USING OPEN-SOURCE INFORMATION EFFECTIVELY

HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

JUNE 21, 2005

Serial No. 109–22

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

24–962 PDF WASHINGTON : 2007

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

CHRISTOPHER COX, California, *Chairman*

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

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

ROB SIMMONS, Connecticut, *Chairman*

CURT WELDON, Pennsylvania
PETER T. KING, New York
MARK E. SOUDER, Indiana
DANIEL E. LUNGREN, California
JIM GIBBONS, Nevada
STEVAN PEARCE, New Mexico
BOBBY JINDAL, Louisiana
DAVE G. REICHERT, Washington
CHARLIE DENT, Pennsylvania
CHRISTOPHER COX, California *(Ex Officio)*
ZOE LOFGREN, California
LORETTA SANCHEZ, California
JANE HARMAN, California
NITA M. LOWEY, New York
SHEILA JACKSON-LEE, Texas
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

CONTENTS

USING OPEN-SOURCE INFORMATION EFFECTIVELY

Tuesday, June 21, 2005

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

The subcommittee met, pursuant to call, at 10:10 a.m., in Room 210, Cannon House Office Building, Hon. Rob Simmons [chairman of the subcommittee] presiding.

Present: Representatives Simmons, Cox, Weldon, Lungren, Pearce, Dent, Thompson, Lofgren, Sanchez, Harman, Jackson Lee, Etheridge, Langevin, and Meek.

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

Today, the subcommittee meets to examine how open-source information can most effectively be used to help strengthen the Department of Homeland Security's information analysis and intelligence production responsibilities.

Open-source information, by its very nature, is unclassified, publicly available information that any member of the public can lawfully obtain. Open-source information may be used in an unclassified context without compromising national security or intelligence sources and methods, thereby lending itself to the Department of Homeland Security's mission to share information with state, local and tribal governments and private sector personnel, many of whom do not hold security clearances.

Open-source intelligence, or OSINT, is produced from open-source information, can help to inform the Department of Homeland Security's partners and customers. For example, DHS on a daily basis produces the open-source infrastructure report to critical infrastructure owners and operators. And while this report is limited in scope and sources, it is an effective way to help ensure that critical partners on the same page with regard to threat and vulnerability information.

I believe that the Department of Homeland Security and the U.S. government need to do more to create open-source products and integrate open-source information into the DHS analytical product. Both the 9/11 Commission and the WMD Commission recognized this in their reports, and each recommended that more be done with open sources.

Open-source information can be the critical foundation for the all-source intelligence product, a key to ensuring that our intelligence efforts are well-targeted and our intelligence analysis is well-informed across the board.

In a rapidly changing post-9/11 world, intelligence collection and analysis must be flexible enough to respond quickly to meet the demands of intelligence users. Open-source material is collected and reported continuously around the world. It is current and readily available. A comprehensive open-source capability provides the tools to find that information quickly and cheaply in a format that is unclassified and easily shared. This can be an important tool in defending the homeland.

We are pleased to have with us today three witnesses.

The first is Dr. John Gannon, who currently serves as vice president for Global Analysis at BAE Systems, Information Technology. Dr. Gannon joined BAE Systems after serving as Staff Director of the House Homeland Security Committee.

In 2002–2003, he was a team leader in the White House Transitional Planning Office for the Department of Homeland Security and previously served in the senior most analytical positions in the intelligence community, including chairman of the National Intelligence Council and assistant director of Central Intelligence for Analysis and Production.

Last year, President Bush awarded him the national security medal, the country's highest intelligence award.

Welcome, Dr. Gannon.

Our second witness is Mr. Eliot Jardines, president of Open Source Publishing, Incorporated and former publisher of Open Source Quarterly, a professional journal for open-source intelligence practitioners. Internationally recognized as an authority on open-source intelligence, he has twice received the Golden Candle award for open-source excellence at open source symposiums.

Our third witness is Mr. Joe Onek, a security policy analyst at the Open Society Policy Center. In this capacity, he provides counsel on issues of civil liberties and constitutional law. Mr. Onek first joined the government as a clerk to Chief Judge David L. Bazelton, of the District of Columbia circuit, and Supreme Court Justice, William J. Brennan.

In the Carter administration, he served as a member of the White House Domestic Policy staff and then as Deputy Counsel to the President. In the Clinton administration, he served as Principal Deputy Associate Attorney General and Senior Coordinator for Rule of Law in the State Department.

In the public interest world, he serves as an attorney and then director of the Center for Law and Social Policy and is a senior counsel and director of the Liberty and Security Initiative and the Constitution Project.

I want to thank all three of our witnesses for being here today. We look forward to your testimony.

And at this point now I would like to recognize the ranking member of the subcommittee, the gentlewoman from California, Ms. Lofgren, for any statement she might wish to make.

Ms. LOFGREN. Thank you, Mr. Chairman. I will be brief and submit my full statement for the record.

I do look forward to Mr. Negroponte's impending report on whether or not an open-source intelligence center or some other approach is the best way to ensure that open-source information is effectively leveraged by our intelligence agencies. And I do believe and agree that this hearing is important today to focus in on that issue.

Information sharing, as we know, is key to our efforts to protect America from terrorism, but while open-source information will undoubtedly contribute to our overall objective of promoting effective information sharing, I believe that this subcommittee must also consider the civil liberties and privacy implications of this and other new intelligence resources.

As Mr. Onek has noted in his prepared testimony, it seems likely that the intelligence community will use data mining of open-source materials in order to target terrorists who may be living and working among us, and that does raise issues relative to privacy, to profiling, and whenever there is profiling, there is the risk of actually missing terrorists because the terrorists know probably better than we do what profile to adopt to avoid being identified.

So I look forward to the testimony of all three of the individuals, and, specifically, as we move forward, I am eager to work with you in making sure that while we protect our nation from terrorism, we also protect our citizens from Big Brother.

And I yield back.

Mr. SIMMONS. I thank the gentlelady for her opening statement.

I note that the chairman of the full committee has just arrived, and I would be happy to yield time to the chairman.

Mr. COX. Thank you, Mr. Chairman.

I would like to welcome our witnesses and look forward to hearing their testimony.

I want to thank you for holding this hearing on this topic.

It is rather obvious that we should be using all of the open-source information that we can get. It is not obvious how to go about that or the degree to which the way that we have approached this over a period of years has kept up with or has not kept up with the pace of change in the production of information. There simply is more information now available than ever before, and what to do with it and how to harness it and how not to overlook the obvious become key questions.

Giving the American taxpayer value for money obviously requires using information from open source whenever possible, but the new idea here is simply to ask the question whether the United States government is effectively using the information that is most available to help solve the national security problems that are the most pressing.

We have a large government structure that was erected during the Cold War. We are trying constantly to keep it updated, but how much, this hearing is asking, how much of what we have got by way of existing infrastructure is left over from those different priorities and that different world, and how much has changed, how much have we changed already to make sure that we are tapping all of the resources that are available to us?

I would not be the first Californian to observe that gold is gold, whether it is found lying in a streambed or in sweltering heat deep

beneath the surface of the earth. It would in fact be a real stretch to suggest that with respect to certain whole fields of studies, such as risk assessment or microeconomics, which homeland security is very much concerned with these days if the U.S. government could even compete with private sector expertise and outside sources in terms of either quality or currency. That kind of information is critically important to meeting the mission of the Department of Homeland Security, particularly its Directorate of Information Analysis and Infrastructure Protection.

It would be equally absurd to suggest in noting its historic underappreciation that open-source information is a panacea, that it should be segregated from information acquired from clandestine sources in a separate entity or agency dedicated solely to its collection analysis, a sort of Federal Bureau of Found Objects. That is exactly the sort of intelligent-specific balkanization that the Homeland Security Act seeks to remedy by requiring the IAIP directorate to generate comprehensive analysis of terrorist threats and U.S. vulnerabilities in order to produce overall risk assessment.

The key is to bring all the available information, regardless of its origin or source, together for comprehensive and expert analysis and then of course to get that information to people who need it in real time so that we can act upon it. That was the ultimate lesson of September 11.

I want to add that it is a particular pleasure today to welcome back John Gannon to the committee, our former Staff Director who worked so hard for 2 years to create what is now this Permanent Standing Committee on Homeland Security. I look forward to his perspectives, as I always have, as well as to the testimony of our other witnesses.

Again, Mr. Chairman, thank you very much for scheduling this important hearing.

Mr. SIMMONS. Thank you, Mr. Chairman, and for taking time at what I know is a very busy time for you.

The Chair now recognizes the Ranking Member of the full committee, the gentleman from Mississippi, Mr. Thompson, for any statement or comments he might wish to make.

Mr. THOMPSON. Thank you very much, Mr. Chairman, Ranking Member, Chair of the full committee.

Dr. Gannon, glad to see you. There is life after Capitol Hill.

[Laughter.]

The other witnesses, we are glad to see you too.

I am glad that we are holding a hearing on the critical issue of open-source information and how the intelligence community can best leverage it in the fight against terrorism. Open-source information, when properly assembled and analyzed, can provide some of the most strategic, tactical and operational data imaginable in order to obtain an ever-evolving, near real-time picture of terrorists' plans.

The 9/11 Commission, the Intelligence Reform Act, the WMD report and our committee's own past authorization bill all can develop effective open-source information initiatives. I look forward to the release of the report from the Director of National Intelligence about whether our nation needs an open-source intelligence center

to centralize and coordinate the use of open-source information by the intelligence community.

That said, I am very concerned about the implication that the mining of open-source information will have for civil liberties and privacy. Emerging technologies are giving both the government and the private sector increasing precise ways of harvest very specific information. Not all of this information is about foreign governments and terrorist groups. Some of it is about ordinary people, like you and me. Our government cannot take a casual approach to open-source gathering.

In an effort to create a homeland security strategy that protects and strengthens our freedoms, our government cannot become an entity that whimsically violates our constitutional liberties and freedoms through surveillance and data mining that trace our every action and utterance.

Let me say that as a young college student in the sixties, I was one of those individuals that got a file created because I attended a speech given by Martin Luther King, Jr., and I am very concerned about the fact that I was generated and considered something other than a patriot by hearing a speech from Dr. King.

Open-source information is a resource that must be tapped to bolster the security of our nation. Information sharing is absolutely necessary to the defense of our nation. The mining of open-source information offers exciting possibilities to protect us from terrorists, but it also raises real risks.

I look forward to the testimony of our panelists today so that we can establish for this committee a formal policy on open-source information.

I yield back.

Mr. SIMMONS. Thank you, Mr. Thompson, for that statement and very much appreciate your perspectives on this important issue.

Other members of the committee are reminded that they can submit opening statements for the record.

And, again, we are pleased to have a distinguished panel of three gentlemen before us here today.

Let me remind the witnesses that their entire written statement will appear in the record, and we would ask that you try to limit your oral testimony to no more than 5 minutes. There will be a clock in front of you there. In that way, we can guarantee that members will have maximum opportunity to ask questions and engage in a dialogue.

That being said, the Chair now recognizes Dr. Gannon for his testimony.

STATEMENT OF JOHN GANNON, VICE PRESIDENT FOR GLOBAL ANALYSIS, BAE SYSTEMS, INFORMATION TECHNOLOGY

Dr. GANNON. Mr. Chairman, it is a particular pleasure to be back here, and I would like to take the opportunity right off the bat to congratulate this full committee for its work in passing an authorization bill, I know what an achievement that is, and also for passing the first responder bill. I think a demonstration of how constructive this committee has been and how bipartisan, really, the approach has been to these critical national security problems.

I did submit a statement for the record, and I will very quickly just summarize the five points that I made there. And, really, these points come out of my own career in intelligence over an almost 25-year period.

The first point I make is that the intelligence community's interest in open source goes back, I think, to the very beginning to the community itself. As an analyst, I often consulted with outside experts. We had, as many of you know, the Foreign Broadcast Information Service, which provided us with daily press and media reports and also translations of those reports and did a fabulous job over my career in supporting our analysis.

Those were the days, of course, when we were dealing primarily with a single strategic threat from the Soviet Union, very much a closed society where it was very difficult to find value added in open source, but I think we did a commendable job of it.

One point I would emphasize, however, about that era, really sort of prior to the mid-1980s, was that we were dealing, I think, in a very different environment where the expertise and the information was pulling from the outside into the community. We really did see ourselves in the community as the center of gravity on information and expertise. So I have described the open source as kind of a frosting on our cake.

Things changed dramatically, really a major paradigm shift, in the mid-1980s, and I had the responsibility of bringing the first computers into the Office of European Analysis in the mid-1980s—five Delta DATAS. I mean, just to demonstrate how the world has changed, those five computers were put up in offices where analysts linked to specialists who handled them. The analysts did not have them at their own desks.

It used to take me in that period about 14 days to get a newspaper from the Caribbean and Latin America where I was covering, and policymakers were quite willing to wait for me to finish my analysis and fulfill the very large information gaps with my judgments and my expertise.

Three issues I think changed dramatically the environment in which we worked in the community. First of all, was of course the information revolution itself where in a period of a very few years we had computers at every analysts' desk, and the analysts became quite adept, particularly the new entrants of that labor force, in dealing with the computer information technology world.

I talked about taking 14 days to get a newspaper to me when I started as an analyst. Today, every newspaper virtually in the world is available to every analyst in the intelligence community before the people in the country in which the newspaper is produced get up and read it. We have gone from an information scarcity environment to an information glut environment, and the community has struggled to manage that glut through the development, first of all, by using technology developed, analytic tools and software that enable us to make sense of all that information.

But also we had the geopolitical change with the collapse of the Soviet Union, which brought again from an environment of a single strategic threat to multiple threats, multiple conflicts, issues where open source was essential for us to understand that range and com-

plexity involved in those issues. And that challenge continues today.

And, finally, the homeland security challenge of more recent years brought not only a whole range of new issues for us to deal with where open source is a critical contributor but also brought us a whole new set of customers in the state and local governments and the private sector, people who need to have some form of intelligence support to do the frontline work or undertake the frontline responsibilities that we say they have.

We did in the 1980s have an organization called the Intelligence Community Open Source Program Office, and what I would point out about this is I think perhaps there are different judgments about the success or failure of that office, but I think, to one degree, it failed to adequately recognize the overwhelming nature of the information change that had taken place.

COSPO I think treated open source as another INT. It treated open source as it treated signals intelligence, measurement and signature intelligence, human intelligence, as one more INT when in fact we had seen a dramatic shift in the whole center of gravity of information and expertise outside the intelligence community into the open source world. So what COSPO, I think, was doing, as I saw it, was trying to take the ocean and putting in a swimming pool.

We were challenged in the intelligence community to face the fact that on the issues that we were dealing with, from the collapse of the Soviet Union onward, were issues where the expertise to deal with them and a lot of the information to deal with them was outside the intelligence community, and we need multiform strategies to deal with that, including the use of technology and also getting our analysts, frankly, to move outside the community, engage with experts who have expertise and information in their heads, which really never gets translated into collection systems.

The third critical point I would make is that we discovered with more and more use of technology to help us deal with the information flow, that expertise of our analysts actually became more important. When you are dealing with a flood of information, having people who really know the issues, who can extract information or interpret information and analyze it, you are required to have more and more senior people how really do know the issues.

And I will tell you, as I went down to a principals meeting to deal with some of these complex issues in the White House, at the end of the day, whatever technology had been brought to bear on our aggregating and analyzing information, I wanted a human being who knew what he or she was talking about. It is, in the end, I think about people.

The fourth point I would make is about structure. I do not think there is any quarrel here or anywhere really in the community about the importance of open-source information and about the fact that the intelligence community is behind the curve and has been for some time in exploiting open-source information.

But how we structure a solution I think is a matter of debate, and from my own experience I am clearly on the side of opposition to new structures, particularly open source directorates, and I am much more in favor of a distributed model that puts technology in

the hands of all analysts so that they can use open-source information. Whether a signals intelligence analyst, a human intelligence analyst, they all need open source, so you cannot separate it out as a separate discipline, in my judgment.

So I think we have to pursue an aggressive approach, bringing technology to bear for the benefit of analysis but not structured in a way that separates open source from the clear need to integrate open source with classified information.

And the final point I would make is I think from the days of the Transition Planning Office and the incorporation, I think, of a lot of the original discussions into the Homeland Security Act, it was recognized that the Homeland Security Department would be uniquely positioned to be a broker of information on critical issues with regard to homeland security. The biothreat, for example, the Homeland Security Department would be in touch with HHS, it would be in touch with John's Hopkins University, University of Pittsburgh, Stanford, places that have repositories of real expertise in bioscience and the biothreat and would be better positioned than in fact an intelligence agency would to bring that expertise together, to be the go-to agency for the U.S. government.

But I would also emphasize, and my own conviction is that, the Department of Homeland Security, while it has a particular role to play in the open-source area, it must have, I think, a fully capable and robust intelligence unit that has full access to the intelligence community and is a full player in that community.

[The statement of Dr. Gannon follows:]

PREPARED STATEMENT OF DR. JOHN C. GANNON

Good morning, Mr. Chairman, and members of the subcommittee. It is a special pleasure for me to participate in this hearing with members and staff with whom I was privileged to work closely in the recent past, and to discuss intelligence issues, with which I have been involved for most of my professional life. The subject of this hearing, the effective use of open-source information, is a priority issue today not just for homeland security but for the whole intelligence and law-enforcement communities.

Intelligence and law-enforcement officers must do their best to present a complete picture, to integrate classified and unclassified information in the story they tell. Open-source information is today more important than ever in getting that story right. The Department of Homeland Security, in my view, should play a pivotal role in brokering open-source information and in leveraging expertise outside the IC. But, to do this effectively, it also must be a key player in the classified world. In today's intelligence business, you cannot have one without the other. Intelligence should identify and fill critical gaps that cannot be addressed by open sources.

Let me summarize the five points I will make this morning:

1. Open-source exploitation in the IC is as old as the Community itself. We have always sought open-source information and selective engagement with outside experts to deepen our analysis and to drive collection priorities. The Foreign Broadcast Information Bureau (FBIS) provided excellent coverage of foreign media during my career. For most of the Cold War period, however, much of our focus was on the closed societies of the Soviet Union, in which there was a scarcity of reliable or useful open-source material to be had. And our open-source effort was directed toward bringing unclassified information into our classified environment, which was the center of our analytic universe.

2. The open-source challenge has increased exponentially over the past twenty years for at least three key reasons. First, the revolution in information technology has transformed the world of both the intelligence analyst and consumer from an information-scarcity environment to an information-glut environment. Second, the post-Soviet geopolitical transformation and the technology revolution have opened closed societies and introduced new, complex regional and transnational issues that more often than not require—as a top priority—heavy

doses of real-time open-source information. And, finally, the emergence of homeland security as a national priority has introduced new analytic issues, new collection targets, and a whole set of new intelligence consumers among state and local governments and the private sector.

By contrast with the Cold War period, the center of gravity for expertise on many of these issues is outside the IC. We need new strategies to get this information, including state-of-the-art analytic tools and far-sighted policies that encourage our analysts to get away from their desks to engage with outside experts. Today, this is all a work in progress.

3. The information revolution, paradoxically, has increased the demand for expert analysts in the IC. Technology is an indispensable enabler for the IC analyst inundated with information. But it is no substitute for human expertise. It takes IC experts to extract the best data from today's fast-moving information flow and to identify the sharpest outside experts for consultation. This is a dynamic process, which aims to get the President, his top advisers, and the Congress the best answer possible information on any national security question—by uniting technology and brainpower and by integrating classified and unclassified information.

4. I believe that the creation of new, large open-source IC structures, such as an open-source directorate at CIA or any other agency including DHS, would be a step in the wrong direction. The challenge for all our analysts today is to integrate, as never before, the classified and unclassified environments. All-source analysts and single-INT analysts (e.g., human intelligence, geospatial intelligence, signals-intelligence, measurement-and-signature intelligence analysts, etc.) all need open-source information to make their contributions to the story being told and to understand where there are collection gaps that they might be able to fill.

OPINT (open-source) analysts, who increasingly staff IC operations centers and selective substantive teams, are skilled technically to exploit open sources. They serve the cause of integration, not of division between classified and unclassified information. An open-source directorate, in my view, would likely complicate this needed integration and further strain resources already stretched by excessive structure in the IC.

5. The Information Analysis (IA) component of DHS serves a Secretary with major responsibilities for prevention of terrorism against the homeland, for protection of our critical infrastructure, and for ensuring that we are able to respond effectively if an attack should occur. The Secretary of Homeland Security, as I (and the Homeland Security Act of 2002) see him, is a key player on the President's national security team, who is uniquely positioned by be an invaluable open-source collector but still needs a fully capable intelligence unit to address his critical priorities and to levy his sensitive collection requirements on the IC. There should be, in my opinion, a direct relationship between the responsibilities assigned to the Secretary and the quality of the intelligence organization dedicated to support him.

This should not require a bureaucratic empire. Senior expertise on homeland issues is far more important than the numbers of intelligence analysts in DHS. But IA must be able to compete in hiring such senior officers. I believe that IA could be effective as a relatively small intelligence unit if it has effective outreach within the IC, across the USG, and beyond to the first-responder community. But it must have adequate facilities and infrastructure and full connectivity with other IC agencies. IA, in short, must be a recognized and respected player in the classified domain. IA must be seen an equal partner with the other fourteen members of the IC. It must have the resources and authorities to play this role. Anything less will perpetuate the unsatisfactory situation we face today.

Critical Importance of Open Source

Open-source information today is indispensable to the production of authoritative IC analysis. It increasingly contains the best information to answer some of the most important questions posed to the IC. Media reports, once the open-source mother lode, are now are just a small portion of the take, which comprises a vast array of documents and reports publicly retrievable but often difficult to find in today's high-volume, high-speed information flow. Open sources provide vital information for the policymaker, who today is much better informed than in the past because of his or her easy and timely access to information, which, in turn, strengthens a firm demand for "on-time" delivery of analysis. Accessing, collecting, and analyzing open-source information, in short, is a multifaceted challenge that can only

be met with a multi-front response or strategy that engages both people and technology in innovative ways.

During the Cold War, covering the globe for the IC was largely a Soviet-centric enterprise. The Soviet Union was the single-strategic threat we faced. Today, global coverage entails the responsibility to assess diverse, complex, and dispersed threats around the world. In addition to traditional intelligence concerns—such as the future of Russia and China; international terrorism, narcotics, and proliferation of weapons of mass effect; and political turmoil in Indonesia or civil conflicts in Africa—the new environment features many nontraditional missions. The IC now provides intelligence about peacekeeping operations, humanitarian assistance, sanctions monitoring, information warfare, and threats to our space systems. Many of these missions are operationally focused, requiring growing proportions of the analytic and collection work force to function in an ad hoc crisis mode.

Clandestinely derived intelligence is as valuable as ever, but, in my recent experience, open source information now dominates the universe of the intelligence analyst, a fact that is unlikely to change for the foreseeable future. The revolution in information technology and telecommunications has fundamentally transformed the globe that the IC covers, the services that it provides to consumers, and the workplace in which its people function. While it is as important as ever to protect our sensitive sources and methods, it is more important than in the past to integrate the best information from all sources—including unclassified—into IC analysis.

- *Information abounds.* Twenty years ago, current and reliable information on the Soviet Union, Central Asia, and other corners of the world was scarce, foreign newspapers took weeks to arrive at an analyst's desk, and policymakers were willing to wait days or even weeks for a paper on their issues. Today, the information is here and now in abundance, policymakers want it in real time, and intelligence requirements are much sharper and more time sensitive. The Washington-based analyst can send a message and get a response from a post in a remote country faster than it used to take to exchange notes by pneumatic tube with counterparts in the same IC building. Technology may make our jobs easier, but it does not feel that way. We are all working much harder.

- *Governments are losing control.* Governments have less and less capacity to control information flows. International terrorists, narcotraffickers, organized crime groups, and weapons proliferators are taking advantage of the new technologies, bypassing governments or seeking to undermine them when governments try to block their illegal activities. As al-Qa'ida demonstrated in planning 9/11, tech-savvy terrorists are adept at exploiting our technology for their nefarious purposes. Non-state actors are likely to be using laptop computers, establishing their own Web sites, and using sophisticated encryption. In the years ahead, these enhanced capabilities will raise the profile of transnational issues that are already high on the IC agenda. In this environment, open-source information will continue to be essential to our understanding of these groups and how they operate.

Solutions

Technology is a major part of the answer to the magnitude of the open-source challenge, but it is no substitute for the other essential component: skilled people. The IC must provide the analytic tools needed to assess and exploit the vast amount of information available, and it must invest more in people, whose expertise is crucial for prioritizing, interpreting, and analyzing this information. The greater the volume of information to assess, the stronger must be the expertise to evaluate it. In this context, DHS, as a top priority, must recruit and retain the necessary in-house expertise and develop the external partnerships to speak authoritatively on threats to the homeland—as the Homeland Security Act of 2002 requires of it.

Today, cognitive analytic tools are continuously under development in both the private sector and the government to facilitate management of the information glut, enhancing the IC's ability to filter, search and prioritize potentially overwhelming volumes of information. These tools do not discriminate between classified and unclassified information. They help the analyst to draw the best information from all sources into an integrated, high-quality analytic product.

- *Clustering* lets analysts exploit the most useful data sets first, as well as to recognize meaningful patterns and relationships, thereby helping the IC perform its warning function.
- *Link Analysis* helps to establish relationships between a known problem and known actors and to detect patterns of activities that warrant particular attention.
- *Time-series analysis* can enable analysts to track actions over time so that unusual patterns of activity can be identified.

• *Visualization and Animation* allow analysts and consumers to see extensive and complex data laid out in dynamic and easily understandable formats and models.
• *Automated database population* is designed to free analysts from the tedious and time-consuming function of manually inputting information into databases, reducing the potential for errors and inconsistencies.

One of the strongest and most consistent demands from IC analysts is ability to search and exploit both classified and unclassified information from a single workstation. The Community is making progress on this. It also is developing better ways to standardize information and tag it using metadata—or reference information—to make it easier to search, structure, and enter information into data bases.

Geospatial intelligence provides an excellent example of how today's skilled analysts—the same analysts in one place or on one team—are routinely integrating both classified and unclassified information in their path-breaking work. They take high-quality orthorectified (three dimensional to scale) imagery and superimpose on it both classified intelligence and vital unclassified information, which creates a complete picture of a terrain, site, facility, or densely populated urban area. Such an integrated picture is operationally useful as well as informative for all consumers.

A good example of the all-source analytic process is the National Intelligence Council's *Global Trends 2015* project of 2001 and its follow-up this year, *Mapping the Global Future,* which resulted from months of close collaboration between IC analysts and experts from the USG, academia, and the private sector. The disposition of outside experts to collaborate with the IC has never been greater. This collaboration or integration of effort should be encouraged as a model for dealing with the complex issues on today's intelligence agenda. The goal, again, is to deliver the best product from all sources.

IA's Future

The US Intelligence Community today is much more than an espionage service. It constitutes the world's biggest and most powerful information-based business, collecting and analyzing both clandestinely derived and open-source information. To do its job well, the IC should be on the leading edge of open-source exploitation so that it will have the best information to inform its analysis and so that it can surgically target our clandestine collection systems on critical information gaps. The IC's comparative advantage over other information-based enterprises is that its clandestine collection has the potential to add significant value to all source-analysis—to the benefit of US National Security.

To function effectively as a member of today's IC, an agency must play fully in both the classified and unclassified arenas. This is not a numbers game. It is about having adequate facilities, infrastructure, analytic expertise, IC connectivity, and authority to fully support the agency's mission. The Department of Homeland Security has a vital mission to protect America. It should have its own intelligence organization capable of supporting that mission.

Mr. SIMMONS. Thank you very much, Dr. Gannon.

Now, the Chair recognizes Mr. Jardines.

STATEMENT OF ELIOT JARDINES, PRESIDENT, OPEN SOURCE PUBLISHING, INC.

Mr. JARDINES. Good morning, Chairman Simmons, Congresswoman Lofgren, members of the subcommittee. I thank you for the opportunity to participate in this hearing.

I am Eliot Jardines, president of Open Source Publishing, a private firm that does open source exploitation support for the U.S. government.

Over the past 14 years, my career as an open-source intelligence practitioner has provided me with an opportunity to understand the significant contributions which the open-source intelligence discipline, or OSINT, can bring to the Department of Homeland Security.

From Peal Harbor to the September 11 terrorist attacks, intelligence failures have largely resulted not from a lack of information

but rather from an inability to disseminate that information effectively.

In looking at the nature of the first responder community, it is apparent that timeliness and flexibility of open-source intelligence is particularly useful. Due to its unclassified nature, OSINT can be shared extensively without compromising national security.

Not only can these OSINT products be disseminated to inspectors at a port of entry, they can also be provided to state and local law enforcement. In fact, OSINT products could be disseminated to the full complement of first responders, such as fire fighters, EMTs, university police departments, hospitals and even private security firms.

Intelligence support to the homeland security community below the federal level is largely non-existent due to classification issues. The way I see it, either we provide top-secret security clearances to all chiefs of police, fire chiefs and sheriffs in the country or we provide them with some means of gaining access to open-source information.

In the event, God forbid, of another terrorist attack, it is these local responders who will be called upon to put their lives on the line. Do we not owe it to them to at least provide them some form of intelligence support?

How do we go about providing this support? First of all, OSINT must be effectively incorporated into the DHS all-source analysis process. This can only be achieved by changing the prevailing mindset that classification is a measure of quality. The highly classified intelligence report is no better or more important than one of lower classification. Its classification is only indicative of the degree of damage done to national security should sources and methods be compromised.

Secondly, we must establish OSINT as an equal partner with the traditional intelligence discipline. This is achieved by providing the infrastructure necessary to acquire, process, analyze and disseminate open-source intelligence. It is essential that a formalized means exists for the exploitation of OSINT.

The third recommendation is to develop a cadre of highly skilled open-source analysts and library professionals to provide tailored open-source intelligence support at DHS.

Fourthly, in order to effectively incorporate OSINT into the DHS analytical process, we must redefine that process. The traditional linear intelligence cycle is more a manifestation of bureaucratic structure than a description of the open-source exploitation process.

In its recent book entitled, "Intelligence Analysis: A Target-centric Approach," Dr. Robert Clark proposes a more target-centric, iterative and collaborative approach which would be far more effective than our current traditional intelligence cycle.

Lastly, OSINT should establish a streamlined contracting process to enable cost-effective outsourcing of OSINT requirements and commercial content procurement.

The effective dissemination of open-source intelligence by DHS is also essential to our national security. One recommendation is to provide all DHS entities with access to the Open-Source Information System, or OSIS. Operating at the "for official use only" level, OSIS has provided the intelligence community with access to open-

source analytical products and commercial content since 1994. Rather than reinventing the wheel with a separate system, DHS should be encouraged to use this network and explore the possibility of OSIS accounts for all police and fire chiefs.

I understand the subcommittee has particular interest in examining whether the Department should establish its own open-source intelligence agency. Both the 9/11 Commission and the Weapons of Mass Destruction Commission have recommended that the Director of National Intelligence consider establishing an OSINT agency or center. I believe it would be a mistake for DHS to rely solely on a DNI center to fulfill its OSINT requirements. DHS should establish its own OSINT agency or center to ensure that its unique needs are met.

In summation, I believe open-source exploitation can provide timely, accurate and actionable intelligence for the Department of Homeland Security, most importantly, at minimal cost.

Thank you.

[The statement of Mr. Jardines follows:]

PREPARED STATEMENT OF ELIOT A. JARDINES

Chairman Simmons, Congresswoman Lofgren, and members of the Subcommittee, I thank you for the opportunity to participate in this hearing. I am Eliot Jardines, President of Open Source Publishing, Incorporated, a private firm which specializes in providing open source intelligence support to the US military, the intelligence community and federal law enforcement. Open Source Publishing has provided open source exploitation, analysis and training for federal agencies since its inception in 1996.

Over the past fourteen years, my career as an open source intelligence practitioner and educator has provided me with an opportunity to understand the significant contributions which the open source intelligence discipline, or OSINT, can bring to the all-source intelligence analysis process. With that said, I am also keenly aware of the limitations of this discipline which should not be viewed as a panacea, but rather a highly effective component of the intelligence toolkit.

The Value of OSINT for Homeland Security

From Peal Harbor to the September 11th terrorist attacks, intelligence failures have largely resulted not from a lack of information, but rather the inability to effectively disseminate that information or intelligence. In looking at the nature of the homeland security and first responder communities, it is apparent that open source intelligence is particularly useful. Due to its unclassified nature, OSINT can be shared extensively without compromising national security.

The flexibility and timeliness of open source intelligence is particularly salient for the Department of Homeland Security because it provides a means by which critical intelligence can be acquired and disseminated without the encumbrances imposed by classification. As an example, during the mid-1990s I was a member of a team which conducted an assessment of how the US Customs Service collected, analyzed and disseminated intelligence. We soon discovered that it was incredibly difficult to disseminate classified information to the tactical level.

Highly classified messages or analytical products underwent a sanitation process which tended to remove important details. The end result was intelligence reports which were too general or broad to be of much use. An attempt to disseminate highly classified documents down to the port of entry level, resulted in the discovery that few if any personnel at that level had the requisite clearances. In other instances, the necessary security infrastructure was unavailable. In one memorable instance, we discovered that a port of entry was able to receive classified faxes, but did not have approved facilities for storage of classified data. The net result was that the classified fax was generally left off. In the rare instances classified faxes were received, they were promptly shredded as no approved means of classified storage was available. With that said, the Customs Service, now the Bureau of Customs and Border Protection, has made dramatic improvements regarding disseminating intelligence. The CPB's Office of Intelligence under the leadership of Roy Surrett, has in many ways set the standard for responsive intelligence support.

However, given the largely unclassified nature of open source intelligence products, the aforementioned issues of clearances and security infrastructure are irrelevant. Not only can these OSINT products be disseminated to inspectors at a port of entry, they can also be provided to state and local law enforcement. In fact, OSINT products could be disseminated to the full compliment of first responders such as firefighters, EMTs, university police departments, hospitals and private security firms. Consider for a moment what a paradigm shift that would represent.

Intelligence community support to the homeland security community below the federal level is largely non-existent due to classification issues. The way I see it, either we provide Top Secret security clearances and the necessary communications and storage capabilities for every single chief of police, sheriff and fire chief in the country, or we invest a far smaller amount to establish a robust OSINT capability. In the event, God-forbid, of another terrorist attack upon the homeland, it will be the local first responders who will be called upon to put their lives on the line. Do we not owe it to them to at least provide some intelligence support?

Integrating OSINT into the DHS analytical process

How then, do we go about providing this open source intelligence support? First of all, OSINT must be effectively incorporated into the DHS all-source analysis process. This can only be achieved by changing the prevailing mindset that classification is a measure of quality. A highly classified intelligence report is no better or more important than one of lower classification, it is only indicative of the degree of damage done to national security should its inherent sources and methods be compromised.

Secondly, we must establish OSINT as an equal partner with human intelligence (HUMINT), signals intelligence (SIGINT), imagery intelligence (IMINT) and measurement and signatures intelligence (MASINT). This is achieved by providing the infrastructure necessary to acquire, process, analyze and disseminate open source intelligence. It is essential that a formalized means exist for the exploitation of OSINT. Of particular importance is the establishment of an open source intelligence requirements management system. Having a requirements management system in place would allow DHS to identify its standing and ad hoc intelligence collection requirements, as well as what entity or activity would be responsible for fulfilling those needs.

For too long, open source exploitation has been delegated as merely an additional duty for intelligence analysts. This is simply a ridiculous notion. No one would seriously propose that intelligence analysts be required to collect their own signals or imagery intelligence. However, that is precisely what we do with open source intelligence. The third recommendation for effective integration of OSINT, is to develop a cadre of highly skilled open source analysts and library professionals to work along side traditional intelligence analysts in order to provide tailored OSINT support to the DHS analytical process. Likewise, these analysts could fulfill an analyst helpdesk function fulfilling ad hoc requirements for DHS entities and the first responder community. It is vital that these OSINT positions be given the importance they deserve and that they not devolve into convenient placeholders for personnel awaiting security clearances.

Fourthly, in order to effectively incorporate OSINT into the DHS analytical process, we must redefine that process. We must begin by redefining the traditional linear intelligence cycle which is more a manifestation of the bureaucratic structure of the intelligence community than a description of the intelligence exploitation process. In his recent seminal work on the issue, *Intelligence Analysis: A Target Centric Approach* Dr. Robert M. Clark describes the traditional intelligence cycle as one that, "defines an *antisocial* series of steps that constrains the flow of information. It separates collectors from processors from analysts and too often results in "throwing information over the wall' to become the next person's responsibility. Everyone neatly avoids responsibility for the quality of the final product. Because this compartmentalized process results in formalized and relatively inflexible requirements at each stage, it is more predictable and therefore more vulnerable to an opponent's countermeasures." [1]

Dr. Clark goes on to propose a more target-centric, iterative and collaborative approach which is far more effective than the traditional intelligence cycle. In Clark's target-centric approach, the process is a resilient one in which collectors, analysts and customers are integral and accountable. Redefining the analytical process is a lengthy discussion which exceeds the time constraints of this hearing. I would however, commend Dr. Clark's book to the Subcommittee for further consideration.

---

[1] Clark, Robert M. (2004). *Intelligence Analysis: A Target-Centric Approach.* Washington, DC: Congressional Quarterly Press, 15.

The Traditional Intelligence Cycle: Where is the Target?

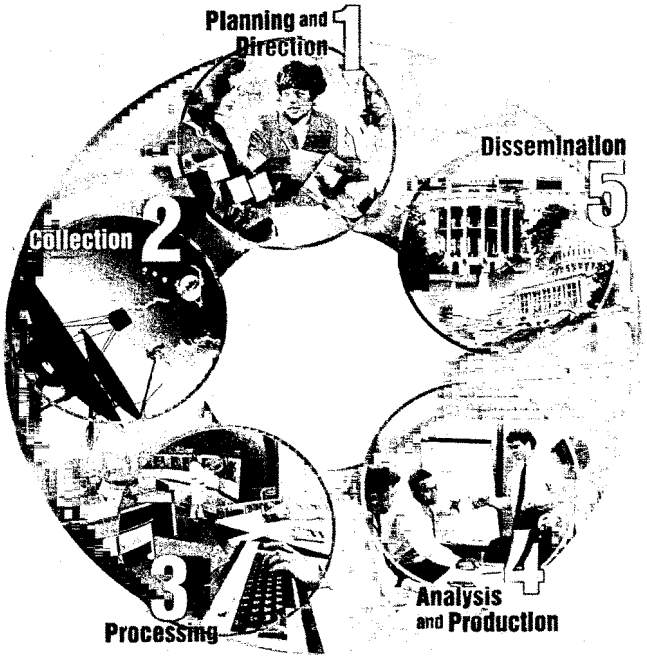

Image courtesy of the Central Intelligence Agency's Factbook on Intelligence, 2002.

The final way to integrate OSINT into analytical activities at DHS is to establish a streamlined and specialized contracting process to enable outsourcing of OSINT requirements and commercial content procurement. Centralizing the procurement of commercial content such as databases, periodicals or commercial imagery for all of DHS would result in a dramatic cost savings which could in turn, be used to fund further OSINT efforts or content procurement. While centralizing content procurement, DHS must ensure the process is flexible and responsive enough to meet time sensitive or "unusual" requirements.

At Open Source Publishing, we are frequently asked by our customers to acquire individual books or maps which typically do not exceed $50.00 in cost. The conventional government procurement process for such small purchases requires a disproportionate outlay of personnel resources and the death of innumerable trees. In particular, the restrictions and paperwork surrounding the use of government credit cards (IMPAC cards) deserves much attention. Very useful in supporting OSINT efforts would be the establishment of a DHS blanket purchase agreement (BPA) to allow any DHS entity to acquire OSINT related products and services in a simple and cost effective manner.

If such a blanket purchase agreement becomes reality, particular care should be given to insure that the standard practice among the large government contractors of charging exorbitant pass-through fees be kept to a minimum. One particularly effective approach is to award the BPA to a number of prime contractors who would be required to disclose all pass-through percentages and "management fees" upfront to subcontractors interested in using the contract vehicle. In order to insure the success of such an effort, it is essential that the all too common "raping and pillaging" by prime contractors be minimized. The procurement of a $50.00 book should not require a $10.00 pass-through fee and $200.00 in management and administrative charges by the prime.

Disseminating OSINT

The effective dissemination of open source intelligence within the Department of Homeland Security and the first responder community is essential to our national security. As mentioned previously, many intelligence failures are a result, not of faulty analysis, but rather the inability to disseminate intelligence or information

in a timely manner. No other department in our government is more reliant on effective information dissemination to fulfill its mission than DHS. Therefore, the unclassified nature of open source intelligence greatly enhances its prospects for wide distribution, and as such should be regarded as a key within DHS.

One recommendation to assist DHS in improving its OSINT dissemination efforts, is to provide all DHS entities with access to the Open Source Information System (OSIS). Operating at the *For Official Use Only* level, OSIS has provided the intelligence community with access to open source analytical products and commercial content since 1994. Rather than re-inventing the wheel, DHS should be encouraged to coordinate its efforts with the Intelink Management Office which manages OSIS. Another recommendation would be to allow *all* police and fire chiefs access to the homeland security related resources on OSIS. This dramatic expansion of access for first responders can be accomplished by simply leveraging the OSIS network's existing infrastructure. While additional OSIS funding would be required, the cost would be dramatically less than creating such a network from scratch. This arrangement also facilitates collaboration among the first responder community via the OSIS network's collaboration tools and training resources, again at little additional cost.

Should DHS Establish an OSINT Agency?

I understand the Subcommittee has a particular interest in examining whether the Department should establish its own open source intelligence agency. Both the 9/11 Commission and the Weapons of Mass Destruction Commission have recommended that the Director of National Intelligence consider establishing an OSINT agency or center. It is my feeling that it would be a mistake for DHS to rely solely on a DNI OSINT center to fulfill homeland security related OSINT requirements. While capable of providing some degree of support, the DNI's OSINT center could not be as responsive to the unique needs of DHS and the first responder community as a specialized OSINT agency or center would be.

Indicative of the need for specialized OSINT support, the Department of Defense's Open Source Council recently recommended the establishment of a DoD OSINT Program Office to better support the unique needs of warfighters and Defense decision makers. While in general I am no fan of establishing new agencies or centers, in this case the unique requirements of the homeland security community warrants just such an action. I think just about anyone would agree that it is a stretch to think that a single OSINT agency or center could adequately provide for all the needs of such widely divergent agencies like DHS, DoD and the Department of State.

Conclusion

In summation, I believe open source exploitation can provide timely, accurate and actionable intelligence to the Department of Homeland Security as well as the first responder community, particularly at the state and local level. Effective use of OSINT at DHS requires first of all, a change of perspective regarding the value of intelligence—which is *not* determined by its classification level. Secondly, it requires viewing OSINT as an equal partner in the all-source analysis process. Thirdly, OSINT should be conducted by highly skilled analysts and practitioners, not merely the uncleared. Fourthly, effective OSINT exploitation requires a complete reevaluation of the traditional intelligence cycle which is largely ill-suited to the demands of the Global War on Terror. Lastly, effective OSINT requires a flexible means of outsourcing and content procurement.

In terms of effective dissemination of OSINT within DHS and the first responder community, it is imperative that DHS not reinvent the wheel but rather leverage existing capabilities such as the Open Source Information System. Finally, it is my belief that the Department of Homeland Security should establish its own OSINT agency or center to meet the unique needs of its constituents. I thank the Subcommittee for its consideration of my testimony.

Mr. SIMMONS. Thank you very much, Mr. Jardines, for that very concise and timely presentation. Thank you.

And now the Chair recognizes Joe Onek for his testimony.

STATEMENT OF JOE ONEK, SENIOR POLICY ANALYST, OPEN SOCIETY INSTITUTE

Mr. ONEK. Mr. Chairman, Ranking Member Lofgren, members of the subcommittee, I thank you for giving me the opportunity to testify this morning.

In recent years, the government's authority and capability to collect and share open-source information about Americans has grown enormously. I think we all recognize the potential benefits of collecting that open-source information in order to protect our country, but at the same time this collection of information raises a variety of privacy and civil liberties issues, and the concerns that it raises is reflected, for example, in the controversy over section 215 of the Patriot Act, the so-called library records provision, and to proposals about administrative subpoenas.

But in my limited time this morning, I would like to focus on another concern, what I would call a civil rights concern, and it is that the danger that if our systems work as well as we hope they will work, the information that the government gathers and shares will be used in ways that unfairly discriminate against Muslim Americans.

Although only a miniscule number of Muslim Americans are involved in any form of terrorism, it is obvious that the government's expanded information gathering and data mining systems will focus on Muslim Americans. Even if they do not single out Muslim Americans directly by name or religious affiliation, Muslims will appear disproportionately on the government's computer screens because they are the people who are most likely, naturally and innocently, to visit or telephone or send money to places like Pakistan and Iraq.

Inevitably, government officials will learn more about Muslim Americans than about other Americans. Many Americans, for example, whether we like it or not, employ undocumented workers in their homes and businesses. Many Americans do not fully report their earnings from tips to the IRS. But the Americans who may be caught doing these things and subject to prosecution may disproportionately be Muslim.

Similarly, there are millions of persons in the United States who are violating the immigration laws. Their offenses range from illegal entry to failure to notify authorities of an address change. Again, Muslim violators will be caught and subjected to deportation in far greater percentages than other violators.

Now, at first blush, there may be seen no problem at all with prosecuting or deporting persons who have violated the law, but our nation's legal and moral values require equal application of the law. When, for example, there are stretches of highway where virtually everyone exceeds the speed limit, it is not permissible for the police to stop and ticket only or primarily those speeders who are African American.

My concern is that the new information gathering and data mining systems will often deliberately focus on persons who are likely to be Muslim, and therefore it is necessary to address the unequal application of the laws that will inevitably follow.

And I am therefore going to make what I understand is a provocative proposal. I am going to propose that information gathered for antiterrorist purposes not be used against individuals except in proceedings that directly relate to terrorism or other very, very serious crimes. Unless this restriction is imposed, criminal and immigration laws will be disproportionately applied against Muslim

Americans. This unfairness will breed discontent in the Muslim community and will undermine the fight against terrorism.

It is important both that our country and be seen by the world as fair to Muslim Americans and that it enlists the full cooperation of the Muslim community in antiterrorism efforts. These objectives can only be met if Muslims in this country believe the government is treating them fairly.

And this proposal does not mean that anybody will be granted immunity for criminal activity or amnesty. The government remains free to bring criminal or immigration cases provided that it does not use information generated by antiterrorist data mining systems in cases not involving terrorism or other similar violent crimes or serious crimes.

This limitation may require some segregation of information, it may impose some burdens on government, but these burdens are a small price to pay to ensure fairness to all Americans and to strengthen the fight against terrorism.

And, interestingly, and I will close on this note, and I think you are familiar with this, the federal government is currently implementing a somewhat similar immunity program under the Homeland Security Act. Section 214 of the Act provides that companies, such as nuclear power plants, that voluntarily disclose to the government critical infrastructure information concerning their vulnerabilities to terrorism are guaranteed that the government will not use that information against them in any civil action. And this is so even though the disclosed information may indicate that the company is not complying with various safety or environmental laws and is thus subject to severe civil penalties.

Congress made the determination in the Homeland Security Act that granting companies this limited immunity served important national security interests, and I believe national security interests are also served by providing limited use immunity to people caught up in our antiterrorism data mining efforts.

Thank you.

[The statement of Mr. Onek follows:]

PREPARED STATEMENT OF JOSEPH ONEK

Mr. Chairman, Ranking Member Lofgren and members of the Subcommittee. Thank you for giving me the opportunity to testify this morning on issues related to the government's access to open-source information.

As the Subcommittee well knows, since 9/11 Congress has enacted many provisionsz—in the Patriot Act, the Homeland Security Act and the Intelligence Reform legislation—authorizing or requiring federal agencies to collect and share more information about Americans. At the same time, new technologies are making it easier for government agencies to gather, store and analyze information. These developments have raised a variety of concerns.

Many Americans, I believe, have a visceral unease about the fact that the government has the capacity to gather so much information about them. That unease explains the powerful opposition to the Defense Department's Total Information Awareness Program. It also explains the opposition to section 215 of the Patriot Act—the so-called library records provision. I . myself agree that section 215 should be amended as proposed in the SAFE Act to prevent fishing expeditions by government officials and keep their focus properly on information relating to agents of a foreign power. I also believe that the government must do a better job of explaining its information collecting and sharing practices. Recently, for example, the Department of Homeland proposed to exempt one of its systems of records from the requirements of the Privacy Act. Its notices explaining the request were so opaque

that it was difficult to understand what records were involved and why the exemption was appropriate.

Another development that, according to public opinion polls, is raising concerns about privacy is the proposal to authorize administrative subpoenas in national security investigations. The Senate Select Committee on Intelligence has reported out legislation granting the government administrative subpoena power under the Foreign Intelligence Surveillance Act (FISA). Administrative subpoenas are now used in many types of investigations, and the government asks why they shouldn't also be used by the FBI in the fight against terrorism. But, as I testified before the Senate Intelligence Committee, the government ignores some very crucial facts.

First, administrative subpoenas are typically used for discrete purposes and to obtain limited types of records. But here the subpoenas would be seeking records relating to foreign intelligence and terrorism. The range of activities that relate foreign intelligence and terrorism is enormous and, therefore, there is virtually no limit to the type of records the FBI will be able to subpoena. The FBI will seek financial records, employment records, transportation records, medical records and yes, sometimes, library records. The collection of this massive array of records creates special problems. Inevitably, FBI investigations will sweep up sensitive information about innocent, law-abiding people. How do we assure this information is not abused? The FBI will also sweep up information about people who have nothing whatsoever to do with terrorism, but who may have committed other infractions, both minor and major. What will the FBI do with this information? These are not problems that arise with the ordinary use of administrative subpoenas.

There is a second crucial difference between the ordinary use of administrative subpoenas and the new proposal. In the proposed legislation, the FBI's subpoenas must be kept completely secret whenever the FBI says that national security requires non-disclosure. This means that a record holder who receives a subpoena that is overbroad or impinges on first amendment rights will not be able to complain to the press, Congress or the public.

This is not an insignificant disadvantage. Just last year, a federal prosecutor in Iowa served grand jury subpoenas on Drake University and members of the university community in connection with a peaceful antiwar forum. The university community protested loudly, the press took up the controversy, and the subpoenas were promptly withdrawn. This cannot happen when the subpoenas are secret.

If subpoenas covering a vast array of records are going to be served in secret, there must be additional safeguards. The most obvious safeguard is prior judicial approval, such as is provided, however inadequately, in Section 215 of the Patriot Act. We should not permit, for the first time in our history, the massive use of secret subpoenas that have not been approved by a judge.

I recognize that the proposed legislation provides record holders with the opportunity to challenge any subpoena in federal court. But this opportunity is no substitute for prior judicial approval. Third party record holders will generally have no incentive to undertake the burdens of a federal court challenge, and the secrecy provisions further reduce the likelihood of a challenge. If, for example, a hospital receives a subpoena for a massive number of medical records and the subpoena is made public, the medical staff and patient groups might pressure the hospital to file a challenge. There will be no such pressure with a secret subpoena. Thus, there will be little judicial supervision of the FBI's use of secret subpoenas.

The FBI should be required to obtain a court order when it seeks access to business records. As already noted, I believe the current standards for issuing such orders, as set forth in Section 215 of the Patriot Act, should be tightened along the lines suggested by the SAFE Act. But in any event there must be a requirement for judicial approval. Such a requirement imposes a salutary discipline on the government. It forces the government to think through and describe, in the words of Deputy Attorney General Corney, the "meaningful, logical connection between the record sought and the subject of the investigation." If the government believes that obtaining a court order is too slow in certain circumstances, it should propose special procedures for emergency situations.

In addition to the general unease about increased government collection of information, there are some highly specific concerns. Civil libertarians are worried that the government might misuse the information it gathers to attack and intimidate critics and opponents. The memory of J. Edgar Hoover's efforts to destroy the reputation of Martin Luther King lives on. And, just recently, there have been allegations that the White House leaked information about a CIA agent in order to punish her husband for criticizing certain policies of the Administration.

These privacy and civil liberties concerns deserve serious attention. But this morning I would like to focus on another concern—the danger that the government

will use the information it gathers and shares in ways that unfairly discriminate against Muslim Americans.

Although only a miniscule number of Muslim Americans are involved in any form of terrorism, it is obvious that the government's expanded information gathering and data-mining systems will focus on Muslim Americans. Even if such systems do not single out Muslims Americans by name or religious affiliation, Muslims will appear disproportionately on the government's computer screens because they are the people most likely (naturally and innocently) to visit, telephone and send money to places like Pakistan and Iraq. Inevitably, government officials will learn more about Muslim Americans than about other Americans. Many Americans, for example, employ undocumented workers in their homes and businesses. Many "harbor" out of status immigrants (often close relatives) by giving them a place to stay or finding them an apartment. Many do not fully report their earnings from tips to the IRS. But the Americans who will be caught doing these things, and subjected to prosecution, will disproportionately be Muslim.

Similarly, there are millions of persons in the U.S. who are violating the immigration laws. Their offenses range from illegal entry to failing to notify authorities of an address change. Again, Muslim violators will be caught and subjected to deportation in far greater percentages than other violators.

At first blush, there may seem to be no problem with prosecuting or deporting persons who have violated the law. But our nation's legal and moral values require equal application of the laws. When, for example, there are stretches of highway where virtually everyone exceeds the speed limit, it is not permissible for the police to stop and ticket only (or primarily) those speeders who are black. The new information gathering and data-mining systems will often deliberately focus on persons who are likely to be Muslims, and therefore it is necessary to address the unequal application of the laws that will inevitably follow.

I propose, therefore, that information gathered for anti-terrorist purposes not be used against individuals except in proceedings that directly relate to terrorism or to other violent crimes. Unless this restriction is imposed, criminal and immigration laws will be disproportionately applied against Muslim Americans. This unfairness will breed discontent in the Muslim community and undermine the fight against terrorism. It is important both that our country is seen by the world as fair to Muslim Americans and that it enlist the full cooperation of the American Muslim community in anti-terrorist efforts. These objectives can only be met if Muslims in this country believe the government is treating them fairly.

This proposal does not mean that anyone will be granted immunity for criminal activity or amnesty for immigration violations. The government remains free to bring criminal or immigration cases against Muslim Americans, provided that it does not use information generated by anti-terrorist data-mining systems in cases not involving terrorism or violent crime. This limitation will require some segregation of information and impose some burdens on the government. But these burdens are a small price to pay to ensure fairness to all Americans and strengthen the fight against terrorism.

Interestingly enough, the federal government is currently implementing a somewhat similar immunity program in accordance with the Homeland Security Act of 2002. Section 214 of the Act provides that companies such as nuclear power plants that voluntarily disclose to the government critical infrastructure information concerning their vulnerabilities to terrorism are guaranteed that the government will not use that information against them in any civil action. This is so even though the disclosed information may indicate that the company is not complying with various laws regulating safety or the environment and is thus subject to severe civil penalties. Congress made the determination in the Homeland Security Act that granting companies this limited use immunity served important national security interests. As I have argued, national security interests are also served by providing limited use immunity to people caught up in our anti-terrorism data-mining efforts.

Whether or not you agree with my analysis, I am sure you do agree that the government's increasing authority and capacity to gather information about Americans requires congressional attention. Recently, the President named his nominees and appointees to the new Privacy and Civil Liberties Oversight Board, and I hope the Board will soon address the questions I have raised this morning. But, in the end, it is up to Congress to assure that the government obtains the intelligence it needs without violating the civil liberties and civil rights of the American people. Thank you.

Mr. SIMMONS. Thank you very much.

I would like to make a comment and then I have a couple of questions, and my colleagues will all have questions as well.

It is my understanding from reading Mr. Jardines testimony that his recommendation is not unlike the recommendations that we had in the recent weapons of mass destruction report that there be somewhere in our government a center of excellence for open-source intelligence. In the case of the WMD report, it would be at the Central Intelligence Agency, but I think history has shown that they have not responded to that opportunity, at least in years past.

I guess my view is that such a center of excellence could reasonably be located with the Department of Homeland Security for several reasons. One, it could be incredibly useful in their infrastructure vulnerability reports because much of that information is publicly available from either state or local entities or private enterprises here in the United States.

But, secondly, by creating such a center of excellence, you develop expertise within the discipline and then those individuals who are expert in the discipline can be placed out in the intelligence community in all-source analysis facilities, just as a photo interpretation, for example, has a center of excellence at NPIC, signals intelligence has a center of excellence at the National Security Agency, and at various times in our history the clandestine service of the CIA has been a center of excellence for human-source intelligence.

So it seems to me that there is some value in that model.

But let me raise what I think is a fundamental question when it comes to open source. I have here aerial photographs of the Natanz Uranium Enrichment Facility in Iran. These are incredibly detailed photographs. Normally, you would not see these except in a classified environment. But in the case of these photographs, they were taken by the Space Imaging Organization, which is an open-source organization.

The value of these open-source products is that if there is an issue relative to Iran and its nuclear activities, you can share these photographs and you can share these images with the American people. So their government is not simply making statements and then saying, "Trust me, we have the secret information that shows this to be the case." You can actually show the American people what it is that concerns us around the world and possibly or potentially show the American people what concerns us here.

Dr. Gannon made a very interesting statement, that governments are losing control. In other words, governments are no longer the sole proprietors of information collection and analysis. And I think that is a good thing. I think that is good for democracy. I think that brings more people into the process, and I would be interested if any of our three witnesses would wish to comment on that analysis.

Mr. JARDINES. Well, I guess as a practitioner in the open-source arena and as someone who has been at the tail end, someone who has needed that open-source material and for most of my 10 years in the military, both on active duty and in the reserves, I was outside the Washington Beltway. In D.C., we have great resources at all levels of classification, but as you move out beyond that boundary, those resources dry up pretty quickly. And I think that the idea of setting up an OSINT center that would drive the acquisi-

tion of open-source information and centralize that is an important model.

In part, in the past, with the Community Open-Source Program Office, it was not successful primarily because it really was not viewed by the rest of the community as a community entity. The leadership and most of the infrastructure was the Foreign Broadcast Information Service, and it simply was not accepted as a communitywide effort.

Given that the Department of Homeland Security is a fairly new infrastructure entity within the intelligence community, I think a lot of those long-standing antagonisms between various intel agencies do not exist, and I think it would be far better received if an OSINT center were in the Department of Homeland Security.

Mr. ONEK. Let me just comment. In a related point, the chairman pointed out the importance of open-source information, and obviously people in a community, for example, have tremendous interest in information about, let's say, a nearby nuclear power plant or a nearby chemical plant, and they obviously are concerned with safety and environmental factors, and in general I think they deserve to know as much as possible in order to assess the safety of their neighbor, of their neighboring entity.

Now, of course, since 9/11, there has been concern that that same information, which is useful to the community, might also be useful to terrorists. So we have had to look more closely at it, and I am not suggesting that that is wrong but we have to make sure that we do not overdue it; that is, we do not overclassify and we do not make it impossible for people in the community who have an obvious need to understand facilities in their backyard do not get a chance to see information.

And so that is I think the dilemma that you face as you try to make more and more information or keep more and more information open source, but I do believe that it is a dilemma that we should meet head on and try to err whenever we can on the side of openness.

Dr. GANNON. I am just sort of speaking for the working analyst. If I were to take either the image you showed me or other imagery and actually take orthorectified imagery, which can be made into three-dimensional presentation, there is a capability really to have accuracy with regard to elevations and setbacks. For the homeland security purposes, we can do an urban area where actually you will have an accurate sense of actually how high things are, what the line of sight is, what the line of fire is.

Tremendous capability there, but in order to build those kinds of models, which are extremely useful not just to inform policymakers but also for operational reasons, the analyst today sits in a classified environment with superb imagery. You can take the classified information we have and put it in that to add to that model, but, invariably, the analyst is also forced to get a lot of unclassified information to finish it.

So my single point I want to keep making here is I think the intelligence world today is about integrating the classified and unclassified information into a superior product for the benefit of our country.

Mr. SIMMONS. Thank you very much.

Ms. Lofgren?

Ms. LOFGREN. Thank you.

I think, clearly, we are already making use of open-source information, but as I was listening to the testimony I was recalling the debate about 30 years ago about what should be collected by the government and what should not be, and there was a discussion at that time about whether police departments should be allowed to keep files that basically consisted of newspaper clippings. And I thought at the time, well, if it is in the newspaper, anybody can read it, what is the problem with that? And that was, I thought, a sound view.

But as technology has moved forward, the ability to compile and amass and integrate information has changed the whole dynamic of what can be found out about people, and I do not know that there is an obvious answer to that issue, but I think we need to spend some time sorting through that, because Americans really have a very strong sense of, "Leave me alone. My private life is my private life. I should have the right to that." That is a very American attitude, and I think it is that attitude that fuels objection to the Matrix Program and to other programs. So I think we need to think through how this open-source dilemma or opportunity meshes with that.

The issue of discrimination has been raised, and I think that is a serious one, and we need also to prospectively think about that.

And, finally, we need to think about the implications of collecting data that is out in the open, amassing it and then using it for a purpose that is not to protect Americans from terrorism but to prosecute in the criminal arena.

And if you think about Americans are starting to understand what is out there. Every time you buy something, there are cameras on every corner, there are cameras at every stop light, every time you go on your fast pass, there is information created. I mean, ID tags are going to connect where you go and what you buy. It is all out there in the open to the point where you could know what every American is doing most of the time. You add that in with the satellite imagery that is available. I mean, Google now has a program where you can really see what is going on place by place.

And the question I have really for each of the witnesses is, what recommendations do each of you have for how we might put procedures in place that would be respectful to the privacy expectations of Americans, what procedures we might consider to avoid the discriminatory impact from the compilation and amassing of this information and also what procedures should we consider putting in place that would avoid whatever intrusions exist being used for a more mundane purpose as opposed to protect the nation from terrorism purpose, really to avoid handing on a platter to a police department for a garden variety criminal prosecution?

I wonder if you have thoughts, each of you, on those questions.

Mr. ONEK. Well, I certainly have some thoughts, which I gave. I really think that when you look at it there are really two ways. One is, are there going to be or should there be certain limitations on the collection side, on the front end? And that I think is what the current debate about section 215 of the Patriot Act or the I think forthcoming debate about administrative subpoenas is about.

What can you collect? How do you make sure that the government is not engaging in fishing expeditions and so on?

And then there is, I guess, what I was trying to speak about earlier, the backend. After you have collected the information, after you have determined that certain information should be collected and you have collected it, are there any protections you can put on it? First of all, can you make sure, and this is more mundane but important, can you make sure that only the right people have access to it within the government? And there, there are technological fixes, including audit trails and so on which can make sure that unauthorized people for their own purposes do not get access to the information. And that I think we can do, and that is probably not controversial.

Then you get to the more difficult issue is how do you assure that the information is not misused, that it is not misused, for example, by governments to attack political opponents, as in the days of J. Edgar Hoover and Martin Luther King, or that it is not used in a way that, although maybe people do not intend it, ends up being like selective enforcement or discriminatory. And I think we do have to, and which is the reason I did raise it this morning, I do think we have to begin to think about that last issue.

I think it is very hard to do, frankly, and I have talking to law enforcement people. I am not suggesting it is easy, but I do think it is necessary to try to do if we are going to be true to our values and if we are going to show in good faith to Muslim Americans here and to the world that we are trying to differentiate between terrorists and Muslims, and that was the point of my oral testimony today.

Ms. LOFGREN. I know time is short but if Dr. Gannon or Mr. Jardines have comments, I would—

Dr. GANNON. I have a quick comment. I started my intelligence career in 1997 in the shadow of the Church-Pike hearings, and I was instructed very clearly that information from any source, open or clandestine, that dealt with U.S. citizens we did not deal with it. There were very clear policies about reporting on and analysis of issues involving U.S. citizens, and it was not just a matter of clear policies. I believe I was held accountable for those polices, and I also believed that my bosses, my leaders were being held accountable for them.

So the point I would make to you in terms of recommendations, I think this does have to become a leadership and accountability issue that is distributed throughout the intelligence business and, again, not just isolated in some unit that is deemed to have the responsibility for this. I think it really does have to—it is like security itself: The protection of U.S. citizens and information involving them has to be the business of every analyst and every collector in the business. And I think that can be done, I think it was done throughout my career.

Mr. JARDINES. If I could just add a couple comments here. I would like to clarify what we are talking about. Open-source intelligence is defined as publicly available information. I keep hearing collection from my colleague. Open sources are not collected, they are acquired, which means someone else collects the information,

edits that information and disseminates. The intelligence community is merely a secondhand user of that information.

So when the congresswoman was mentioning traffic cameras and those kind of things, all of those fall outside the scope of open-source intelligence. Gaining access to those kinds of cameras or credit reports that would go through the traditional—

Ms. LOFGREN. Right, but if I could clarify my point, that aggregation and distribution, because of technology, is already occurring. And so we are at a point where if we set policies, we can actually have a very large impact. Google is in my district and the googlization of the world is occurring. We are just at the beginning really of where we are going to be, and the opportunity to set a framework for how we are going to respect the privacy rights of Americans is unique, and we ought not to pass it by.

And I appreciate the gentleman and the chairman's indulgence for my being over time.

Mr. SIMMONS. Absolutely. And thank you for the questions.

The Chair now recognizes the distinguished chairman of the full committee, Mr. Cox.

Mr. COX. Thank you, Mr. Chairman.

I want to focus on the findings and recommendations of the Silberman-Robb Commission, the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. This is a big, fat report that has been available to us in open source only since March 31, two and a half months, and I am very, very pleased we have the opportunity in this subcommittee to dive into a piece of it.

The Silberman-Robb Commission recommended the creation of an open-source directorate within the CIA.

Dr. Gannon, you in your testimony disagree with that recommendation. My first question to you is, why? Should there be an open-source directorate somewhere else at DHS or is this an inherently bad idea?

Dr. GANNON. Well, I think, in my view, we have a functional problem; that is, that analysts are not using open source enough, and we, once again, want a structural solution to a functional problem.

So my view is that all analysts, all-source analysts or imagery analysts or signal analysts, they are all now in a position where they need open-source information to interpret their own collection contributions. And then analysts, the all-source analysts, need all-source information more than ever in order to produce the best analysis that they can.

So it has to be, in my judgment, a distributed model that gets the technologies out to all those analysts so that they can avail themselves of the best information, and creating any kind of a center which is deemed to be the all-source center is concentrating, not distributing. So I think there is a danger that you would be creating structure there that in fact would impede the kind of integration of classified and unclassified information that I think is absolutely essential and I think is the trend in the community today.

Mr. COX. The Silberman-Robb Commission said, "We believe part of the problem is analyst resistance; in other words, the analysts do not want to use open-source information. We believe that part

of the problem is analyst resistance, not lack of collection." And so another of their recommendations was that we, the United States government, and specifically the CIA, train some of the new analysts specifically in the uses of open sources and then, in the parlance of the report, they would be evange-analysts and go out and encourage other people to get with it and use new technologies and so on.

This, they believe, would also address another problem, a more fundamental problem, and that is the intelligence communities, and here they are not speaking just of the CIA, surprisingly poor feel for cultural and political issues in the countries that concern policymakers most. So they see open source as one means of getting people culturated in the target areas of their investigation.

Do you agree, Dr. Gannon, with those two assessments: First, that there is analyst resistance to using open-source information, and, second, that there is a pervasive problem in the intelligence community in the form of a lack of feel for cultural and political issues in the countries that policymakers are concerned about?

Dr. GANNON. I think the commission did a superb job in its investigation side. I think some of the recommendations, in this one especially, I think the commission is going to end up being human like the rest of us, making an effort to improve the situation but I do not think recognizing adequately the baseline in the community right now. I think it is a mixed bag.

All of the analytic programs in the intelligence community are actually embedded in collection-dominated organizations. So both the collection perspective, the clandestine collection perspective, and the security environment does create, I think, impedance to the aggressive use of open-source information. So there are some structural issues there to deal with.

But in fact there are many models. I cited the geospatial imagery, but I did distribute a copy of the Global Trends 2015 exercise where for 18 months our analysts dealt with outside experts where they asked the question, what are the threats going to be to the United States, where is the best information and best expertise to deal with it. And they integrated that over an 18-month period into the report that is before you.

So I think there are some best business practices for the use of open source.

But, again, my point is, I want to change the behavior of those analysts, not change structures. And to change the behavior I think you have to impose on leadership the responsibility to get them the technology that will access open-source information and enable those analysts also through leadership to get out of the community so they can speak with folks outside.

I will cite one case when I was chairman of the National Intelligence Council where we did an estimate on Iran and we were trying to deal with the political turmoil in Iran, and when I got the draft before me I realized that we did not have a single analyst in that intelligence community that had ever been to Iran.

So what do you do about this? I do not think an open-source directorate was going to help me there. What we did was we asked the question, who is in Iran? Who does know the ground truth there. And we worked with allies and broke tradition and actually

brought some allies to work with us to stimulate the kind of debate you need with regard to the change that was taking place there.

So those kinds of things are happening, but my point is, I want systems and leadership that is going to drive those analysts to change their behavior so they do use open source more, and I do not see how the structure of an open-source directorate does that.

Mr. COX. Mr. Chairman, my time has expired.

Mr. SIMMONS. Thank you, Mr. Cox.

The Chair now recognizes the distinguished Ranking Member of the full committee, Mr. Thompson.

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

I was trying to get some information. I am glad you said that, Dr. Gannon.

There was an AP story yesterday that one of the heads of the Counterterrorism Department at the FBI said that you really did not have to have any experience in terrorism or anything to run the Department, and I am glad to see somebody at your level that would say that you absolutely have to have that kind of experience if you really want to get a good product. And I was just trying to make sure we get that in the record, because some of us disagree with that statement.

Mr. Onek, for the last 6 months, there have been security breaches in a lot of commercial databases—ChoicePoint, LexisNexis, Time-Warner, CitiGroup and over the weekend MasterCard—where personal information of hundreds of thousands of Americans have been compromised.

Should we be concerned that some of this open source, if not properly safeguarded, can cause a threat to us as a country?

Mr. ONEK. Well, I think that what you are talking about raises a somewhat different concern, because you are talking about information that is in the hands of commercial entities and not in the hands of government, and I think there are different sets of problems. I think the major concern with the information that is in the private hands are things like identity theft and the problems that that pose. And, obviously, that is a very different concern than the concern you have when information is in the hands of government.

ChoicePoint cannot prosecute you, it cannot deport you. It can, I suppose, defame you if it wanted, but it usually does not have any motive to do it because it is a profit-making not a political or partisan entity. So I do not wish to make light about the problems that have just been revealed about the lack of security, because I know the problems that they can cause for individuals, and it can happen to any of us at any moment, but I do think that the issue of government information is a different issue and I think ultimately a more serious issue.

Mr. THOMPSON. Well, Mr. Jardines, you are one of those private folk who gather information that sometimes can, for whatever reason, become compromised. What safeguards have you as a profession instituted so that this information you gather is not falling into the hands of potential terrorists or what have you?

Mr. JARDINES. In general, I cannot speak for the overall industry but in terms of what we at Open Source Publishing do, we maintain systems with robust security features. Our focus is primarily

foreign intelligence issues, so we do not focus that much on U.S. persons information. But it certainly is a real issue.

As someone who knows just how much information is publicly available out there, it scares me to death what is out there, but the reality is this is something that if it is truly open-source information, what we do is the same thing that any member of the general public could do.

Does it bother me that you can go to Google and type in my telephone number and pull up my address and a map to my house and a picture of my house? Yes, it does. Is there anything I can do about that? I do not think so. If the committee would like to do something about that, that would be wonderful.

But at this point, I feel like we are arguing—it is the same as arguing, "Gee, the roads are publicly available and there is the threat of some level of abuse by the fire and police departments, so therefore we need to regulate how the fire and police departments drive their vehicles on our public roads. The reality is the information is already out there. It is not being collected by the government; it is already out there.

And so while I certainly, as an Hispanic, am very, very sensitive to the issue of profiling, there are steps in place and if we need to add some sort of civilian oversight board, then that is great. But my biggest concern is for that police chief or that fire chief who has to respond to these kind of events should have some degree of foreknowledge about what the possible risks are to him, and at this point we have decided, well, we cannot give him a clearance so let's just ignore him completely.

Mr. THOMPSON. Thank you, Mr. Chairman.

Mr. SIMMONS. Thank you, Mr. Thompson.

The Chair now recognizes the gentleman from California, Mr. Lungren.

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

I have got to take some of my time responding to some of the bankshot criticism of section 215, which of course is not the subject of this hearing but there has been some things said on the record that at least I have to respond to.

Let's at least make clear what we are talking about in section 215 of the Patriot Act. It requires a federal judge to find that the requested records are sought for. That is the relevancy standard. For an authorized investigation to obtain foreign intelligence information not concerning a United States person or protect against international terrorism or clandestine intelligence activities. Some of us believe this involves greater judicial oversight than a grand jury subpoena where a grand jury subpoena is typically issued without any prior involvement by a judge.

Section 215 orders are also subject to greater congressional oversight than our grand jury subpoenas. Statutorily, every 6 months, the AG must fully inform the House and Senate Intelligence Committees concerning all requests for the production of tangible things, whether from library or anyplace else. There is no comparable provision for the oversight of grand jury subpoenas.

I am also informed that another section of the law requires informing the Judiciary Committees of the House and the Senate. There is also specific language in section 215 which provides that

an investigation under this section shall "not be conducted of a United States person solely on the basis of activities protected by the First Amendment to the Constitution of the United States."

I bring this up only because I keep hearing a recitation of criticism of section 215, and we ought to at least know what it is we are talking about, and, unfortunately, that is not the subject of this hearing and we do not have the time to go into it, but I needed to take some of my 5 minutes to at least put that on the record.

This is serious business, I know we all understand that, but it also shows that the proper regulation against abuses is the oversight by the Congress. That is why the statute is set up. The Judiciary Committee has had 12 hearings thus far. We have submitted hundreds of questions, written questions, to which we have received responses from the Justice Department.

And in the area of collection or utilization of open-source documents, as in anything else, the proper place to make sure it is not abuse is right here, the Congress. That is why some of us think that the oversight that we are conducting is appropriate, necessary and ought to be even more robust than it has been in the past.

I would like now to ask a question of Dr. Gannon. This goes to the question of changing the culture and so forth. Intelligence communities are somewhat insular, you admit. It is difficult to change that culture. And what I would like to know is whether or not when going to open-source data, do we need to ensure that there is a possible governmental/private partnership? That is, will we run the risk that when we look to open sourcing that the intelligence community is going to create its own matrix, its own way of getting it, rather than take advantage of those private sector operations that are already out there mining this information?

And are these private organizations—private industry, academic institutions, and so forth—sufficiently capable of processing that open-source information in such a way that they can give it to the intelligence community so those analysts can do their work?

Dr. GANNON. I do think reliance on those organizations is inadequate for the intelligence community. I think that the system works best when there is a real partnership, just as you are suggesting, between the analyst dealing with the classified world and then the open-source world where they tackle a problem together so that they are developing analysis that is continuously integrating the classified with the unclassified.

And I will assert, in my four years as chairman of the National Intelligence Council, their willingness to disposition of outside sources of expertise, and this means everybody from Wall Street to the aerospace industry to work with the intelligence community has never been more positive.

I was never turned down by anyone, and usually the reason I asked them was that we sat down and said, "Who has got the best answer to this question?" Even on something like the annual report on the ballistic missile threat, we discovered that while a lot of that did rely on clandestine collections, in fact we could not do some of the technical analysis without going to the aerospace industry, and some of the economic analysis we needed to go to academia.

So when we went out with a problem to the outside, we were able to develop the kind of partnerships. And when you work with

them, as we did in Global 2015 over 18 months, you develop sustainable kinds of partnerships.

I think the outside world there is a distrust of the intelligence community that can be broken down if you actually are able to show your partners the results of what you are doing. There is always a suspicion that when we ask for information the door slams and they never understand how it is used. And the private sector does not like to provide information on that basis. I think the community has to recognize we are in a new environment and we do have to have policies that allow us to share in a back and forth manner more than we have.

Clearly, it is a partnership, but I think it is a partnership that begins at the very beginning of tackling serious national security issues. It is not something where you do yours and they do theirs and then you join at some place down the road.

Mr. SIMMONS. I thank the gentleman.

The Chair now recognizes Mr. Etheridge.

Mr. ETHERIDGE. Thank you, Mr. Chairman.

Gentlemen, thank you for being here.

As we talk about open-source gathering data, I think you heard from the committee the concerns as we gather that data really is in the minds of the public what we gather, from what sources, and certainly there is a risk environment out there today with all the sources we can pull it in from, especially as we look at open source.

My question for each of you, as we look at the blurring of the line, especially when you are looking at open source versus the investigation of law enforcement, Mr. Onek you raised the issue of intelligence investigation, which does not have the same constraints, of course, as the legal law enforcement.

And, Dr. Gannon, you touched on the issue that the CIA outside the United States if American citizens happens to be involved, that is off base.

My question would be, as we view this, the issue of mining data. Basically, as you start to pull it in, and we have alluded to the fact that we may have to have constraints, talk a little bit more about this. Because as you start to pull in open source versus the other, eventually you get to the point where it gets blended, and then you have got the real problem of trying to separate what is what as it relates to moving forward and moving this data.

And I think this is where the American people really have some concerns, but at the same time we want to make sure we have the right data as it relates to protecting the American people from terrorism.

Mr. JARDINES. Well, the intelligence community already has a number of constraints on it with regard to open-source information. One item I would say is, unfortunately, we are not blending open-source information with the all-source analysis process. The Silberman-Robb Commission mentioned that analysts were resistant to use open-source information. What the Commission did not mention was that is because the community has made every effort to make it very difficult for them to get access to it.

One of the three-letter agencies here in Washington, D.C. does not have Internet access for each analyst. That to me is a mind-blowing concept that we do not have that. Likewise, we do not even

put unclassified data up on the classified networks in many cases because we are told, "Well, the classified networks are for classified information." Yet, that is the analysts' operating environment.

But I think there are constraints in place. I am not extremely familiar with the Department of Homeland Security's intelligence infrastructure, but they exist, and if those need to be looked at more carefully, I am certainly open to that.

Mr. ETHERIDGE. But then how do we get the open source available for use then?

Mr. JARDINES. In part, I think, as Dr. Gannon mentioned, making open-source resources available to the analysts.

Where I would disagree with Dr. Gannon is in that I think we need an organization to provide that open-source information to the analyst. Sure, analysts can go out and do their own, but to say we do not need an organization to provide some level of vetted, analyzed open-source information is like saying all analysts should collect their own SIGINT or their own imagery intelligence. No one would recommend that because all-source analysts do not know how to do SIGINT, and they do not know how to do IMINT.

The reality is if all-source analysts have the time and the expertise to do effective open-source exploitation, I would be standing in the unemployment line right now.

Dr. GANNON. Mr. Jardines is right that I have been using open source more generically to really mean any information that is not classified, not simply information that you can get from the Internet. So, clearly, I am including in it information that through whatever means the government can get it, whether it is a subpoena or whatever, is non-classified information.

So, for example, the records of my credit card purchases and so on and so forth. So I obviously have been talking here in a somewhat broader context, and I agree that there are certainly constraints on it. I think Congress is wrestling with it. It is wrestling, as Mr. Lungren pointed out, with the 215 issue. I think there has been oversight, and really all I was trying to do is raise some issues that I think have not yet been looked at and to say that we are going to have to keep doing it.

In a way, and I will stop in a second, my testimony presupposes the success of this committee and the government in assuring effective use of open source. I am sort of at the next stage. I am assuming you have succeeded, as I hope you will, and you have government officials who do have the ability to get their hands on this information, and I am saying, "Okay, what protections do we need," because after all we all want them to be successful. Then when they are successful, what problems does it raise.

Mr. ETHERIDGE. Thank you, Mr. Chairman. I see my time has expired. Thank you.

Mr. SIMMONS. Thank you.

The Chair now recognizes Mr. Dent.

Mr. DENT. Thank you, Mr. Chairman.

My question to Dr. Gannon, how much danger is there that having the government communicate information uses open sources that it could reveal or perhaps or confirm the existence of classified information? Would the government be seen as confirming that classified information?

Dr. GANNON. I think this has been an occupational hazard and timely memorial on the intelligence business, but it is an eminently manageable problem. I think we, for example—I recall the Congress told us that we needed to produce a declassified version of the ballistic missile report, and I would say 80 percent of that was produced from clandestine sources. The community protested that it could not do it, Congress said, "You will do it." We did it, and I would say probably 80 percent of the analysis was actually derived from clandestine sources could be declassified.

My point to you is, I do not think this is as big a problem as you suggest. I think in dealing with the kind of hardship everybody was talking about, there is a benefit on both sides, that people who come from the outside who work with the intelligence community will assume that as we work a problem together, if there is classified information that would totally contradict a trend or a path that is your taking, the intelligence analyst would stop it.

On the other hand, the intelligence analysts are benefiting tremendously from that outside infusion of expertise.

But I think this is a manageable problem, and I think leadership within the intelligence and the policy community at times have been particularly sensitive about particular issues, and they have halted communication. But for the most part, I do not see this as a problem that is particularly worrisome.

Mr. DENT. Thank you.

Mr. Jardines, a few moments ago that you mentioned that you were frightened about some of the information you see in open sources. Specifically, what type of open source information frightens you the most and why?

Mr. JARDINES. There are a number of things that one would consider generally innocuous. For example, the newspaper, when you buy a house, publishes the fact of who bought the house and where it is located and how much it costs. I can take that information and then pull up additional information regarding tax assessment. I can get a sense of how big the house is. Once I have the lot number, I can go down to town hall and get the building permits, I can get copies of closing documents, which in many cases contain information about mortgages and what not, and we begin to put together information that someone who really wanted to spend the time and energy to figure that out or may want to do harm to you would have a fair amount of information available.

Unfortunately, it is already out there. I cannot make the newspaper pull it back, but that is the world we live in. I do not like it, but there is going to be this level and much more coming, and I do not see that that is going to change. We have instance access to information and the ability to aggregate it.

Mr. DENT. Are you or any of the panelists suggesting that there are any special privacy issues with the government distributing open-source information then? If that frightens you, should the government be judicious in how we disseminate that type of open-source information?

Mr. JARDINES. I think the fact that you are disseminating it, in my hope, we would be disseminating it down to a very diffuse level, down to local police departments. I do not see that that is going to be an issue, because someone would think, "Gee, if I am going

to release this publicly, perhaps I should think about does this betray sources and methods, are we establishing a pattern here that talks about what we may be interested in?" And, obviously, if there is some libelous information and what not, it is subject to public scrutiny. That is the thing about open source is we cannot hide it, it is unclassified.

Mr. DENT. I see my time has expired. I was going to ask you to talk about the accuracy of this open-source information, but I guess I will have to leave that to one of the other questioners.

Mr. SIMMONS. I thank the gentleman.

The Chair now recognizes the gentleman from Rhode Island, Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman.

Gentlemen, thank you for your testimony and for being here today.

I guess I have a couple of questions. First, I would start out with I am a big believer that we need to use open-source intelligence more aggressively than what we have been on a very broad scale. And I am cognizant about, especially I am reading a book right now by our colleague, Mr. Weldon, who is very critical of our intelligence community and its failure to use open-source intelligence more aggressively.

But I am also a believer that we should not be duplicating efforts. I think in government all too often we pass measures that are duplicative and not necessarily coordinating in nature. We do that as a feel-good measure and think we have fixed the problem and we have not necessarily done that.

So my question is with respect to creating a new open-source intelligence directorate, how would that be different from the work done by, for example, the National Intelligence Council? You can help educate me and the committee with how that would be complementary or duplicative if we were to do that.

The other question that I have is, what role, if any, should the DNI play in coordinating the collection, analysis, production, dissemination of open-source intelligence? And what steps we should be taking in general to get the intelligence officers and analysts to use open-source intelligence resources more aggressively than they have in the past?

If you could take those, I would be interested in hearing your response.

Dr. GANNON. Well, I will start and you can help me by repeating your first question. I think the DNI has a critical role to play here. I think the DNI has—and I think we ought to give him the time. I think to interpret so many of the recommendations that have been made so that he can make the best judgments about how to proceed within the community.

With regard to open-source information, I think he will have a deputy for open-source information, and it will be his responsibility to deal with dissemination issues and also deal with some of the privacy issues that have been expressed here. Because I think the issue on open source is not that we want to in any way impede the dissemination of open-source information. We want to certainly manage the way that it is used in the production of intelligence

products, the way it is interpreted and particularly if it deals with U.S. citizens.

I think there can be policies in place that will instruct analysts and hold them accountable for the way they use open-source information. But I think the basic goal that I think John Negroponte will adopt is to encourage much more actively the use of open-source information to both put the systems in place, technology, the policies in place that will encourage that and then to hold his leaders accountable.

And I think the test John Negroponte would want to apply with regard to any product that is produced in the intelligence community is not whether it may be right or wrong but did it avail itself of the best information available from all sources before we presented this intelligence to the President or his national security team?

Mr. LANGEVIN. If you do not have a separate open-source intelligence directorate somewhere, whether it is within DHS or under the DNI, how do you, in a sense, compare or test that collection or that analysis of data?

Dr. GANNON. Well, I think there is a management structure dealing with the analysts in every one of the agencies of the intelligence community. I think they can be held accountable for the proper use and training in open-source areas. I think the risk of having an open-source directorate is that there is the impression that we have now centralized this priority or this function within a directorate where it really does need to be distributed and imposed as a responsibility through the analytic community.

And I think there is a manager in the community now that it is recognized that we are not where we need to be on open source, and some of those managers, by the way, are dealing with problems with security and other sort of institutional resistance that is not just the analyst, it is embedding of these programs and sensitive collection-dominated organizations. So there is no analytic community that is organized apart from the collections community.

So I think, again, on any intelligence product, again, I would not ask the question, is it right or is it wrong or 6 months later I would not ask, was it right or wrong, I would ask, did it use the best information available from all sources, including open source? And that is an easy test because you could find the information that might have been better with regard to any particular issue.

Mr. LANGEVIN. Any members of the panel want to comment on that? And also getting to the question of how would the work of an open-source intelligence directorate be different from the work of, for example, the National Intelligence Council?

Dr. GANNON. I think they are completely different functions, actually. The National Intelligence Council is a group of a dozen or so senior experts where it focuses first on expertise. A design goes back Director Colby back in 1973 when he established the System of National Intelligence Officers. What he wanted is prominent experts that could speak to him about issues that should matter for U.S. national security and then for him to the intelligence community so that they could drive the analytic priorities and the estimate of work that they did.

I do think the open-source directorate is about being at the kind of leading edge of the technologies and methodologies for the use of open source and imparting that to the analytic community. It is not there to do substantive products. It is more with a resource and a technical know-how kind of organization.

Mr. SIMMONS. The Chair now recognizes the gentleman from Pennsylvania, Mr. Weldon.

Mr. WELDON. Thank you, Mr. Chairman, for holding this hearing, a very important hearing.

And thank each of you for testifying.

I want to walk my colleagues through a case study that I think is very appropriate for this hearing, and I want to take my colleagues back to 1999. I was then Chairman of the Defense Research Subcommittee. We were standing up information dominance centers for each of the services, and the information dominant center of the Army, called the LIWA, the Land Information Warfare Assessment Center, was headquartered at Fort Belvoir. They were also linked with SOCOM down in Florida, which was doing amazing work and using the same model that the Army was using. They were bringing together disparate systems of classified data, including open-source data, which the CIA was not using at that time, to understand emerging transnational threats.

John Hamre was the Deputy Secretary of Defense, and I asked him to go down and look at this capability because I was increasing the funding for it and he did, and he said, "You are right, Congressman."

We put together a brief, a nine-page briefing, which I would like to enter into the record.

Mr. SIMMONS. Without objection, so ordered.

Mr. WELDON. This brief in 1999 called for the creation of a national operations and analysis hub, the policymakers tool for acting against emerging transnational threats and dangers to U.S. national security. And the concept was to bring together 33 classified systems managed by 15 agencies, including open-source data to do massive data mining and using tools like Starlight and Spires and other cutting-edge software technologies to be able to give us the kind of information to understand emerging threats.

John Hamre said, "I agree with you, Congressman, and I will pay the bill. The Defense Department will foot the bill for this, and I do not care where the administration wants to put it, at the White House, the NSC, wherever, but you have got to convince the FBI and the CIA because they have a large part of this data."

So at John Hamre's suggestion, on November 4 of 1999, almost 2 years before 9/11, we had a meeting with the Deputy Directors of all 3 agencies. I went over the brief, and the CIA said, "Well, Congressman, that is great, but we do not need that capability. We are doing something called CI–21, and we feel we have enough capability and we do not need that extra capability that you are talking about.

Well, at the time, the Army and SOCOM, passed by General Shelton and General Schoomaker, who was Commander of SOCOM, were doing a classified program called, "Able Danger," which has not yet been discussed in the open, and I do not know why the 9/11 Commission did not go into it, because Able Danger

was focused on al-Qa'ida. Able Danger was a classified project of SOCOM and our Army looking at the cells of al-Qa'ida worldwide so that we would have actionable information to take out those cells.

What I did not realize was that they had actually produced a chart until 2 weeks after 9/11.

Now, Mike, unfold the chart.

This chart was taken by me in a smaller form to Steve Hadley 2 weeks after 9/11. Now, it is difficult for my colleagues to see even though I have had it blown up.

Hold it up, Mike.

This chart identifies the major al-Qa'ida cells, and if you look to the chart in the center to the left, there is the picture of Mohammad Atta. What the military did in 1999 and 2000 through the use of open-source data, and this is not classified what I am showing you, they identified the Mohammad Atta cell in New York and identified two of the other three terrorists.

What I have since learned, and I have two—Mr. Chairman, if we want to do a classified hearing on this, I have two military personnel who will come in and testify who were involved with this. But SOCOM made a recommendation to bring the FBI in and take out the Mohammad Atta cell. And the lawyers, I guess within SOCOM or within DOD, said, "You cannot touch Mohammad Atta, because he is here on a green card, as are the other two suspected terrorists. And they were also concerned about the fallout from WACO.

So now we have obtained through an open-source capability that the CIA did not want to pursue, "We do not need that." When I took this chart to Steve Hadley and opened it up in the White House he said to me, "Congressman, where did you get this chart from?" I said I got it from the military, special forces command of that Army.

This is what I have been telling you we need to fuse together our classified systems. And Steve Hadley, the Deputy to the National Security Advisor, said, "I have got to show this to the man." I said, "The man?" He said, "The President of the United States." I said, "You mean you do not have this kind of capability?" He said, "Absolutely not, Congressman."

So he took the chart and he gave it to the President of the United States.

In 2003, George Bush announced the TTIC, the Terrorism Threat Integration Center. The TTIC is identical to what we proposed in 1999 but the CIA told us, "Trust us. We know better. We know how to do this kind of capability. We know how to do this emerging threat." They did not produce that chart. It was done by military capabilities to the Army's Information Dominant Center and through special forces command, tasked by General Shelton and General Schoomaker.

Now, to add further insult to injury, bring out the next chart. This is the capability that is now available but I have been told it is not capable of being produced through the NCTC, the National Counterterrorism Center.

This is al-Qa'ida today worldwide. Every one of those little dots is a person or a cell, and every one of them are identified. This is

a worldwide global depiction of where al-Qa'ida is today, the key cells that are threatening us, their linkages to other nations, their linkages to terrorist attacks. This information is all obtained through open-source information. I have been told by the military liaison to the NCTC that the NCTC could not produce this today.

Mr. Chairman, this is something that this subcommittee has to pursue is I have been told that at the NCTC we have three separate distinct entities and the stovepipes are still there. For the life of me I cannot understand why there is resistance among the people who are paid to do our intelligence to fuse together information to give us a better understanding of emerging threats. This comprehensive capability is now being pursued by naval intelligence under a new task force that I hope will be picked up by John Negroponte who I gave a brief to 2 weeks ago.

Open-source intelligence has been extremely valuable and can be extremely valuable. I am not convinced yet that we are there.

Mr. SIMMONS. I thank the gentleman for his statement. I would request by unanimous consent that both charts be entered into the record of this hearing, and I would be happy to consult with the ranking members or members to have a follow-on discussion in closed session of this issue.

Do any of the members wish to respond or shall we go to the last member, the distinguished gentlelady from California, Ms. Harman?

I apologize. Ms. Sanchez?

Ms. SANCHEZ. Thank you, Mr. Chairman.

Mr. SIMMONS. I did not see you around the corner there.

Ms. SANCHEZ. I know. These chairs get lower every week. I do not know why. Someone is playing a game on us or something.

I actually have some questions. The first one will be to our former majority head staff to the committee, and, John, I just want you to know that at least I miss you. You have had a chance now to be on that side, you have had a chance to be on the inside during a very formative time here in particular with respect to this committee, and there have been a lot of things that we have done since 9/11 with respect to intelligence or just trying to get our arms around this whole issue of intelligence, including what we did making the directorate have some responsibility for open-source information.

With what you know—I am sort of trying to pick your brain—with what you know, because when I look at what we thought we were doing after 9/11 with respect to homeland security, one, get intelligence, not making new intelligence but getting intelligence that exists and sort of coordinate it in a real-time fashion so we could thwart a terrorist action; the second thing, of course, trying to figure out how we put limited resources to fortifying those things which are important to our critical infrastructure; and, third, how do we respond if in fact an attack comes through?

I want to get back to the first one, this whole issue of intelligence. I guess I would ask you, what do you think is the Department of Homeland Security's real niche in trying to figure out this whole issue of intelligence, given that now we have the intelligence czar position, et cetera. What do you think we should be looking at when we oversee the Department's look at intelligence?

Dr. GANNON. First of all, I would say that from my perspective, having been on the Hill and the White House and the intelligence community, I think a lot of the actions taken after 9/11 were reactive kind of actions to improve our capability to stop a terrorist attack. And I think if you look at what we did on the foreign side by going after the terrorists where they were and what we tried to do domestically, we certainly did I think do a lot of damage to terrorist infrastructures abroad. We did certainly raise the costs of doing business for terrorists with what we did domestically. And we have not had a terrorist attack. So I think we can perhaps take some comfort in that.

But I also think that both with regard to the Department of Homeland Security or the homeland security issue at large and intelligence, I think in either case we really developed a strategy, a kind of focused and resource-responsible strategy that will sort of protect us long into the future.

And I think now with the appointment of John Negroponte and with Mike Chertoff in the Department, I think there is a real opportunity now to stand back and say, "Look at all the things we have done. A lot of them did not turn out the way we thought we would."

I think within the intelligence I think we have had—I think our intention was to strengthen analytic capability, but in some cases I think we have stretched analytic resources to a point where I think we should take account of that fact. I think we have tried to streamline and to integrate accountability when in fact we have in many ways divided it. And I think as I have moved around the intelligence community, we have perhaps created so many new analytic units, that we are doing a lot more production than we are analysis. But I think that is all correctable.

But I do think we should be now looking at, you said, a baselining of what we have done thus far and working together to translate this into strategy. And I would also emphasize from my experience I think it is critically important for the intelligence community of the executive branch and the Congress really to work together so that we are sort of working the same agenda, because there are all sorts of things that we can say are wrong.

The question is, how do we want to measure success for John Negroponte over the next year or two? I think that really does depend on having a consensus on what are the priorities of things for us to do.

And, really, the priorities are not about massive new structures and costly new programs, it is about fixing human intelligence, which has been a problem we have known for some time. That means getting the resources into the field and into strategic kinds of planning of human programs. Rebuilding the analytic capability, again, is something that does not depend on structure, it depends on putting resources there.

So there are a number of issues that—there are really probably four or five issues that I would want—community training is another one. I think this has been an issue for some time where we can clearly do integrated training that would be to the benefit of the intelligence community.

So I would like us to give John Negroponte the time and really work with him and show confidence in him and Mike Hayden and their teams so that we can sort of admit that we have not done everything right in recent years. We do want to get it in a strategic direction, but there really cannot be a strategy that will succeed unless it has the support of the White House, the intelligence community leadership and the Congress.

So my answer to the Department of Homeland Security is I continue to believe, as I have all along, that if you have a Secretary of Homeland Security with the responsibilities that this one has and has under the Homeland Security Act and I suspect will continue to have for protecting America, first of all, preventing terrorism against the homeland, for protecting our critical infrastructure and for the quality of response that we have to a terrorist attack, that requires significant sustained intelligence support.

So he has got to have at the end of the day, however we change the Homeland Security Act or however we narrow down or focus in what has to be I think a real assessment of what roles and responsibilities need to be across all these agencies, I think you have got to have a strong intelligence capability for this Secretary.

Ms. SANCHEZ. Thank you, Doctor. And I see my time is up.

I just want to say to Mr. Onek that I had a question about some of your concerns, and I will submit them for the record, because I am very interested in your ideas on the impact to the Muslim community in particular.

Mr. ONEK. Thank you.

Mr. SIMMONS. The Chair thanks the gentlelady and now recognizes the distinguished Ranking Member of the House Intelligence Committee, Ms. Harman, from California.

Ms. HARMAN. Thank you, Mr. Chairman. I want to say first that I think you and the Ranking Member, Ms. Lofgren, bring enormous experience and skill to this subcommittee's activities. I am proud to serve on it.

And to our witnesses, whom I have known for many, many years, you all, but especially Dr. Gannon and Mr. Onek, have been there for the key fight, and you are resources that I hope not just we but those who lead our intelligence community will continue to call on. It is a pleasure to listen to you and to learn from you.

Time is short, and I personally have to walk out of the door in about 3 minutes, so I just want to make a couple of observations. First, John Gannon just commented on the question I would have asked, which is how to measure success. I think that is a critical question. Joe Onek put a useful metric before us which is to consider the front end, the back end and then how to prevent misuse of the back end.

But I really think what we can contribute and what you can contribute is a way to think about succeeding, not a way to think about criticizing but a way to think about succeeding. And I think it is frankly the question we also have to ask about our venture in Iraq, but that is not the subject before this committee. But if you have the answer to that, I would welcome it.

So let me just comment that I hope as time proceeds we will think about this. I hope as Secretary Chertoff releases his review of the Department activities we will think about this. I hope as

Negroponte ramps up the activities of the DNI we will think about this. Because the goal is not to rehearse old fights and certainly the goal is not to point out where we come up short, but the goal I think is to help good people in the field who are doing their darndest to produce accurate, actionable and timely intelligence get it right.

And public sources are a big part of this getting it right, and we have ignored them at our peril, every one of you has said that. How we do the mix, whether we separate out public sources or integrate them in everybody's job, I kind of like your concept, John, that a structural response to an operational problem does not solve it, but, nonetheless, getting it right is what we should be after, and getting it right as we protect the privacy of Americans is what we should be after.

So I apologize for not asking questions and running out the door, but I, again, Mr. Chairman and Ranking Member Lofgren, appreciate the fact that you have called this hearing and appreciate the content of this hearing. Thank you.

Mr. SIMMONS. I thank you for your remarks and for bringing your talent and expertise to these important subjects.

I do not believe that any members want to do a second round and so I would be prepared to close, and I simply want to thank our panelists for beginning this very important discussion on open-source information and open-source intelligence.

I think this has been a tremendously educational 2 hours. I believe that there is a great opportunity to follow up on this, to bring in at some data, appropriate date, the Department of Homeland Security to see where they are in this area and as well to consider a closed session on the issues that Mr. Weldon raised.

Again, if there are no additional comments from my colleagues, I would like to thank the panelists for their participation, and we stand adjourned.

[Whereupon, at 12:00 p.m., the subcommittee was adjourned.]

FOR THE RECORD

PREPARED STATEMENT OF THE HONORABLE SHEILA JACKSON-LEE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. Chairman and Ranking Member, I thank you for holding today's very important hearing on open-source information. I find it very timely, especially after my experience with the Committee on the Judiciary in analyzing ,the sections of the PATRIOT Act for reauthorization. As we pass legislation that facilitates the collection, storage, and use of intelligence information, it becomes more important to monitor the government's adherence to the fundamental Constitutional principles on which this nation was founded.

Of particular concern to me is Section 215 of those provisions. Section 215 of the USA Patriot Act permits the government to scrutinize peoples' reading habits through monitoring of public library and bookstore records and requires bookstores and libraries to disclose, in secrecy and under threat of criminal prosecution, personal records of reading and web surfing habits. This harms freedom of thought, belief, religion, expression, press, as well as privacy.

The Fourth Amendment of the Constitution protects Americans from unreasonable searches and seizures. However, several provisions of the Patriot Act authorize federal law enforcement to skirt the line of reasonableness. For example, section 206 of the Patriot Act "amends FISA and eases restrictions involving domestic intelligence gathering by allow[ing] a single wiretap to legally 'roam' from device to device, to tap the person rather than the phone."

Also, the Act allows federal law enforcement to delay notifying subjects of sneak-and-peek searches, as long as notice is provided within a "reasonable" time. A

sneak-and-peek search is one in which a law enforcement official searches the premises of a subject but delays the notification required by the Fourth Amendment until a later time. This type of delay is allowed when notification of the subject might have an "'adverse result.'"The "reasonable" time may be extended for" good cause." These expanded surveillance powers are especially troubling because of their apparent contravention of the Fourth Amendment's protection against unreasonable searches and seizures.

As the body charged with exercising oversight over the homeland security-related aspects of intelligence-gathering, this hearing is of extreme importance relative to setting the parameters of privacy policies. One of my concerns relates to the proposed establishment of the Homeland Security Operations Center Database (HSOCD) and possible exemptions from the Privacy Act of 1974. I would hope that this prospect is not slated to take effect absent a sufficient number of hearings in committees of jurisdiction.

Mr. Chairman and Madame Ranking Member, again, I thank you for your efforts..