever use law enforcement applications directly, that is downstream. Most of the standard operating procedures will be available and the guidelines by 1 October. I believe we can meet that deadline.

Mr. CARNEY. Certainly, Mr. Secretary, you understand that we are anticipating downstream; we are trying to do that, too, to make us all think about how this is going to go forward. We all have jobs to do, we all have our roles in protecting this Nation, and we've got to get it right. So I just want to get as much clarified up front as we could.

Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you very much.

We yield 5 minutes to the gentlelady from Texas, Ms. Jackson Lee.

Ms. JACKSON LEE. Thank you, Mr. Chairman. And let me thank you for the hearing; as well as the subcommittee chairwoman, Ms. Harman, for her insight.

Allow me to first of all lay the framework and make it very clear that I don't intend to suggest untoward activities or thoughts behind this program by any of the individuals who work for the American people. I believe your intentions are well. However, I have come to understand since being on the Select Committee on Homeland Security, this Committee was set to ensure or to assure the American people that the Congress of the United States must have as its highest priority the securing of America. So I would take great issue and offense and will continue to have this offense to have discovered this process and program in the Wall Street Journal.

And then it seems that the administration embraces August as a month where they make big announcements. Maybe it is so that you can have the complete limelight, and Congress is not in session. But that, I think, does damage to the constitutional premise of the three branches of government and how we are to work together. So we find that you issue a fact sheet on August 15, 2007, which leaves a great deal of question as to the good purposes and good intentions of making sure that Congress and this Committee is a real partner.

We have a very important responsibility that I will never undermine or deny, to protect the American people, but also their civil liberties and civil rights. Let me remind you of an incident by the former majority leader of this Congress, Tom DeLay who decided to use the FAA and to use a government plane, and I will not suggest it was Department of Defense because our facts get somewhat strayed, to go after State legislators in the Texas legislature regarding a question of redistricting. I am sure the utilization of the plane on behalf of the United States of America and the American people was originally of good intentions but, unfortunately, ultimately a member of this body abused the process. So abuse is not

unknown to government. And I would simply suggest that our concern is more than legitimate because of the way, first of all, that we were apprised of it. It almost seems that we wanted to make sure that we were not a partner.

Let me pose this question to Mr. Allen and again thank him for his service. I know that it may have been raised before, but we realize that these satellites are coming in from the Department of Defense, and we know how to find a firewall that we want to keep, based upon the Posse Comitatus Act, and we also know that you have had for 30 years access to the National Geographical Survey Civil application system, which is also a satellite. What precise mechanisms are going to ensure us that we are not violating the Posse Comitatus Act with the use of this spy satellite? And again, if you would recite for me the firewall, the, if you will, complete concreteness that there will not be an abridgement of the civil liberties of individuals who could be caught up in the fishnet of the local law enforcement requesting utilization of this equipment, Mr. Allen.

And if all would answer this question, I appreciate it.

Mr. ALLEN. I think all should comment. We certainly want to keep you informed and be transparent. I have told the chairman that, evidently in this case, we did not fully brief him or his subcommittees at a level that was required, and that is regrettable. And I have said that, and so did the Secretary of Homeland Security has said that.

Ms. JACKSON LEE. And it opens us all up to exposure.

Mr. ALLEN. So let me again say that that was not done well. But I think we have set forth here an organized structured process to bring into order processes that are occurring and have occurred over decades for other purposes than just civil applications. Scientific research. We want to continue that. And we believe that, in response to the Blue Ribbon Commission that there are other things that we can do on a very protected basis for civil rights, civil liberties, and privacy to help assure better the security of this country. We do not call them spy satellites, we call them remote sensing capabilities or classified satellites. These are imagery satellites that we are talking about. We are not talking about anything beyond that.

I will let me colleagues again speak to any issues relating to constitutional questions or Posse Comitatus or questions of firewalls.

Mr. SUTHERLAND. Congresswoman, we have described the different layers of review that are incorporated here and the concepts that you are laying out and other members are laying out about the importance of protecting civil liberties. That is a principle that has been embedded throughout. I laid out in my testimony why I am optimistic that we will have a good working relationship to be able to bring the kind of analysis that you are talking about into the work of the NAO.

I think that much of the concern here in the Committee could be alleviated by more extensive briefings from NGA, which again has had nearly 30 years of experience in working through these issues and how they deal with Posse Comitatus, how they deal with routine requests, and just to have a depth of understanding of how

they deal with their process onto which then we are adding additional layers of review.

Ms. JACKSON LEE. Mr. Toefel, you are solely responsible for this. Give me a straight answer on the Posse Comitatus, please.

Mr. TOEFEL. Ma'am, I will do the best I can. Understand that I am the privacy officer; I am not in a legal position, and I am not here testifying in my other government capacity as a judge advocate in the Army National Guard. So I will do the best that I can do to describe the Posse Comitatus Act, but it is really something for our lawyers to do.

As I understand the Posse Comitatus Act, it prohibits direct support to law enforcement activities such as arrests. When in title 10 status——

Ms. JACKSON LEE. Using Department of Defense.

Mr. TOEFEL. Yes. When in title 10—and if I recall correctly, the language of the Posse Comitatus Act addresses the Army and the Navy. Again, I am here as the privacy officer, not as a judge advocate or a representative of the General Counsel's Office at the Department. So if I am getting this incorrect, understand it is a policy guy speaking with you, ma'am, trying to do his best to answer your question. So——

Ms. JACKSON LEE. I am just trying to get you to help Mr. Sutherland.

Mr. TOEFEL. I am doing the best I can, ma'am.

So NGA can provide indirect support, technical sorts of things, but it must be done under the direction of law enforcement. Again, as I understand the Posse Comitatus Act.

There is no Posse Comitatus Act implication if the national technical means are used under title 50 status. And, as I understand it, they can then provide support. But, again, this is as a nonpracticing lawyer trying to answer the question about whether the Posse Comitatus Act applies.

Ms. JACKSON LEE. I know my time is up. I just want to say that I think they have tried their best to answer the question, but it has not been fully answered, and we need to pursue it further.

Chairman THOMPSON. I was going to make that point. Ms. Harman had already raised that issue, and I am sure these gentlemen will have that opportunity to respond in writing to some of the inquiries we will have.

Thank you, gentlemen, for your presence and presentation and response to the questions. As you know, we will probably have significant issues to share with you that have been raised with the committee. We look forward to not only your acknowledgement of those issues but your prompt response back to the committee, given this October 1 time frame that we have been told that this program is scheduled to begin. Thank you very much.

Mr. ALLEN. Mr. Chairman, thank you. We look forward to responding and getting back to you promptly. Thank you.

Chairman THOMPSON. Thank you very much.

We would like to ask our second panel to come forward, please.

Chairman THOMPSON. We would like to welcome our second panel. Our witnesses, Mr. Barry Steinhardt is director of the ACLU program on technology and liberty. And Mr. Steinhardt served as

associate director for the American Civil Liberties Union between 1992 and 2002.

The second witness, Ms. Lisa Graves, is the deputy director for the Center for National Security Studies, a nongovernmental organization that researches and advocates for civil liberties on national security issues.

We would like to welcome you to the hearing. And, without objection, the witnesses' full statements will be inserted in the record.

I now recognize each witness to summarize his or her statement for 5 minutes, beginning with Mr. Steinhardt.

STATEMENT OF BARRY STEINHARDT, DIRECTOR, ACLU PROGRAM ON TECHNOLOGY AND LIBERTY, AMERICAN CIVIL LIBERTIES UNION

Mr. STEINHARDT. Thank you, Mr. Chairman.

The government's use of spy satellites to monitor its own people, and let me emphasize that. This is to monitor the American people. This is not weather phenomena. This is not our National infrastructure, bridges or the like. This is people who are being monitored here, represents another large and disturbing step towards what amounts to a surveillance society. Our response, especially the Congressional response to this new technology, will serve as an important test case for how wisely we handle the introduction of powerful new technologies.

Congress needs to act before this new technology, this new tool is turned inward on the American people. We need to establish a regime of checks and balances and law that protects us against their misuse.

The chairman and this Committee have taken an important first step in calling the Department of Homeland Security to account and holding this hearing. You have our thanks, Mr. Chairman. But it has been interesting. I have heard a lot of discussion this morning about the respective roles of the three branches of government here. Most of the discussion about the two other of branches of government beyond the executive branch, that is the legislative branch and the judicial branch, have come from the members of this Committee.

One of the things that I find disturbing about this discussion this morning, not the Committee's participation in it but the Department's, is the degree to which you have been told by the Department of Homeland Security, "trust us; we can handle all of this powerful technology, and we will handle it in a manner that is consistent with our principles and consistent"—they haven't even said consistent with the laws, but I suppose that is implied.

I guess I am from the Ronald Reagan school here, trust but verify. You need to verify that in fact this technology will not be misused. And one way in which you can verify that is to establish a clear legal framework for how this technology can in fact be used. As Mrs. Harman said earlier, the capabilities here are extraordinary. They go far beyond what the human eye can process. These are very powerful technologies, everything from thermal imaging that you discussed a little bit this morning, to infrared, to ultrawide band. We can tick them all off. But the point is, these are extraordinarily powerful technologies, and they go well beyond

what you and I could see if we happened, for example, to be in a helicopter. We need to have laws that make it clear how these technologies can be trained inward on the American people.

Now, there is a very good starting base for all this, and it has been referenced here this morning, and that is Posse Comitatus. In my written testimony, we discuss this in greater length, and with the Committee's permission, we will make available to you a memorandum from our legal counsel on the applicability of Posse Comitatus here. But it is important to remember what the basic principle of the Posse Comitatus and the ensuing Federal statutes was. The notion that military is not to be trained on the American public; it is for our National defense. It is not to be used for law enforcement purposes. These are the Department of Defense satellites. These offices are within the Department of Defense. This is the military. And we need to be very careful that Posse Comitatus and that principle that we not use the military we have trained on the American public; these are not folks who are trained or capable in protecting the rights of Americans. That is why we have set them apart and said, you protect us from foreign enemies, but we do not use you for domestic law enforcement. So I think Posse Comitatus raises important questions.

We have four recommendations for the Committee which I will just highlight now. The first is that Congress should demand and the Department of Homeland Security should impose a moratorium on the domestic use of these satellites and enactment of this program. The moratorium should not be lifted until the Congress receives answers to the key questions that you have already begun to ask and the many other questions that will arise as you learn more details. But that moratorium is extraordinarily important. There is no hurry here. You have heard, if it is necessary to use this, for example, to track a hurricane or even to look at another natural disaster, there is already sufficient authority for that.

Secondly, Congress should not authorize the enactment of this program before enacting statutory checks and balances to ensure not only the proper oversight of this program but that the potentially enormously powerful surveillance tools that are at play here be used properly. This measure should include rules for when domestic satellite use is permissible and be combined with judicial oversight.

Lastly, the Congress should strengthen and make truly independent the chief privacy officer and civil rights officers of the Department of Homeland Security. As Representative Thompson pointed out in his letter to Secretary Chertoff, those bodies, those offices appear to have been marginalized through this process. I think this morning's testimony made that clear as well. It is possible to give these bodies true independent authority where they report equally to the Congress as they do to the Secretary of their agencies, that it is possible to get beyond a discussion which is purely internal to the agency to have those officers report to you, report to the American public, and make sure that our civil liberties and privacy is in fact being protected.

With that I will take your questions. Thank you for your indulgence.

[The statement of Mr. Steinhardt follows:]

PREPARED STATEMENT OF BARRY STEINHARDT

Summary of Recommendations

1. Congress should demand, and DHS should impose, a moratorium on the enactment of this program. The moratorium should not be lifted unless Congress receives answers to the key questions outlined above and raised by the Chair and Congressman Markey.

2. The moratorium should not be lifted until Congress authorizes it.

3. Congress should not authorize the enactment of this program before enacting statutory checks and balances to ensure the proper oversight of this potentially enormously powerful surveillance tool. Those measures should include clear rules for when domestic satellite use is permissible combined with judicial oversight of such use.

4. Congress should also strengthen and make truly independent the Chief Privacy Officer of the Department of Homeland Security, which, as Rep. Thompson pointed out in his letter to Secretary Chertoff, appears to have been marginalized by the department in the course of planning this initiative. Congress should also institute similar independent privacy officers for other arms of our national security establishment.

My name is Barry Steinhardt and I am the director of the Technology and Liberty Program at the American Civil Liberties Union (ACLU). The ACLU is a nationwide, non-partisan organization with nearly 500,000 members dedicated to protecting the individual liberties and freedoms guaranteed in the Constitution and laws of the United States. I appreciate the opportunity to testify about the privacy and civil liberties implications of domestic spy satellites on behalf of the ACLU before the House Committee on Homeland Security.

A surveillance society?

Government satellite technology is representative of a larger trend that has been underway in the United States: the seemingly inexorable drift toward a surveillance society.

The explosion of computers, cameras, sensors, wireless communication, GPS, biometrics, and other technologies in just the last 10 years is feeding what can be described as a surveillance monster that is growing silently in our midst. Scarcely a month goes by in which we don't read about some new high-tech method for invading privacy, from face recognition to implantable microchips, data-mining to DNA chips, electronic identity systems, access passes that record our comings and goings, and even plans for RFID radio computer chips in our clothing and other consumer goods. The fact is, there are no longer any *technical* barriers to the creation of the surveillance society.

While the technological bars are falling away, we should be strengthening the laws and institutions that protect against abuse.

Unfortunately, even as this surveillance monster grows in power, we are weakening the legal chains that keep it from trampling our privacy. We should be responding to intrusive new technologies by building stronger restraints to protect our privacy; instead, we are doing the opposite—loosening regulations on government surveillance, watching passively as private surveillance grows unchecked, and contemplating the introduction of tremendously powerful new surveillance infrastructures that will tie all this information together. (The ACLU has written a report on this subject, entitled *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society,* which is available on our Web site at www.aclu.org/privacy.)

Given this larger context in which the plans for domestic deployment of our spy satellites are being made, several conclusions are clear:

- This step is part of a trend of turning our nation's surveillance capabilities inward upon our own population.
- If spy satellites are to be deployed domestically, it is vital that the most rigorous checks and balances and oversight mechanisms be put in place.
- There is much that we do not know about our nation's satellite surveillance capabilities.
- A moratorium should be placed on this program until Congress receives answers to the key questions about the program, enacts far-seeing statutory protections against its misuse, and explicitly authorizes the program.

The government's use of military spy satellites to monitor its own people represents another large step toward a surveillance society. Our response—and especially the Congressional response—to this new technology will serve as a test case for how wisely we handle the introduction of a powerful new surveillance technology by the government.

Chairman Thompson and the Committee have taken an important first step in calling this hearing. But other steps must be taken before this program is allowed to go into effect.

There is much that we do not know about this classified system of spy satellites that was designed for military and foreign intelligence purposes. One fact seems plain:

The satellites have capabilities that far exceed those that are in commercial use.

- They have far better resolution. They can see much more clearly and in greater detail.
- While perhaps not as nimble as they have been portrayed in popular entertainment like 24 or *Enemy of the State,* they apparently do have advanced targeting capabilities.
- They can and do see far more than the human eye. There is much we do not know about their ability to pierce opaque objects, but there is every reason to believe they have some (and perhaps substantial) capacity to do exactly that with the power to convey information about how Americans live and work.
- The military and the intelligence community are at the cutting edge of technological change. The satellites are only going to grow more powerful and capable and change will occur quickly.

The Congress needs to act before our military satellites are deployed domestically. You must act before they are turned on our own people.

It is vital that the most rigorous checks and balances and oversight mechanisms be put in place. The domestic use of spy satellites represents a potential monster in the making, and we need to put some chains on this beast before it grows into something we cannot control.

Our laws aren't strong enough

The Department of Defense ("DoD") and Department of Homeland Security ("DHS") have strongly implied in media reports that there is no legal guidance available to them regarding the use of spy satellites. Nothing could be further from the truth. Congress has thought long and carefully about this issue. Beginning in 1981 and steadily updated over the subsequent two and a half decades, Congress has passed detailed statutory guidance as to how the military is to act when involved with civilian law enforcement. Currently embodied by Title 10 Sections 371 through 382 of the U.S. Code and military regulations such as DoD Directive 5525.5, federal law controls everything from the use of military equipment and facilities to emergency situations like those involving weapons of mass destruction.

Military involvement in civilian law enforcement is something that Americans have always regarded with deep unease and the Posse Comitatus Act reflects those concerns. When Congress updated the Posse Comitatus Act it did so with careful deliberation. Authorizations for military involvement were limited, originally only allowing the military to operate directly in one area: suppression of the drug trade at the border. Congress generally limited the military to indirect assistance—loaning equipment and training civilian police. Direct action by the military could only be undertaken outside the United States.

These laws have been updated over the years, but the basic prohibitions (currently embodied in 10 USC 374) have remained intact: direct assistance by the military is permitted only for a limited number of crimes, and monitoring of individuals is largely limited to the area outside the continental United States. DoD and DHS simply cannot be allow to step in and pretend that none of these rules apply and that this substantial body of law does not exist.

While there is substantial law to be applied in this situation, it may not be sufficient to contend with the new reality of military spy technology stationed miles above the earth, rather than soldiers with their boots on the ground.

Unfortunately, given uncertainties about the precise technical capabilities of the spy satellites and the applicability of the Posse Comitatus Act in this context, Congress cannot regard the act as a reliable legal bulwark against the abuse of satellite technology. In addition, it is certainly conceivable that a domestic law enforcement agency could in the future launch its own spy satellite, or that one of the spy satellite agencies could be transferred out of the Pentagon and into a civilian branch of government. In either of those cases, Posse Comitatus would lose all relevance—and yet it would still be crucial that the use of spy satellites be subject to checks and balances.

In any case, permitting domestic spying by the military using powerful high-technology spy satellites certainly runs contrary to the spirit of the act and the concerns that prompted its passage: the fact that the might of the military is a dangerous thing in a democracy—a tiger in our midst—and must be carefully bounded and restricted in light of the experience of so many societies throughout history where the

military has become a political force with power that comes not from the ballot box but from the barrel of a gun—or the lens of a camera.

Aside from the Posse Comitatus Act, another apparent restriction on the use of satellites domestically is the U.S. Supreme Court decision *Kyllo v. United States,* in which Justice Antonin Scalia, writing for the majority, found that police could not peer inside a private home using a thermal imaging device without a warrant.[1] That ruling should prevent some hypothetical uses of satellites, such as the scanning of entire neighborhoods for the presence of heat sources.

The need for oversight

Of course, without proper checks and balances there is no guarantee that appropriate limits would be observed. Whenever we contemplate the introduction of tremendously powerful new technologies into our domestic arena, our current generation and the current Congress needs to think like Founding Fathers, and Mothers. It was not clear in 1776 what the threats to freedom and democracy would be as the new nation developed, but the Founders were wise enough to put in place a robust system of checks and balances that has withstood the full range of human folly and perfidy for over 200 years. When it comes to spy satellite technology, we may be living in the equivalent of the year 1789 right now. Put another way, we may be looking at a potential monster is still in its infancy. And if this technology is going to be permitted to be turned inward upon the American people, we need absolute certainty we have the right kind of restraints in place to ensure that, as it grows and evolves in ways we cannot predict, it will not trample on Americans' privacy or other rights.

It is not simply a matter of whether we believe rogue agencies will flout the law (though in the absence of oversight that would certainly be a possibility over time). Often, it is not clear what the law says, and the issue is whether that will be decided in secret or hashed out in public. For example, take the Supreme Court's *Kyllo* ruling against thermal imaging inside a home. When satellite use includes non-visible spectrum technologies, questions must inevitably arise about the interpretation and limits of that ruling and how it applies to specific uses. For example, scientists use satellite images outside of the visible spectrum to study the earth and environment; that would not seem to be a violation. But it is not clear where the boundary between that application and the one struck down in *Kyllo* would lie.

The question of oversight is partly the question of who gets to decide such questions and make such interpretations. If satellite surveillance is permitted to take place completely within the shadows, then those interpretive decisions will be made unilaterally by the military itself, and will almost certainly be made in a manner that is as generous as possible to the military.

We believe that the first step in imposing the needed oversight over this program is for a moratorium to be placed on its commencement. The second step is for Congress to ask all the key questions that need to be asked in constructing proper systems of oversight of this program—and for answers to be provided by the National Reconnaissance Agency, the National Geospatial-Intelligence Agency (formerly the National Imagery and Mapping Agency), the Department of Homeland Security, or whatever other agency might be appropriate.

Only with the answers to those key questions can Congress begin the task of writing legislation to impose checks and balances on this program, and only with the passage of such legislation should Congress authorize the start of this program.

Key questions for Congress to ask

Two members—Congressmen Thompson, the chair of this committee, and Rep. Edward J. Markey, a member of this committee—deserve our thanks for raising the right questions and beginning the process of vigorous oversight.

Chairman Thompson has done so not only by calling this hearing, but also through his August 22 letter to Homeland Security Secretary Michael Chertoff (attached for reference). In that letter, Rep. Thompson requests regular briefings on the status of the project, and expresses well-deserved dismay at DHS's decision to launch a program such as this without making use of DHS's own Chief Privacy Officer and Officer for Civil Rights and Civil Liberties, and the president's Privacy and Civil Liberties Oversight Board.

We share Mr. Thompson's concerns; the failure of the government to avail itself of even those weak oversight institutions that now exist does not bode well for how oversight will be conducted over this program by the government in the absence of more serious oversight mechanisms enacted into law. It also serves as a reminder

[1] 533 U.S. 27 (2001)

of how important it is that true checks and balances include truly independent countervailing institutions that cannot simply be written out of the process at will.

A good start to Congressional oversight of this program has also been provided by Rep. Markey in his capacity as Chair of the Subcommittee on Telecommunications and the Internet of the House Energy and Commerce Committee. In his August 16 letter to Mr. Chertoff (attached), sought the answers to a number of vital questions about this program, including:

- **Privacy and Civil Liberties.** What DHS has done to ensure that the program would not violate privacy? In particular, what current policies and procedures govern the domestic use of satellites? Have inadequacies been found in those processes? Have or will new policies be developed before the program is launched? Will any agencies retain any of the output from spy satellites after it has been evaluated? What privacy and security safeguards will be used for the storage of the information? How will the Department handle complaints from individuals subject to surveillance under this program?
- **Legality.** Has DHS conducted an assessment of the legality of the program?
- **Science.** Might the surveillance efforts erode the current scientific mission of the satellite program?
- **Commercial alternatives.** Why has DHS not turned to commercial satellite providers to meet the objectives it is seeking with this program?

All of those questions, like those posed by Rep. Thompson, must be answered before this program can be allowed to go into effect. In addition, I would like to add several more questions that we believe Congress must obtain answers to.

What are the capabilities of today's spy satellites?

The striking thing about our spy satellites is just how much we do not know about them. And it's difficult to draw conclusions about the domestic use of spy satellites when we don't know what they're capable of. In order to craft the right restraints, we need to know just what this monster looks like—and how it is likely to grow.

For example, we do not even know the answer to perhaps the most basic question: what resolution they are capable of. We know Google can go to half a meter, and experts outside the intelligence community say that government satellites exceed that. But, we do not know by how much.

Government satellite images presumably differ in several ways from publicly available online images provided by Google, Microsoft and other Web providers. Online images are merely snapshots taken at most once every few months. Spy satellites may have or gain the capability of producing live, moving images like that from a video camera. Satellites may also be capable of sweeping through much greater geographical areas, and/or of quickly moving their lenses to examine a particular spot within a much greater area at a moment's notice. And they also have capabilities such as radar and infrared imaging. And of course, they can observe ground activities silently and invisibly.

We do not know what they can do in terms of penetrating roofs or other structures, live monitoring, the scanning of large geographical areas, the use of artificial intelligence to guide imaging, or other capabilities that we might not even think of. Without knowing the answers to such questions, we cannot even begin to evaluate their potential threat to our privacy.

There is a lot of discussion and speculation about this topic on the Internet and elsewhere, and many experts have ideas of what the limits of this technology are. Undoubtedly, many will emphasize those limits to you in trying to downplay the privacy threat of this technology.

But Americans have the right not just to be free of secret government spying of their innocent activities, but also to have *confidence* that they are not susceptible to the constant possibility of being invisibly observed. So in our view the government must completely declassify and disclose publicly the full extent of the technological capabilities of any satellites that will be aimed at the American people, and you, Congress, must think like Founding Fathers and institute checks and balances that would be strong enough to protect Americans' privacy even in the face of every gee-whiz satellite capability that Hollywood has ever imagined.

What might spy satellites be capable of in the future?

The Congress also needs to know how satellite technology is likely to develop in coming decades given how rapidly technology is advancing. A reasonable forecast of future progress might be made based on factors such as:

- The continuing exponential growth in computing power and data transfer rates
- The similar rapid growth in the power of digital imaging that we have all seen in the prices and capabilities of consumer digital cameras

- The continuing development of imaging technologies outside the visual spectrum, such as infrared, ultra-wideband, various kinds of radar, etc.
- The possible solution to research problems that are currently being worked upon.
- The amount of resources that are likely to be devoted to the development of our spy satellite technology in coming years

Of course a wise policymaker will institute checks and balances that account not only for reasonably foreseeable developments, but also the possibility for the sudden emergence of new inventions that are today completely unanticipated.

Just what uses does our security establishment envision putting these new satellites to?

Are there really serious advantages that spy satellites can provide to police and Homeland Security agencies that cannot be provided by commercial satellite images of the type available on the Internet or elsewhere? If so, what are those uses? Are the advantages provided by this program substantial enough to counterbalance its threat to our privacy? Or is this just another example of an arm of our security establishment seeking to find new missions and new reasons for being in order to expand its budgets and bureaucratic reach? Or is law enforcement being seduced by the siren call (to which many of us are susceptible) of really cool toys?

If this new program does not actually show substantial promise in making people safer, the matter should end there. There is no need to engage in detailed balancing tests or evaluations of a program's effect on privacy if it is not going to increase security.

Recommendations

We recommend 4 basic steps in response to this situation.

1. Congress should demand, and DHS should impose, a moratorium on the enactment of this program. The moratorium should not be lifted unless Congress receives answers to the key questions outlined above and raised by the Chair and Congressman Markey.
2. The moratorium should not be lifted until Congress authorizes it.
3. Congress should not authorize the enactment of this program before enacting statutory checks and balances to ensure the proper oversight of this potentially enormously powerful surveillance tool. Those measures should include clear rules for when domestic satellite use is permissible combined with judicial oversight of such use.
4. Congress should also strengthen and make truly independent the Chief Privacy Officer of the Department of Homeland Security, which, as Rep. Thompson pointed out in his letter to Secretary Chertoff, appears to have been marginalized by the department in the course of planning this initiative. Congress should also institute similar independent privacy officers for other arms of our national security establishment.

Satellites are but one of many powerful new technologies that are entering our lives at this exciting point in our history. Many of those new technologies promise wonderful new innovations and conveniences-but many, in the absence of due concern and care over their effect on privacy, and in the absence of strong privacy regulations, threaten to become an out-of-control monster that moves us closer than ever to a genuine surveillance society. Congress needs to craft sufficiently strong restraints on this program to ensure that it does not go out of control—to protect Americans against the potential for unacceptable uses of satellite surveillance. And it should treat military spy satellites as a test case for how other technologies should be handled, ideally backed up by an overarching privacy law that will create more clarity and stability of expectations for Americans living in an era of constant change.

Chairman THOMPSON. Thank you very much.

I would now yield 5 minutes to Ms. Graves for summation of her testimony.

STATEMENT OF LISA GRAVES, DEPUTY DIRECTOR, CENTER FOR NATIONAL SECURITY STUDIES

Ms. GRAVES. Thank you, Mr. Chairman. We appreciate very much the invitation to be here. On behalf of the Center for National Security Studies and my partner, Kate Martin, we appreciate very much the opportunity to testify today about these very important matters. I am going to dispense with the statement that

I prepared because I found the testimony this morning so astonishing that I would like to respond to some of the points made. And, in addition, I would like to associate myself with the remarks of my colleague over here. I thought those were very important observations.

The Center for National Security Studies stands by our statement about our grave concerns about the proposed activity, whether it is down the stream or the present proposed activity. Calling the potential unilateral deployment by the executive branch of these extraordinary surveillance powers on the homeland domestically is a dramatic change in the law, and we do think that it is like Big Brother in the Sky.

Now, I understand that there is classified information about the range of this technology, about the scope of it. Let me just be clear about our understanding from the public records. There are assertions that the current resolution of even the imaging satellites is between 0.5 meters and a meter. In essence, for things that are 3 feet across, 3 feet wide. But that is in essence the commercial technology right now. The current estimates in the public domain about the true possibilities of this surveillance are that it is within the inches range of its resolution. That is in the public domain of that speculation. And that actually informs in some way this new desire to implement this new technology, because it is now about people, about being able to monitor people.

So when the Department of Homeland Security says, don't worry, we can't tell if you need a hair cut, I would say, yet. They are still looking at people. The purpose of this, the examples highlighted in this so-called Blue Ribbon Commission about how they would like to use this, are directed at people. So I hope you won't be misled unintentionally about the scope of this authority. But let me just add a few additional things.

I was astonished by the assertions today that no law needs to be changed to accomplish this. Let me just refer you to the record that was before the House Judiciary Committee in 1981 when Congress, not the executive branch, when Congress considered whether to allow the military to be involved in the enforcement of drug laws extraterritorially and at the border. This was the record.

Before Congress at that hearing there were opinion after opinion of legal opinions of the Office of Legal Counsel about their understanding of the scope of Posse Comitatus and whether it would reach or not reach the activity, the specific activity proposed, versus this far-reaching Federal, State, local, tribal, civil, criminal application proposed to be begun on October 1st.

We know more about what William Rehnquist and the Nixon administration thought about the scope of Posse Comitatus than we do about this administration. And we know from other sources, including the torture memos, that this administration has taken a very expansive view of its authority domestically in a wide range of areas. And, in fact, according to the torture memo there is a memo that was written by John Yoo in which he asserts that Posse Comitatus generally prohibits the use of the Armed Forces for law enforcement, absent constitutional or statutory authority to do so.

Now, I would hesitate to associate myself with the comments or legal views of John Yoo. But if John Yoo has a memo out there,

which we can provide you the full site, I think it is in my written testimony, you should have that memo and you should have any subsequent memos. You are entitled to those memos. This body is entitled to those memos. There is ample precedence from the Reagan administration for getting those memos. You should have the general counsel. But you shouldn't just have all assurances. You should have this in writing. And, more than that, the American people should have this in writing. We are entitled to this as a matter of our democracy.

Obviously, there are things we can't know in terms of some of the specifics of the particular operations or sources or methods of those operations. But the fact of the matter is that there are fundamental constitutional principles at stake and statutory principles at stake.

The suggestions that were made by the panel before us that this is useful in disasters, that this is useful in hurricanes, what they didn't tell you was that those are already exceptions that are long recognized in the law. This is not about the use of this technology in hurricanes or disasters. It is about the use of this technology for law enforcement purposes. And I referred in my testimony to the lengthy report of Professor Pyle who goes through why, from a constitutional perspective, it is essential that it not just be about having the military arrest people. The limitations on military surveillance, technology being deployed domestically are not just about that sort of really direct intervention law enforcement; it is much broader than that as part of our constitutional system. And there is good reason for that, and let me just give you two.

One is, as Professor Pyle documents, and the Center of Sam Ervin also documented, the use, the direction of the military toward the collection of information about Americans raises substantial civil liberties concerns. As Senator Ervin said after his lengthy review of this, after a simple request, a request against the capacity of the Defense Department, that began with a simple request to help the Defense Department keep order, the Defense Department obtained files and created files on over 100,000 people, including Members of Congress.

And the second point, let me conclude with this, is to say the second reason why this is so important is because public trust is essential for our national security. Public trust has been eroded by the unilateral actions of this administration time and time again. The public press is enhanced by the direct full intervention of this Committee of Congress in these important matters of our democracy, and public press is enhanced by the public's involvement in those debates. And so we would urge, along with the ACLU, that this program not be permitted to go forward as planned on October 1, and it should not go forward until it is fully investigated in a series of lengthy examinations by this committee and other committees examining the scope and rights of the American people.

[The statement of Ms. Graves follows:]

PREPARED STATEMENT OF LISA GRAVES

Chairman Thompson, Ranking Member King, and distinguished Members of the Committee on Homeland Security of the United States House of Representatives, we thank you for scheduling this full committee hearing so quickly to examine the administration's announced deployment of spy satellites to surveil Americans in the

continental United States. The Center for National Security Studies appreciates the opportunity to testify about our grave concerns regarding this unwise and proposal made unilaterally and containing no checks against abuse. The Center was founded over 30 years ago to help protect civil liberties and human rights against erosion by claims of national security, in the aftermath of the first wave of disclosures to Congress regarding extensive, secret military and civilian government surveillance of Americans in this country.

Kate Martin, the Center's director, and I work closely on surveillance issues, and the types of military surveillance of the civilian population first disclosed in news articles during the August recess pose significant threats to our constitutional system and civil liberties. The administration continues to be tone deaf on matters of civil liberties, with all due respect to my colleagues on the first panel—their comments are an after-thought, a sound bite. As the Chairman mentioned in his letter, this satellite deployment was basically a "fait accompli" by the time it got to the agency privacy designees this spring.

At the outset, I would like to raise some questions and try to help clarify the scope of the surveillance at issue today. I will then discuss core constitutional and legal principles that call into question the extraordinary surveillance activities proposed. I will conclude by describing the need for more oversight and proposing some solutions.

I. Civil Liberties and Privacy Concerns Raised by the Civil Applications Committee's Report.

In May 2005, the Director of National Intelligence commissioned a Civil Applications Committee Blue Ribbon Study, which was completed in September 2005. Several of the Committee's recommendations, including the creation of the Domestic Applications Office in the ODNI have apparently been adopted. The domestic deployment of military satellites is also apparently the result of these recommendations. However, it is not known what other actions have been taken in response to these recommendations. It is important to understand the breadth, scope and danger of the recommendations.

While the deployment of military satellites to monitor U.S. civilians has been the focal point of the press on this breaking story, the actual scope of Intelligence Community (IC) powers that could be deployed is broader than that, including "national satellite sensors; technical collection capabilities (archival, current & future) of the DoD; airborne sensors; NSA worldwide assets; military and other "MASINT" sensors; and sophisticated exploitation/analytic capabilities." Civil Applications Committee's Report (CACR), at p. 8. MASINT, which is the acronym for "Measurement And Signatures Intelligence," describes technologies that "exploit fundamental physical properties of objects of interest" and techniques that include advanced radar, electro-optical sensors, infrared (including spectral) sensors, geophysical measures such as acoustics, and materials sensing, processing, and exploitation systems. MASINT is distinct from other techniques averred to in the report such as "imaging" (photography, both still photography and real-time video-type recording) and signals intelligence (SIGINT), which includes electronic surveillance, commonly called eavesdropping or wiretapping. While this list might sound like Big Brother incarnate, it might give some Americans comfort to know that these are the capabilities that have been created to protect us against *foreign enemies.* It should be obvious, however, that deploying these extraordinary powers against people in the U.S. would fundamentally alter the relationship between the government and the governed. Calling this "Big brother in the sky" is modest given the array of array that might be available multi-headed, medusa-like powers to monitor Americans encompassed by this array of arrays.

The Committee concluded that there is "an urgent need for action because opportunities to better protect the nation are being missed," a finding contradicted later in the same report: "During the course of the study no one said they were failing in their mission due to lack of access to IC capabilities. There was no *'Burning Bridge' identified* by the participating agencies and stakeholders." *Compare* CACR p.4 *with id.* p. 10 (emphasis added). To be plain, the question is whether this blurring of the lines between civilian and military activities is wise and prudent. The report has a view on that as well: while law enforcement has "traditionally focused on arrest and prosecution and the IC on disruption and prevention. These mission foci are blurring" and this blurring should be considered a "'feature' as opposed to a 'flaw.'" *Id.* p. 12.

The report also casts a critical eye toward civil liberties, asserting that the protection of "individual civil liberties" and protection of sources and methods "are the predominant concerns" in the "risk-averse" environment. *Id.* p. 10. It then sets up a decision-making process about deploying IC technology domestically in which the

protection of civil liberties in just one of ten factors. The report then proposes "fast-tracking" consideration and decisions on such legal concerns. *Id.* p. 18. It is striking that Congress is not mentioned anywhere in the process for flagging legal concerns and deliberating about how to resolve "issues on the boundary or not covered by policy."

While the report contends that a "strict set of legal and protection of civil liberties guidelines would be followed," such secret guidelines could be changed at the direction of the executive or the whim of a zealous attorney at OLC, such as a John Yoo. That is precious little protection. In fact, the report relies upon the kind of now-discredited parsing of words engaged in by the Office of Legal Counsel in the first term of this administration. For example, one of the reasons why the report supports encouraging the U.S. Marshals Service to use IC technology is that because their job is to execute warrants by apprehending fugitives there is "a very low probability the IC's involvement would be subject to a judicial proceeding," a kind of don't ask-don't tell/win-win situation according to the operating "ethos" of the report. *See id.* at p. 24.

Even when reading legal precedents, the report puts its thumb on the scale of increasing surveillance of the American people, by providing a roadmap for activities that proponents would likely argue are permissible, if the government took more of a "risk management" rather than "risk-averse" approach to civil liberties issues:

- Warrantless "aerial searches of private property";
- Warrantless "use of highly sophisticated mapping cameras to photograph the interior of a building"; and
- Warrantless satellite surveillance of this same kind.

The report does acknowledge that the Supreme Court recently held that thermal imaging of a residence without a warrant was unlawful. *See Kyllo v. United States,* 533 U.S. 27 (2001). However, the report notes that there is "no clear authoritative guidance issued on the impact" of this decision on the use of domestic MASINT.' CACR at p. 30. Despite this decision that post-dates other decisions relating to aerial searches, the report goes on to justify expansion by claiming that the Congress "did not substantiate the allegations of the illegal use" of photographic sensors to image domestic areas, hardly a ringing endorsement of doing so now. *See id.* The report is also critical of the "cultural aversion toward collection of domestic imagery based on concerns involving the potential of congressional oversight sanctions centering around 4th Amendment concerns." *Id.* at 32.

The report credits the tragic events of 9/11 and the "global war on terror" with creating a better environment for domestic expansion of these authorities. And, the report suggests that simply having a Privacy and Civil Liberties Oversight Board is sufficient to ensure that Americans' privacy is being protected. The actual report of the PCLOB earlier this year demonstrated far from model oversight—the report was basically a rubber-stamp of White House initiatives. The White House's editing of the report led in part to the resignation of the only Democratic appointee of the five-member board. (Subjecting the board members to Senate confirmation, as the 9-11 implementation bill did, is unlikely to change the make-up of the board until the end of the next presidential term.) This utterly inadequate Executive Branch "check" is no substitute for robust congressional oversight and judicial review to protect the Fourth and First Amendment rights of Americans. To the contrary, as the Committee recognizes, the PCLOB can be enlisted to help ratify, the domestic use of IC capabilities. *See id.* pp. 31—32 & n.11.

It is also quite worrisome that the report recommends revising Executive Order 12333 that governs U.S. intelligence activities "to permit as *unfettered* an operational environment for the collection , exploitation, and dissemination as is reasonably possible" of domestic intelligence activities. *See id.* at p. 31 (emphasis added). We are also concerned that the report proposes a way around U.S. person rules by adding unique ID numbers to information derived through foreign intelligence electronic surveillance to make it easier to know more about subjects without their names attached. *Id.* p. 41. Lest any Member believe this issue is distinct from the disastrous changes in the law rammed through Congress before August vacation, it is clear that surveillance of Americans' communications is included in the report's recommendations for expanding domestic applications of satellite and other IC technologies. Yet it seems highly likely that there has been no forthright or comprehensive briefing of Congress on how this issues impact each other; certainly there has been no public debate to evaluate the potentially severe impact on the privacy rights of Americans.

While asserting the need to abide by "the rule of law," the report concludes that many rights "have now been abridged at least in practice if not in law." *Id.* at p.38. The defense contractors call this the "new normal" and note that there is a whole body of "Presidential memoranda and executive branch decisions that direct certain

actions and events that are germane," documents that it is highly likely the congressional branch, charged with writing the law—in contrast to the executive branch that is charged with *executing* the law—has likely never even seen. *See id.* p. 39. The report concludes by positing a very troubling, Cheney-esque point of view, claiming that the Church and Pike Committee investigations "created a hyper-conservative view of what can be done." *See id.* at p. 42. It recommends that overseers should not look for "black and white" distinctions but instead "experimentation" should be the rule, while remaining thoughtful about the "legitimate" rights of Americans, whatever those may be. *Id.* at p. 43. That's a very sunny view, but the reality is that there is no country in the world where domestic intelligence collected in secret has not been misused by the government in power, usually against its political opponents, including the United States. The long-standing rules and understandings that this report and the DNI's proposed office seeks to undo would turn back the clock to the dark days when military surveillance of the American people was the "new normal," but would do so with exponentially better, more intrusive technology than J. Edgar Hoover ever dreamed of.

II. Constitutional and other Legal Considerations Support Being "Risk Averse" to Protect Rights

The proposed expanded surveillance of Americans call to mind the 1998 movie, "Enemy of the State," where Will Smith's character is tracked by NSA and other government agents via satellite surveillance, through tiny GPS transmitters, via bank records, and through via electronic monitoring of domestic conversations and call data without warrants. It's just a fictional movie, of course, but it is one of the more recent visual depictions of some of the IC capabilities at issue here. In response to questions raised at the time of the film's release about whether the National Reconnaissance Office (NRO), which maintains the spy satellite network, could "read the time off your watch" NRO spokesman Art Haubold pointed out that, "legally, his organization is not allowed to turn its surveillance systems on the United States." If the Domestic Applications Office is allowed to pursue the proposals made by the Committee, that assurance will no longer be true.

The principle at stake, as stated by the NRO, was that satellite technologies were not allowed to be turned on the U.S. Now the administration spokespeople are left with saying don't worry, we won't be able to "tell if you need a haircut," not the same kind of assurance at all. To the contrary, it implies the opposite of the uniform assurances made before this administration—now they might be watching but can watch you, they just do not yet have the technology to see everything.

Less than a decade ago, commercial satellites could conduct what is known as panchromatic electro-optical surveillance with a resolution of one to .5 meters. According to public accounts, the actual resolution of military satellite technology four decades ago, in 1967, was one meter, which means the ability to distinguish objects almost three feet across. Recall the black and white photos later released regarding the Cuban missile crisis. There is no doubt that military technology has made dramatic leaps forward since then and while the true resolution is secret, public estimates are that the military can create visual images of much better quality than the commercial applications, in the range of 10—15 centimeters, or objects up to four inches across. That is why the Department of Homeland Security can claim there is no worry about seeing your haircut from space. To which I would add one word: yet. It's imminent.

What this means is the government will have the capacity to photograph from satellites or platforms on high not just borders or buildings or missiles or cars but ordinary people. And there are the other sensors, infra-red, thermal, audio/greatly amplified hearing devices and the patented technological capacity to sort through conversations in a crowded room. There are GPS transmitters, which Americans rely on for driving directions or in their cell phones and which the government could easily use to track individuals.

There is only one given in this debate: that technology will continue to improve. As Bill Gates has remarked, technology will improve often in "great leaps over relatively short periods." The resolution of military satellite images and quality of other IC sensors are only going to get better and better, especially with the amount of money available for R & D.

The rules for turning military satellites inward on the American people should not depend on how great the photo resolution and GPS tracking technology is at the moment. The rule should depend on principles, what the report disdains as "black and white distinctions". These conservative principles, which the report criticizes as "risk averse," are the principles that have preserved our civilian democracy from military control. One principle that has been the glue that has preserved the compact between the citizens and the state is that the branch that uses power cannot

be the branch that creates the rules for such use or enforces them. Turning military satellites and sensors inward on Americans should not be the unilateral decision of the DNI, or other intelligence officials, or of the proponents of the untrammeled executive power.

Much has been said over the years about whether the *Posse Comitatus* Act applies or does not apply to a given activity. The posse comitatus statute itself has a bit of a checkered past, as it was passed a decade after the end of the Civil War in response to complaints by Southerners against federal troops still policing reconstruction efforts and in particular the rights of African Americans to vote. The statute makes it a crime to "willfully use" the military "to execute the laws," except in cases "expressly authorized by the Constitution or Act of Congress." Congress has created several exceptions over the years, such as emergency situations as with an insurrection or health quarantine as well as narrowly drawn exceptions for circumstances involving nuclear weapons or assassination. Other exceptions have been less well drawn, such as enforcement of federal drug laws, although that has been confined to the borders.

It is plain that under the terms of the statute Congress can make exceptions, although it is not plain to us that every exception would pass constitutional muster. We believe that a new statutory exception for the deployment of spy satellites to spy on the American people without any judicial check would not only swallow the rule but would be unconstitutional. It does not appear, however, that the Executive Branch is asking for your permission or a statutory exception. It is instead a "fait accompli."

I suspect their arguments are two-fold. First, that so long as they are not permitting the military to arrest a person they are not executing the law. (But the military has already taken a citizen and others into custody inside the United States without charges as "enemy combatants.") This would be a rather narrow interpretation of what it means to execute the law, especially for an administration that claims for itself maximum deference in its executive functions. The more sophisticated argument they might make on this point is that such IC capabilities would be passive, not directed at executing the law. (Such an argument might reach back to some lower court decisions stemming from the particular facts of the massacre at Wounded Knee where a military officer was reported to have directed law enforcement agents.) The statute should not be read so narrowly.

On these points I would refer the Committee to the eloquent legal analysis of Dr. Christopher Pyle. As he demonstrates in his memorandum, "the primary objective of the Posse Comitatus Act has not been merely to forbid energetic, aggressive, intrusive assistance, but to forbid routine assistance as well." He presciently observed that "the political pressures for information may cause the armed forces to redefine the 'normal course of military operations' so as to re-involve the military in the surveillance of civilian political activity." This forecast unfortunately came true in the case of the recently abandoned "TALON database," which the Defense Department used to collect information on innocent Quakers and members of other peaceful religious groups that have spoken out against the war in Iraq. As Dr. Pyle noted:

> During the late 1960s, it was 'normal' for the U.S. Army Intelligence Command to dispatch plainclothes agents to observe nearly every demonstration in the United States involving 20 or more persons, to infiltrate domestic political groups, to maintain huge data banks on dissidents, and to share information about wholly lawful political activity with civilian law enforcement agencies, including some with notorious records for violating First Amendment rights. Overseas, it was normal to open civilian mail, wiretap American civilians, and violate confidential communications between American civilian attorneys and their clients.

(I would ask to make his full statement part of the record, as an attachment to my testimony.) While some of these specific activities have since been prohibited, the proposal to deploy satellite and other technologies involves the same dangers.

I would submit that there are also larger principles at stake than that particular statute, based on the Constitution's structure of limited powers. For example, the Constitution means to make the imposition of martial law the rare exception by barring standing armies and forbidding the suspension of the writ of habeas corpus except in rebellion or invasion (and grants that power to Congress, not the president, in Article I). As Senator Sam Ervin noted: the "Constitution clearly contemplates that no part of the armed forces may be used in the United States for any purpose other than the following: (1) to repel a foreign foe; (2) to quell a domestic insurrection against the government; or (3) to suppress domestic violence which the states are unable to suppress without federal aid." Senator Ervin conducted a lengthy and thorough investigation of the use of the armed services to spy on Americans, and I would ask that a historical article and letter from him regarding military surveil-

lance be included in the record as an attachment to my testimony. In his article, Senator Ervin noted that Congress had documented the abuses that occurred the last time the military was permitted to engage in domestic surveillance. Among the many examples cited, I would note in particular the following example from an Army Intelligence unit in Chicago in the late 1960s and early 1970s:

> He described how this unit targeted for surveillance 800 persons in Illinois, collected by overt and covert means information about them, stored such information in dossiers, and transmitted some of it to intelligence installations elsewhere. Among those persons spied upon were Senator Adlai E. Stevenson, Representative Abner Mikva, and United States Circuit Judge and former Illinois Governor Otto Kerner, as well as state and local officers, clergymen, journalists, lawyers, and contributors to political and social causes.

Senator Ervin also stated that through notes, recordings, and photography, the dossiers recorded the "attitudes, aspirations, thoughts, beliefs, private communications, public utterances" and financial information. The stated justifications for some of this surveillance was predict civil disturbances. In all, "[m]ore than 100,000 civilians were subjects of surveillance by military intelligence. . . . Their reports were fed into scores of computers and data banks across the country. No meeting or demonstration was too trivial to note; no detail of one's personal life too irrelevant to record."

While the military acknowledged its failings and adopted new rules to prevent such surveillance by individual personnel, Senator Ervin's warnings from the past about the need for clear rules are again relevant given the technology now available. History was already repeating itself in the TALON database and, while we welcome the announcement of its demise, the potential for mission creep by the military, with its enormous resources, is still quite dangerous. It is the nature of the military to take actions on a massive scale, with individual collectors simply following orders, collecting against requirements from on high. Indeed, one of the military's strengths is its massive force and capabilities. But this sledgehammer-like strength should not be deployed, even or perhaps especially via surveillance, against the American people as a whole or against selected groups or individuals here in the U.S., without judicial oversight, in response to requests by civilian law enforcement agencies at all levels of government seeking military involvement and assistance in the enforcement of all kinds of criminal and civil laws.

III. The Need for More Complete Disclosure and More Investigation into this Matter

Clearly, more investigation is warranted.

Two years ago, the report produced by the non-governmental Civil Applications Committee recommended establishing a "Domestic Applications Committee" in ODNI to fund and accommodate access to current Intelligence Community "collection and processing capabilities" as well as to increase funding for R & D, acquisition and "Tasking, Collection, Processing, Exploitation, and Dissemination" (TCPED). In essence, military contractors studied the potential to use military resources domestically and agreed that these military resources should be used for domestic intelligence and domestic law enforcement with increased funding. I suppose one should not be surprised by this result.

What should surprise, or at least offend, Congress is that in the two years the DNI has had this report and on the eve of its implementation it took the press to discover this revolutionary plan. It appears that this Committee was not informed that the DNI had begun to implement this taxpayer-funded study. (Although the administration told reporters that it had briefed "key" members of this Committee, as well as Appropriations and Intelligence, press also reported that neither the Chairman nor the Ranking Member of this Committee were aware of it before it was reported in the news.) There is no public record to support the conclusion that the DNI consulted with this Committee before striking a deal in May with the Department of Homeland Security and its secretary Michael Chertoff, to provide access to information about people in the U.S. collected via satellites flying over the U.S. There is no record to indicate that DHS sought advice from this Committee before entering into the reported Memorandum of Understanding (MOU) or that the Members of this Committee have seen this MOU and have a clear understanding of its scope, its intended effect and its likely unintended consequences.

How many times have Director McConnell or Secretary Chertoff or their staff been up to Congress in the last four months or two years, making assurances and claims, without mentioning this massive expansion of domestic surveillance? How much longer can you continue to rely on assurances when time and time again Executive Branch officials have omitted key facts or provided you with carefully se-

lected information in response to only the precise questions asked. This game of hide and seek is unbefitting a democracy.

There is also no record to support the conclusion that Congress has any concrete estimate of how much this might cost or what the opportunity costs are of directing military satellites toward the American people, let alone a full and accurate assessment of civil liberties and privacy concerns, other than what has been presented by military contractors and *political appointees* of the Executive Branch. It is the nature of the Executive Branch to maximize executive power and discretion, which is why robust checks are essential. We have witnessed this inherent tendency in overdrive over the past six years due to the extreme views of Vice President Cheney about inherent, unlimited power of the president, views that have been adopted and implemented throughout the Executive Branch. Some of the related OLC opinions were written by the discredited John Yoo, whose views the subsequent head of OLC, Jack Goldsmith called "tendentious," "overly broad" and "legally flawed." *See* Jeffrey Rosen, "Conscience of a Conservative," The New York Times Magazine (Sept. 9, 2007).

I mention this background because in my observation Congress needs to establish its own Office of Legal Counsel for purposes of assessing the scope of authority under the Constitution and statutes, because the Justice Department's OLC has an institutional bias in favor of the branch within which it resides. In some ways the Congressional Research Service fulfills this role, but it has not been given the responsibilities or credit it deserves to be a counterweight to OLC's defense of presidential power and diminution of congressional controls, as evidenced in this recent period. Despite the great flaws in some of these OLC opinions, they are important markers for what the Executive Branch thinks it has the power to do. The tradition prior to this administration was to make almost all of the opinions that relate to the interpretation of public law public even if redactions were needed. And, yet, as we sit here today debating whether public statutes, such as the Posse Comitatus Act preclude the deployment of military satellites to target or track civilians in the U.S., this Committee does not have the relevant memos from the administration to assess what the administration thinks it has the power to do with or without the consent of Congress. Specifically, the administration apparently reinterpreted the Posse Comitatus Act, along with several other statutes in October 2001. As stated in footnote 16 of the OLC August 2002 "torture memos":

> We recently opined that the Posse Comitatus Act, 18 U.S.C. s. 1385 (1994), which generally prohibits the use of the Armed Forces for law enforcement purposes absent constitutional or statutory authority to do so, does not forbid the use of military force for the military purpose of preventing and deterring terrorism within the United States. See Memorandum for Alberto R. Gonzales, Counsel to the President and William J. Haynes II, General Counsel, Department of Defense, from John C. Yoo, Deputy Assistant Attorney General and Robert J. Delahunty, Special Counsel, Office of Legal Counsel, Re: Authority for the Use of Military Force to Combat Terrorist Activities within the United States at 15–20 (Oct. 23, 2001).

What does this memo say about using military force or tools, such as satellites or what is known as "remote sensing" data or devices on these shores? Was the administration's rhetorical argument that the battlefield is everywhere translated into legal opinions that would permit the military to electronically surveil Americans without warrants and seize and "arrest" civilians on the general ground of terrorism prevention, hold them in military brigs and detain them without trial. These matters are all inter-related and Congress has not yet gotten to the bottom of what has been wrought, although it has now begun to do so.

We respectfully request that this Committee begin a comprehensive review, jointly with the Judiciary and Intelligence Committees, of how domestic surveillance powers are being used. As former CIA advisor Suzanne Spaulding has noted:

> The inquiry should start with an open question about the design or efficacy of oversight and accountability mechanisms. The inquiry should ask first whether some powers should ever be granted to the government; whether the law or institutional safeguards can ever be adequate to protect constitutional government and individual liberties against the kind of power a government will amass when it harnesses all potential technological surveillance capabilities.

The proposal to deploy military surveillance powers domestically only adds to the urgency of the need for a systematic review of domestic and foreign surveillance powers, as currently deployed and as proposed by the administration. In the absence of such an examination and full disclosure to Congress, no new surveillance powers should be approved and ratified.

We also believe this Committee has a duty to insist on seeing the Yoo memo and any subsequent memos that attempt to justify domestic use of military satellites for

intelligence gathering in the U.S. related to terrorism or for other purposes. Has this memo and any later clarifying memos by Jack Goldsmith or by officials at ODNI or elsewhere on the application of the posse comitatus or other restraints been provided to this Committee? If it has been provided, we would ask that it be made public to the extent possible. We suspect, given this administration's dubious claims of the need to classify or keep secret even interpretations of public laws, that the Committee has not received the Yoo memo or any others we have identified. We do not think, however, that the Congress should permit the Domestic Applications Committee to implement recommendations until these and other key documents are transmitted. Even then the Congress should examine carefully this dramatic expansion of the use of military resources in the US homeland against people in the US and withhold approval if the only case that is made is that it might have some utility.

The administration seems to be operating under a variant of the bureaucratic dictum, it is easier to ask for forgiveness than permission: often they seek neither permission nor forgiveness. They simply act in secret, violating statutes such as the Foreign Intelligence Surveillance Act, until their unlawful conduct is leaked and then they investigate the whistleblowers. They then seek to legalize what they have done and institutionalize it with Congress' acquiescence. We are concerned that the administration plans to implement the domestic satellite spy program with or without the formal blessing of Congress, although it is possible that this expense is obscured in some ambiguous line in the so-called black budget.

Congress, however, has some tools in its constitutional toolbox and should enact a funding rider to prevent any more American taxes from being spent on the Domestic Applications Committee or the implementation of the satellite-spying proposal. This House should use the power of the purse and let the president threaten to veto the federal budget over this, or the House should at least take steps to force the president's allies in the Senate, from whatever side of the aisle they hail, take a vote on the record in favor of spy satellite surveillance of the American people. Congress should not just let this proposed activity be implemented without those who support spying on Americans paying any price. Without such credible action by this Congress, the next 14—17 months at least will be filled with more liberty eroding policies being implemented without consequence. Once implemented, such programs and expenditures can be very difficult to undo.

IV. Conclusion

Intelligence officers have sometimes described the IC's capabilities as a "weapon." We believe these incredible powers should not be trained on the American people. The Center for National Security Studies stands by its initial fears about the proposed surveillance—it is big brother in the sky. The military surveillance activity that could be deployed unilaterally by this administration as proposed "experimentation" is nothing short of revolutionary. We call on this Committee to continue to investigate this proposal and to withhold funding unless and until full information is received and it is clear that such capability is necessary and consistent with the Constitution and the protection of civil liberties. Thank you for considering our views.

Chairman THOMPSON. Thank you very much. I thank the witnesses for their testimony. I now recognize myself for 5 minutes of questioning, and I yield that time to the gentlelady from California.

Ms. HARMAN. Mr. Chairman, I thank you for that. I apologize to you and our members and the witnesses for having to leave in 5 minutes, but I have found this 3 hours extremely useful.

You were all here and heard my rant to the first panel. I stand by that, but I would now add a few things and ask you a question.

I like Mr. Steinhardt's idea about a moratorium. I think on a bipartisan basis this committee is very concerned, and Mr. Brown's comments could have been any of our comments in terms of the overreach of executive power into our homes in a way that we have not permitted. So, I think a moratorium is a good idea. The Committee will be sending a letter to Mr. Allen later today requesting all the materials that you have suggested we get. And, as far as I am concerned, I would like us to do whatever we can to delay this program proceeding until we have fully reviewed those materials.

There is no intent to delay it unnecessarily, but we are on the front end of this, an expansion of the power to look into the activities of Americans in America, and we have to insist that it fully comply with our Constitution and our laws. And if the laws are not adequate, we have to add laws. So that is my first comment.

My second comment is I agree with you on Posse Comitatus; we didn't get a full answer today. But I think the full answer is not as easily explained as it was by the couple of witnesses who tried to address it. They said they are not expert on it. And I know the history as you do, and I actually worked in the Senate when Sam Ervin was in the Senate. I am a fossil. So I remember that, and I remember how careful he was to protect Americans, and we had better take care again. So that is my second point.

My third point is that we have been rolled on the Terrorist Surveillance Program in Congress. That thing was full blown before I as a member of the Gang of Eight was briefed on its operations. I was not briefed on the legal underpinnings until after the President disclosed the existence of the program. And I could consult a few people and come back to the Gang of Eight format and insist that we be briefed. But even now, facts are coming out. And the bottom line is, this is administration feels free to disregard the law Congress passes in exercising the President's Commander in Chief authorities. And there has been a very clear Supreme Court case on that, and it is called the Steel Seizure case that at least persuades me that the way they are proceeding is improper.

So since we have been rolled, I intend not to get rolled again. And this is what I want your comment on. I think, unless we fully understand what is proposed—and I am not even certain Mr. Allen in his colleagues fully understand what is being proposed—and know—and I know Mr. Green feels the same way—that we have some sort of careful Article 3 court review mechanism in place, we should just not go here. Just not do it.

Like anyone else, I think we want to find out the plans and activities of those who would intend to harm us, including Americans. But if we give up our Constitution and our system of laws to find out those plans and activities, I think they win.

So that is basically my comment on the philosophical question of how to proceed. And I have just a minute of time left, and I do want to respect my time limit here, so please answer me briefly, if you can.

Ms. GRAVES. Let me just say, I appreciate very much your leadership, Congresswoman Harman. You have been a tremendous leader on these issues from the national security standpoint and taking due care for our civil liberties.

Our concern echoes yours in that this unilateral activity basically, it is presented as a fait accompli. It is presented as they are starting October 1, whether you do anything or not, unless you do something to try to stop them, basically. And we think that is entirely the wrong way to proceed in this democracy. We think it is the wrong way to proceed from a civil liberties standpoint. And we don't have confidence given the track record of this department, even with their good intentions and, with this administration, that they will actually protect civil liberties. We know they are reviewing to rewrite Executive Order 12333, and we know that they are

reviewing and have reinterpreted countless laws that we don't even know about. So we can't trust them and take their word for it.

Ms. HARMAN. Thank you.

Mr. STEINHARDT. If I could add two points to that. I entirely agree with Mrs. Harman. There needs to be a time out here. There needs to be a break in order for the Congress to step in and make clear what the rules are.

I would just say parenthetically, I didn't regard your earlier remarks as a rant. I thought they were forceful and insightful.

Finally, I commend to the Committee an article that appeared in this morning's Washington Post on page D–3, if my printout is correct, that discusses how the Department of Homeland Security has dropped now the use of a large data mining program some of us have been concerned about known as ADVISE. And part of the reason they dropped it is not only really their inability to implement it, but also because they learned that in fact they had violated the law by using data involving real live Americans.

Chairman THOMPSON. Excuse me, Mr. Steinhardt. We are going to have to go and do a vote. And in deference to the Committee members who stayed, I am going to ask them to do 2 minutes starting with Mr. Green.

We heard you. We have already dispatched a letter to the Department talking about the Advise program and raising a lot of the concerns in the article.

Mr. STEINHARDT. Of course, Mr. Chairman.

Mr. GREEN. Thank you, Mr. Chairman. And I sincerely thank you for your vision and your foresight and your willingness to host this hearing. It is exceedingly important. My comment will be brief.

This is a technology that is not only omnipresent but also invisible. We will not know the extent to which it can be penetrate our privacy without sufficient oversight. The best of intentions are the means by which the road to a place that none of us want to go has been paved. I just think, Mr. Chairman, that we are at the genesis but there are revelations yet to come, and we are to shape the revelations. Thank you.

Chairman THOMPSON. Thank you.

Mr. Perlmutter.

Mr. PERLMUTTER. Thank you, Mr. Chairman. Just a lot of thoughts based on your testimony, and just kind of a thought that I had. I had signed on to the impeachment bill of Alberto Gonzalez, and then I saw the Bourne Ultimatum the next night. And it made me nervous actually as to the capability and the capacity of this government to just look in on all of us. And that was confirmed for me, and it wasn't a government company, or it was a major corporation. I visited their plant. And the resolution of the camera that they had in the ceiling, just to be able to see just a tiny pore on my hand was unbelievable.

So the fears that you all have expressed as to the capacity of the government, the potential for abuse are things that we have just got to deal with.

You know, there is a piece of me that, though, thinks that there may be a proper component for law enforcement, I don't know all about the Posse Comitatus, but the proper role, so long as we have procedures in place that respect the rights of each and every one

of us. And we haven't really had a chance to see if those procedures are in place and that the oversight is in place. And I am just glad that you two are looking at this. And hopefully that prior panel, you know, Congresswoman Harman has been a major supporter of the Intelligence Community, but she has also been a supporter of each and every one of us having our rights protected. And hopefully that panel got it, that this is something that is of major concern to all of us. And I am with you on the moratorium. Thank you.

Chairman THOMPSON. Thank you very much. Now, chairman of the Oversight Committee for the full committee, Mr. Carney.

Mr. CARNEY. Thank you, Mr. Chairman. I, too, want to associate myself with the much of what is being said here today.

Now, I do have a quick question. Do you see from your perspective a use in satellites as a tool in law enforcement and protecting society?

Mr. STEINHARDT. You know, we are not Lignites; we are not saying this technology should be smashed and never used. What we are suggesting is there may be appropriate uses, but the Congress needs to establish what the procedures are before they can be used. And they need to be narrowly tailored, and we need protective rights. Let us do that first before we begin to understand the technology.

Mr. CARNEY. Understood.

Ms. GRAVES. And let me just say that that is the way the Posse Comitatus Act has proceeded in the past. It is written to provide for whether there is a constitutional exception, which I wouldn't say is just unlimited Commander in Chief power. But a constitutional exception, or statutory exceptions, that those can be created. Of course, an exceedingly broad statutory exception could be subject to the constitutional challenge. So we would obviously urge that Congress really have as much time as the administration had. They talked this morning about how extensive and lengthy and thorough their review was either in the last 3 months or in the preceding year and a half, by primarily political appointees. Whether it is the privacy officers or others, you should have at least that amount of time to unravel this and take a look at these issues. And we would support the moratorium on that basis as well.

Mr. CARNEY. Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you very much. I think my comments have been echoed in the questioning and comments of the Committee.

I want to thank the panel for their valuable testimony and for the members for their questions.

Some of you may have noticed the empty seats there at the witness table. We had invited two DNI witnesses to testify at this hearing, and they declined the offer as they didn't want to be on the same panel as our friends from the ACLU and Center for National Security Studies. No offense to either one of you, of course.

As I noted previously, this is a very serious issue, and one hearing alone will not suffice. I believe additional hearings and briefings are merited. DHS has promised certain get-backs to the committee. And, when they are provided, I hope to hold additional hearings. I have asked Ms. Harman and Mr. Carney to take the

leadership on many of these issues, and I hope and expect that DNI will participate in those hearings.

In addition, I think that the lack of answers and legality of the proposed programs require testimony from the general counsel of both DHS and DNI going forward.

Hearing no further business, the committee hearing stands adjourned.

[Whereupon, at 2:10 p.m., the committee was adjourned.]

VerDate Nov 24 2008 09:52 Aug 21, 2009 Jkt 000000 PO 00000 Frm 00066 Fmt 6633 Sfmt 6011 H:\DOCS\110-HRGS\110-68\48963.TXT HSEC PsN: DIANE