# Office of the Director of National Intelligence

## Transcripts from the DNI Open Source Conference 2008
## Washington, DC

## September 11, 2008 – September 12, 2008

---

*The links below will forward you to the appropriate transcripts:*

**Remarks and Q&A by the Deputy Director of National Intelligence for Collection**
**Mr. Glenn A. Gaffney**

**DNI Open Source Conference 2008**
**Washington, DC**

---

MS. SABRA HORNE (ODNI Senior Advisor for Open Source/Outreach): Good morning. Welcome ladies and gentlemen and welcome to the Second Annual DNI Open Source Conference. We're thrilled to have you here. I'm Sabra Horne, Senior Advisor for Outreach and the organizer for this event. We see many familiar faces here, a lot of the wonderful folks we've worked with over the past few years as well as those of you who were able to attend the conference last year.

But in this last year, we've added many, many, many new faces to our friends and family list – those of you who know that using open source is vital in ensuring that we protect our national security. Our list of friends and family has grown, and grown, and grown. You recognize that open source information is critical in transcending the confines of the traditional Intelligence Community. In thinking about how we could top the success of last year's event, we wondered, was it possible? Is it important for us to gather Intelligence Community professionals with subject matter experts from around the world to address our most pressing questions? We wondered, is there a need for intelligence professionals to listen, to learn from the experts who they can get the most productive information from?

We heard from you and 3,500 of your closest friends; the answer was yes. Our goal with this conference is to bring together that ever expanding network of folks who know that open source information is critical. So to you, the fortunate 1,800 who were able to get in the door today, we say, we proudly announce to you that we have here representatives from over 80 colleges and universities, from 35 states, 47 think tanks, 56 nongovernmental organizations, representatives from state, local, tribal agencies from 38 states, from 370 private firms, from 60 media outlets, and from 38 countries around the world. And with this motley crew, we can and we will break down the barriers to collaboration, overcome our challenges of disconnected networks of different languages, lexicons, and acronyms, of jurisdictions, states, and country borders, to develop and enrich symbiotic relationships to best meet our security challenges.

In creating this exciting agenda, we listened to you. So this agenda was created by you and for you. Over the next two days, you will hear from many of our top leading experts in the Intelligence Community as well as subject matter experts from around the world. We'll hear from Glenn Gaffney, our Deputy Director of National Intelligence for collection, about his vision for the new universe of open source information. You'll hear from General Hayden, who will talk about the importance of open source within the Central Intelligence Agency. Unfortunately, General Clapper is not able to join us but we'll hear from Christine McKeown, the Assistant Deputy Undersecretary on how open source is affecting the DOD.

Tomorrow morning, we have a special focus on Homeland Security and we'll hear from Mr. Charlie Allen in regards to the new developments with Open Source as DHS. And we'll have an

exciting panel discussion about privacy, technology, and open source. Many, many things to CENTRA, especially Steve Schlaikjer, Patricia Rader, Jaclyn Harnett (ph), and Meredith for all the amazing hard work and good humor and good cheer and diplomacy. So thank you so very much. We also want to thank Harold Rosenbaum and the rest of CENTRA for all the support they've provided us over the year.

You told us this year that you wanted more training and hands on experience with open source capabilities. So here, over the next two days, we will actually train over 1,000 individuals in open source trade craft. Many thanks to Mark Johnson from the Open Source Center for achieving this amazing feat. Thank you, Mark. Plus, we have demonstrations and learning centers all around this venue. So please make sure you get around to see them all. We've slowed the breakneck speed of last year's conference a bit so that you all have more time to mingle, chat, and network with your colleagues. So please take advantage of that. We also have areas, business center areas over in the other part of the venue, where you can actually relax and enjoy a bit of a cup of coffee and some conversation.

Don't miss, also, our Meet the Speakers session which takes place this afternoon, where you can mix and mingle. Please keep in mind that this is a completely open, unclassified, public event, so please keep in mind your comments at all times. Finally, we'd be remised if we didn't note that today is Patriot Day and we didn't note the changes in information sharing that have taken place over the last seven years since the tragic events of 9/11.

Before that day, could we have imagined the information sharing that takes place? Could we have imagined gathering 2,000 individuals in this room, with media, with international partners, to share information? I don't think so. So to the sacrifice of others, our gratitude is great and our memories long. And also in accordance with the presidential proclamation, we will note, at 8:46 A.M., a moment of silence in recognition of those who have fallen.

Now, it's my honor to introduce Mr. Dan Butler, our Acting Assistant Deputy Director of National Intelligence for Open Source. Mr. Butler has been part of the DNI since the very earliest days of its stand up and served as the senior advisor for policy. His 25 years in military intelligence and law enforcement gave him a great appreciation for open source. And it is his vision for the broadening and furthering of the wider open source community that drives him to this day. Mr. Butler. Enjoy the conference.

(Applause.)

MR. DANIEL BUTLER (Acting Assistant Deputy Director of National Intelligence for Open Source): Sabra, thank you and also, I'd like to echo Sabra's thanks to CENTRA Technology and the great team that CENTRA put on organizing this conference this year. They've done a terrific job, a lot of good work behind the scenes. I want to thank FBC, also, for organizing our Tech Expo, which is occurring right across the atrium. I strongly encourage that you visit our exhibiters. They have some remarkable new capabilities that they would like to share with us in the community and share with all of you, who come from the broader community beyond the Intelligence Community.

Want to thank our co-host, the DNI Open Source Center, Doug Naquin. Thank you, director for supporting us this year and co-hosting the conference and the Department of Homeland Security, Charlie Allen, Barbara Alexander. He's the senior executive responsible for Open Source. They've been terrific in helping us put together a fantastic conference – what I anticipate will be a fantastic conference for all of us here today. And, of course, I want to thank all of you. Thank you for coming. Those statistics that Sabra just recited are very impressive and they – it excites me to know that we have been able to draw 1800 people out of the 3500 people that wanted to come to the conference to join us here today in collaborating on how we can use open sources better to perform our mission of creating decision advantage.

Let me start by echoing comments that you saw in the video right at the outset from Director McConnell, our boss, here at the Intelligence Community. Admiral Mike McConnell talked about the thing that he thought would be most important if there was only one thing that his tenure was remembered for and that was collaboration. And I see no better example of collaboration than what we're doing today. The great work that we've done bringing so many experts and practitioners, analysts, collection-requirements managers, operators, collectors together within the Intelligence Community to work on open source issues. And more importantly, collaborating beyond our community to include so many of you that are here from academia, the private sector, think tanks, and our international partners. Thank you very much for joining us.

Congressman Rob Simmons, in the video that you saw at the outset, mentioned that we've come along way and I couldn't agree more. We really have come a long way and I'd like to highlight for you just a few things that I've seen occur in the three years that I've been here at DNI. In 2005, Ambassador Negroponte, our first DNI, established an office in his office focused on open source issues. And I've had the privilege of serving in that office for three years.

Ambassador Negroponte established the DNI Open Source Center and he built that around a real – a venerable institution that for over 40 years has done nothing but hone the fine craft of open source intelligence, the farm broadcast information service. The new DNI Open Source Center has done remarkable work and I think you'll see some of that today and you'll learn some of it as our various speakers tell you what we've been able to accomplish in just the last three years.

In 2006, we published an open source vision for the Intelligence Community. This little red book, which I'd like to call it the little red book to tease my former boss, Eliot Jardines, our first Assistant Deputy DNI for Open Source. And yet, it's had a profound effect on our community. Just 12 pages have driven an awful lot of reform, change, innovation within the Intelligence Community and beyond. We wrote the first Intelligence Community directive on the National Open Source Enterprise in 2006 and we established a highly collaborative community collection committee focused on open source intelligence strategy, planning, and policy.

This collection committee, which advises my boss, Mr. Glenn Gaffney, on open source issues, is comprised of senior executives of flag offices from across the community that meet regularly. Typically it's been about six times a year and their agency subject-matter experts, who meet much more frequently. Typically a month – every month on various issues and they meet

regularly to approve our open source enterprise. They're doing terrific work and you'll hear a little bit more about that today.

In 2007, I would say if you had to capture in one word what we started to do it would be invest. We invested in greater open source capacity across the community. We expanded the DNI Open Source Center, their capacity to provide open source research and analysis on very difficult issues. We expanded access for Intelligence Community analysts to quality, commercial open source products and services and, of course, we organized our first DNI open source conference.

In 2008, we established foundational open source training and dramatically increased the training of Intelligence Community analysts in fundamental open source skills. We delivered training and open source exploitation to several state and local fusion centers across the country, a program that's expanding over the coming year. And we're using this conference this year, as Sabra mentioned, to whet your appetites and deliver more introductory training to a broader array of government professionals.

We invested. We continued to invest in 2008. We invested in dedicated open source support to AFRICOM, the newest combatant command, a very unique hybrid command, an exciting initiative that you'll hear more about tomorrow from General Clapper's representative, Ms. Christine McKeown. We invested in open source proof of concept innovation projects. Several of these were in direct support of AFRICOM and we leveraged open source expertise and outreach networks of the Department of State, the U.S. Army's Foreign Military Studies Office, and the Marine Corps.

We invested in the National Air and Space Intelligence Center, in my opinion, one of the crown jewels of our national open source enterprise. We invested in IC librarian professional development, something that was long overdue. We invested in the National Virtual Translation Center, a critical capability that allows us to reach out and tap the skills of capable linguists across the country and around the world virtually. You'll learn more about that today and tomorrow. You'll hear from our director of the NVTC, Mr. Jeff Robinson, and Ben Thomas, from the DNI's foreign language program office.

In 2008, we worked hard to strengthen our partnerships with academia and private industry and with the close collaboration of open source experts and analysts from across the community, we designed and have fielded an Open Source Collection Acquisition Requirements management system – we call it OSCAR – to connect intelligence consumers, analysts and collections requirements managers with providers of quality open source intelligence from across our national open source enterprise.

Finally, we've revised our vision and strategy for the first time since 2006. You'll hear important ways we have revisioned, as I like to say, later today from the director of the DNI Open Source Center, Mr. Doug Naquin, and a panel of colleagues and experts and senior representatives from the Intelligence Community, the Department of Defense, and the Department of Homeland Security. I strongly encourage you to hear Mr. Naquin's presentation and learn more about how we're building our open source enterprise of enterprises.

That brings us to today. We've done a lot but where do we go from here? How do we continue to leverage open sources to achieve clear decision advantage over our adversaries and how does this fit into our long-range vision for the Intelligence Community's future? First, I'd like to say a word about humility and that's probably not a word you hear often being uttered from the lips of someone in the Intelligence Community. But it's important that we think in terms of humility as we tackle the problems that we have in the Intelligence Community. According to Wikipedia, humility is one of the seven capital virtues, something we'd all do well to have in greater abundance. And I'm reminded of something Ted Turner, the founder of CNN once said, "If only I was more humble, I'd be perfect." (Laughter.)

We in the Intelligence Community must recognize that we're not perfect, far from it. But a little humility goes a long way and I put that in the context of open source. We don't have all the experts, all the best ideas, all the answers. In today's day and age, a little humility on our part will free us to be more open to outside expertise, ideas, and answers. I like how Carol Dumaine, the Deputy Director at the Department of Energy's Intelligence and Counterintelligence Office puts it. As Carol might say, "We need to move from thinking of ourselves as an Intelligence Community to a community of intelligence." I think our humility is on display today and we invite you into our open source community of intelligence. Help us achieve the wisdom and decision advantage we need over our adversaries.

Secondly, I'd like to call your attention to DNI's new Vision 2015, a globally networked and integrated intelligence enterprise. These are easy to get your hands on and get a copy of. This is a very bold vision for the future. It captures, well, the world we will operate within the next decade – over the next decade and I think it illustrates our humble recognition and we must adapt and learn from experts wherever they reside.

I'd like to just pull out three quotes from DNI Vision 2015. First, there is no typical customer. We will be providing intelligence to a computer-literate generation that grew up with the Internet and user-generated content, for example, YouTube, blogs, wikis, in which they acted as both consumer and contributor of information in an on-demand environment.

Second, to respond to the dynamic and complex threat environment of the 21st century, our operating model must emphasize mission integration, a networked, knowledge-sharing model that rapidly pulls together dispersed and diverse expertise and resources against specific missions. And third – and this is probably my favorite line in Vision 2015 – no aspect of collect requires greater consideration or holds more promise than open source information. Transformation of our approach to open sources is critical to the future success of adaptive collection.

Thirdly, today, I'd like to call your attention to the DNI open source challenge, where we challenged you, the community – the broader community – our community of intelligence – to demonstrate how we might transform our intelligence enterprise to deliver clear decision advantage to our customers in the future. You'll hear more from Dr. Mark Lowenthal this morning as he introduces the process that we went through to conduct this very innovative outreach to the broader community and I think you'll be impressed by the submissions that we received and that will be presented to you tomorrow.

Finally, I call your attention to the visionaries, leaders, and talented practitioners who imagined what is possible and challenged us to defy convention, embrace innovation, and fully exploit open sources to achieve decision advantage and they're all around you in you this room today and they'll be all around you over the next two days during our conference. Please take advantage of that opportunity.

It's my pleasure, today, to introduce one of national security community's true visionaries, a leader focused on the future, an innovator. His biography in your program tells it well, so I won't recite that. An astrophysicist, a career intelligence officer, and I would be so bold as to describe him as one of our community's most creative, unconventional thinkers and leaders, Director Mike McConnell's deputy and the Intelligence Community's senior executive responsible for leading, inspiring, and coordinating our vast Intelligence Community collection enterprise to include our national open source enterprise, our Deputy DNI for Collection, Mr. Glenn Gaffney.

(Applause.)

MR. GLENN A. GAFFNEY (Deputy Director of National Intelligence for Collection): Good morning. I'm going to wander around a bit because it's my practice to wander around. As the Deputy Director for Collection, I get asked to come and speak in a number of different forum and a lot of times those are classified forum and a lot of times when you're in those forum, you've got a podium, you've got a sign above your head, and that sign above your head usually sets the classification level. And I learned very quickly that one of the things that made me uncomfortable was standing in front of a podium where we were dealing with special access programs because I'd stand in front of the podium and the sign above my head said SAP, all right? And so I've trained myself to get away from the podium. While it may be true, I see no need to advertise it. (Laughter.)

Thank you for the opportunity to come and speak to this great conference. I heard nothing but wonderful things about last year's conference and was excited to have the opportunity to come and speak, to meet you all here today. It is important to be here. It's important because of the critical nature of open source and this intelligence enterprise and it's important for the opportunity that it represents in terms of what open source can do for the future of the intelligence enterprise.

Now, one of the things that I got asked very early in my new life as a congressional cat toy* within the DNI was, Glenn, what's the future of collection? Where are we going? Not where we're going with HUMINT, not where we're going with SIGINT, not where we're going with our space program or any other aspect of the program. We're going to work all those things and we do all those things and we do them very well but it's a broader question and it's a question that comes to the DNI. What is the future of collection? And I thought, well, as the Deputy Director for Collection, I probably ought to ponder on that for a little bit. And so in thinking through and I came up with what amounts to two words: integrated performance. It's that simple and it's that complex.

We are an incredibly well-resourced intelligence enterprise. We use that enterprise and optimize that enterprise and have been doing so for many years with great effect against some of the most pressing challenges that this nation and our allies face. But if we look at the world across the board, and I'm sure you've heard it in other forum before, we don't own the technology playing field like we once did. Anyone surprised by that statement? It's not there for us the way that it was for us before. It's there more from a collaborative and interactive nature but it contributes. That lack of owning, that technological playing field creates a more level playing field across the board.

When you take that piece and then you look at what could argued be the cost per bit of information, globally, goes down weekly. Add to that that the cost of entry into the intelligence business has gone down dramatically. A laptop and a modem and you're in the game. You may not be any good at it but you're in the game. And so if we think of cost per bit going down, not owning the technological playing field, lower cost of entry into the business, we see a level – a more leveling of the playing field, a leveling of the playing field relative to the intelligence enterprise and those who would do us harm.

And so when I sat back and I thought from a DNI perspective, as the Deputy for Collection, as I look out at this incredible enterprise with the responsibility for oversight and how we move this forward, what do we see as the future of the enterprise? The future must be the speed at which we integrate this incredible resource to deliver new advantage for this nation and our allies' leadership in protecting and defending democracy and our citizenry. That's what it's about, the speed at which we take these great things that we have developed and braid them together with singular purpose to answer critical questions that are at this nation's – right at this nation's doorstep, is the way that we will achieve and it will be the definition of our strategic advantage going forward.

Open source is one of those absolutely critical strands that we must continue to develop and braid within that discipline itself so that we go, as Dan said, not from just an Intelligence Community but a community of intelligence and how we bring those pieces together, right? And combine it and integrate it for a new level of product; a new level of performance for the nation.

In a few minutes, we're going to have a moment of silence. I'm going to read a quote for you. It's one of my favorite quotes. It's been hanging in my office since about September 13, 2001. I've used it as a guiding principle and I think it's apropos to what we're talking about today and where we're going from the way we think about open source and we think about this intelligence enterprise going forward. Abraham Lincoln in 1862 said, "The dogmas of the quiet past are inadequate to our stormy present. The occasion is piled high with difficulty and we must rise with the occasion. As our case is new, so we must think and act anew."

We've seen this playing itself out over and over again since 9/11. You've seen it just in looking at the open source enterprise and the way that it's developed. We must be diligent and persevere and continue to challenge ourselves to think and act anew in order to continue the progress and build on that for new results. I want to talk for a minute about how we think about open source. So can I have – I have two charts, I think. Can I have the first chart? Somewhere? That's me. (Laughter.) There we go.

Very simple Venn diagram, the Venn diagram that I drew myself many years ago and I didn't – wasn't the first one to drew it. We all drew it, all right? We used to think about collection in terms of three Venn diagrams that overlapped: HUMINT, that which we collect via the humans, all right, agents in the field; technical means; and then open source and how we looked at how they overlapped and how they worked together. Nice. It was a good construct in the Cold War. It was good construct, really, before the information age began to take hold. Not the way we think about it today. And so when I came into the job eight months ago and sat down with Dan and talked about what my vision for the way we needed to approach open source; that we needed to look at it differently. Dan said really interesting, Glenn. I think I have a picture you'd like to see and so could we put up the second chart?

It's not three overlapping circles anymore. It's two overlapping circles, if you will, the HUMINT and the technical pieces, that are operating in an information plane, in an information universe. We can't just limit our thinking to that one simple circle and what we get via just a handful of open sources. We need to think about that great information universe that's out there; how we look at that and take advantage of that; and then look at how then we drill down using some of those other areas, some of those other intelligent disciplines that we have to build on that to incorporate with that to get at a different level of information associated with it.

And the information enterprise and those who work in is a much broader thing than one element or two elements or a couple of elements in the Intelligence Community. Across that information universe, we have this open source area that we're looking at as the IC and then we've got a broader element of this, which is other elements within the U.S. government, other elements in the U.S. government that aren't necessarily the IC, who have needs to gather information and develop that information in the prosecution of their mission.

We need to meet them where they are, collaborate with them, work with them, let them define to the extent to which they want to work within or with the Intelligence Community in this regard and how much for the prosecution of their mission they need to work or want to work separate from that. Absolutely critical that we get the best of breed piece moving forward as we look through and talk through the different approaches, the different strategies, the different venues that we use, and always sharing what we are learning, what we are discerning from working this information with each other.

The Open Source Center has made great strides, right, in this regard and it is a shared and common vision. Beyond the U.S. government, of course, is our international partners, academia. We need another level. We need new levels of partnership and interaction along those same lines that I just talked about in this area, again, why I'm excited by what we've got here, what's represented here; the talent, the thought that's represented in this room.

Now, I've got several boundaries here that we need to look at relative to capacity requirements and the way that we work the mission space but I've also got another piece on the other side that talks about our need to manage concerns on things like intellectual property, privacy, right, and the policy concerns that exist at each of those boundaries and maybe some that we haven't even discovered yet. Being sensitive to those, it's absolutely critical as we move this forward and

there's an entire session in this conference on national intelligence and privacy. It becomes how we think about privacy and security as oppose to security versus privacy.

It's absolutely critical, as I mentioned before, that we take full advantage of the broad range of information and the broad range of approaches that are represented here in this room. The diversity of information and thought that we have here that's represented here is exciting to me and I hope – and it's why I came, all right – and I hope it's why you are here as well. But, again, coming back to Lincoln's – the quote that I used from President Lincoln, the idea is wrapped around thinking differently.

I had a lesson from an earlier job in my operational career where we got into a different type of an operation. We got into some really good information. It was a tremendous amount of information but we had been – we had been treating it much like we had treated a lot of other operations in the way that we were just – we were getting the information in, processing the information, and putting that information out, a traditional reporting kind of a stream. And we sat – several of us sat and we looked at it and thought, you know, this is good and we're getting really good stuff out of it but there's got to be more here. What might we do differently to try to unlock some other things, some new insights that we didn't have before?

And so we took one of our conference rooms and turned it into a workroom, wired it up, and went out across the community and got a handful of top analysts. We wanted some of the – we wanted some of the top analysts that were out there: young, fresh minds coming at this data from a new perspective. So, good, I want you to come in. We're going to set you up. We're going to give you access to this information and then we also took a developer, right, a technology developer who was working on information systems – information management techniques – and put them in there with these analysts. I said, here's what I want you to do. I want you to come in and teach us – look at this data, see what you can do with it, and think about the data and how we get information out of it, and what might be discerned. I want you to think differently.

The main product was a lab to think about the data and what we could get. The product – we were already putting some product out – I wanted to see what more we could get. But I asked the analysts, get in here and do everything you can to break the system. Push it beyond what we've designed it for and when it breaks, tell the guy who's sitting right next to you, who's the guy who built it what you were trying to do and why it broke and let's see if we can turn that cycle, right, into a hours-and-days cycle of discovery, pushing the system beyond where it was designed to go and fixing it so we can that much further. And we had a really high time because in the space of a couple of months, this group – it started with six, then it was 15, then it was 25, then we had to cut it because people were waiting to get in the door.

People were real excited to get in there to see what they could discover. And we were turning the code around and getting the code set up and fixed so that they could push the thing further and further, if not daily then by the week and get more and more information out of it. That experience – that fortunate experience that I had and that one set of operations changed the way that I thought about information. I suspected it and then I saw it. This may be no news to most of you who work in this – you know, who work in this domain but it was an exciting revelation

from my perspective. And, again, to me, it just points at a small area of what could be a tremendous resource given this open source enterprise and where we need to go in the future.

Given that, though, let's talk about, you know, just how deep this rabbit hole goes. Many of you have heard about – some may not – that what we refer to as the double-humped camel looking at the workforce dynamics, all right? About 45, 50 percent of our workforce in the Intelligence Community has been here less than five years, first hump of the camel. Then we've got the trough that's represented by the hiring gap of the '90s. Then we've got the second hump of the camel, people like me who have that, you know, graying retriever look, right, coming along, who were, you know, here at the – you know, for the Cold War piece.

What does that mean in terms of the way our Intelligence Community develops and moves forward? What does it mean as we move that new group of intelligence professionals into more and more areas of responsibility faster than we ever did ourselves? How do we give them the exposures and experiences that are absolutely required? How does our ability to work information and think about information differently – to mash up information differently within an intelligence context provide a new infrastructure for them to lead this community in the 21st century? Think about the information age and all the cultural change that we're going through.

We are, by some estimates, 15 years into what is a 30-year change cycle, culturally. Some of us are living it with that double-humped camel. Being able to think differently about how we mash up this data becomes incredibly important, not just from the open source perspective, but because it provides an incredible laboratory, that think arena, where we can draw in a much broader section of the open source community and learn what that mash-up infrastructure – what else might be done, how we push that. And while we are doing that we are also within the borders of the classification system and the way we protect sources and methods – the work that we are doing to link the networks, to link information, to link agencies, the infrastructure that we are putting in. What I see is the ability for what we learn in the open source community in the best practices, and looking at how we mash up and learn new things from that information and laying it right on top of that new infrastructure that we're building.

Now, this gang coming along on this first hump, they are the mash-up generation. Make no mistake. There's a great little book – good little book called "Got Game," all right – read it a few years ago. At first it was very depressing for me because it proved once and for all that I was not a tweener. I was actually part of the Cold War generation – tail end of the baby boom. Why is that? Because the Internet and things like that, to me, are a hobby. I don't measure my life experiences by what I learned online with my buds, but somewhere approaching 45 to 50 percent of our workforce does.

Now, look, we can, as intelligence professionals – how many of my fellow intelligence professionals do I have out here in the audience? We can, as intelligence professionals, work through, do what we can do, and let evolution take care of this, because they're coming; it will happen, but that's not enough. We owe it to this nation, we owe it to our allies, we owe it to the citizenry, we owe it to those young professionals who have chosen a career of service to our country to build that infrastructure, to enable the thinking, to put the pieces in place and let them show us things that we didn't dream were possible moving forward.

If you think about that 30-year cultural change cycle and you measure that relative to my career 23 years in, compare it maybe to some of your own careers, what does that mean? That means that the sum total of our career as part of this cultural change won't be about that great op that we ran. It won't be about that great technical endeavor that may have been undertaken and achieved. It certainly won't be about that great contract that you laid down. It won't be about the amount of money you've made. The sum total of our career is going to be measured by how well we have left the enterprise, how well we have built the enterprise for that next generation to lead against the security threats that face this nation and our allies in the 21st century. That's what it's all about.

Second quote – are we there? Okay. Please join with me now while we observe a moment of silence for those who lost their lives on 9/11 and those who have lost their lives in our response to terror post-9/11.

(Pause.)

Thank you. We will not forget and we will not let up.

As we think about how we move forward, all the things that I just talked about – our responsibility, our responsibility to this next generation, of citizens of this next generation of intelligence professionals – I'm reminded of a second quote, again from President Lincoln, who said, "I am not bound to win, but I am bound to be true. I'm not bound to succeed; I am bound to live by the light that I have. I must stand with anybody that stands right, and stand with him while he is right and part with him when he goes wrong." I'm not bound to win; I am bound to truth. I am bound to partner with those who seek truth. Think about those cords, those braids that we want to tie together relative to a community of intelligence and how we bring that together for a new level of integrated performance; what we can learn in this community and how we lay it over on the other part of the community.

It's important for us to remember that we're not bound for our individual idea. We're not bound to our individual program. We're not bound to this agency, this enterprise, this university, this piece. It doesn't matter. We are bound to truth. Ladies and gentlemen, the name of the game today is the same that it has always been. It is the pursuit of truth. We refer to it as intelligence inside this community circle, but that's why we do it. It is about discovering, discerning truth, and using that truth for its best for our citizenry.

When we look at all of these things – again, I will close by talking about how important it is to look at the opportunities that present themselves, for all the things that I've just mentioned that are represented right here in this room, opportunities to discover and integrate new images and new information from a wider range of sources in near real time; opportunity to discover new sources of language, thought, cultural perspective with in situ experience where the action of interest is occurring; opportunities to look at different in situ actors and their responses to provide new insights; opportunities to watch how stories develop, deconstruct, and reconstruct between traditional and non-traditional forms of media; opportunities to discover new approaches to mash up data and to deliver new insights.

There's an incredible landscape of opportunities that's before us. I am convinced of our continued success because of the talent, the skill, the desire that's represented here in this room. Have a wonderful conference. I will be here as much of it as I possibly can to get to know some of you to talk to you about your ideas, your thoughts, but I'm really excited about what you're going to accomplish for these next two days. This conference is a beginning. Bind together in a new way. Take us new places. It's what your colleagues, it's what your folks back home, expect from your government. Thank you. (Applause.)

I think Dan wants me to answer a couple of questions.

MR. BUTLER: You have a good 25 minutes, Glenn, and here's some that we got from the audience.

MR. GAFFNEY: Okay, the first one is, "How do you determine which intelligence source is for any given issue?" We have an intelligence process that sets out looking at what the gaps are in our understanding about particular issues. That comes from discussions that we have with policy-makers, discussions across with other analysts. Those analysts then, based on those discussions and based on their analytic prowess, their ability to understand, identify critical gaps that are out there and then put those gaps before the collection community and say, what can you do for us? We begin then to evaluate all the different sources that are out there and look at what those different sources can provide, and look then at what the right mix is of those to get the kind of information that we need, right, to address the questions that the analysts are asking – policy driving the analysis, analysis driving the collection, all right?

Again, it's part of why I talked about how we think about open source. We used to think of it as just one more piece in that puzzle, but I really believe the open source enterprise and the information age gives us a whole new area to think about it and to think about it differently, which is what I based most of my remarks here today. It's a limited resource, though, when we look at what's out there – not just on open source; I'm talking about the whole shooting match, all of collection. And so that's why we have to continually look at what's the right mix, how do we optimize that? If we're going to move things and focus assets in a different way, we have to think about what the real costs are and what the opportunity costs are associated with that against what we believe we stand to gain by answering that question, or getting after that question, all right – again, an area where I think it makes it even more important for us to look at all of what open source and what mashing up data can provide in terms of new insights, in a faster and more timely way.

It says, "Given how many open source practitioners are out there, how do you determine best of breed?" I'm not a good judge. So what I'm interested in is how do you determine best of breed? How will you, in working together, right, discover new avenues, because right now there's a lot of different pockets of open source work going on. They may not call it open source work; they just may call it research, but it's going on. How do we discover that, all right, identify it with each other, begin to tie it together, test it, try it, see how it applies, and then build on that? It's not a top-down thing. It can't be. It's got to be by the practitioners themselves.

"In your experience, how has open source intelligence cued other INTs in critical situations?" I can't get into some of the specifics of what it cued in terms of what we did as a result of it, but, you know, as we look at – as we have looked at open source reporting, at open source information coming in, it has given us some insights, not so much from – well, in the cueing perspective it's been about, this is going on over here, we knew that in general, but now we end up with a specific point that we might want to apply pressure to, using some of the other INTs to drive deeper on, right? It gives us a landscape that gives what I will call a first order of targeting, if you will, to understand where we might focus the other resources and how we might build on that.

In addition to that – again, I'm answering specific to cueing – in addition to that, it is an intelligence producer in its own right because, again, just because it's open doesn't mean that it's wrong. As a matter of fact, with the cost per bit going down and the amount of information that's out there, new insight and that discovery of truth becomes a real issue, a real benefit, right? And so, open source, in many ways, becomes the source, is the source of first resort, not just another source. And you'll hear Doug and you'll hear Dan talk about those things throughout the conference, I'm sure.

"Your staff has been quite zealous in promoting the value of open source. Why?" (Laughter.) Because they work for a zealot. (Laughter.) No, they're zealous in the pursuit because they believe this. It's not just another job in the train of jobs that they have. They're zealous in its pursuit, because I sit with them every day and we talk about what they're doing, and they are excited about what they see going on out there and are looking for, how can we use that to improve this intelligence enterprise? And they get more excited by it by the moment. Now, the suggestion here that comes after it – is it because Congress said it should be a priority? No. I'm glad Congress said it was a priority, and that's a great area that we can partner with Congress on and we do partner with Congress on in terms of the discussions that we have with them in terms of the open source enterprise and where we're going with it. It is fundamentally because we believe in its value and believe in the opportunity that could be provided via open source.

They just keep coming in. (Laughter.) This one's a long one. Hang on for a second. (Pause.) Yeah. It says, "It would seem, in an area of what could be declining budgets for our national security community, open source might actually fare well if the high return of investment of open source intel is appreciated. Care to comment?" I'd say, exactly. Economically it's a no-brainer. The partnerships and what they can produce going forward even increase that return on investment. In the information age we end up with the law of increasing return instead of the law of decreasing return, or so it's been said by some, right, but it's an interesting idea to ponder. Just think about it in terms of your cell phones or your email account. Now, it's been so long since we've had email we've forgotten what it was like when we first got it, but when we first got it, a lot of coffee pot and cooler conversations were, do you have email? Oh, you don't have email? You need to have email? It's really great. You do all this stuff. Why not? Why? Because everybody that I knew that got on e-mail made what I was spending for email suddenly that much more valuable. It's the law of increasing return, associated with being hooked up, wired, and interconnected.

Again, open source provides this incredible laboratory for us to get the best, to begin to look at what that return on investment can really be. And as we look at open source as a primary source of intelligence in certain key areas, not just another source of intelligence, and a primary source not because they're the only ones looking at it, but because we said right up front, we want to go after this using open source. You hear the difference in there? Not the only source by default; the source by design. That's where we need to move. That's where we are moving. It's some of the ways it's being used today.

"Is there a unique role that academic organizations can play in open source support to the IC?" Yes, but it's not just support. Think about the centers of learning that are our academic institutions. The whole idea of encouraging critical thought and in taking advantage of that information age in that library and in that great laboratory, that library that is the open source universe, how that gets put together and used and challenged to our students, how to use that information differently to come up with new ideas and new insights?

We're going to run out of time, if not for any other reason because I'm a slow reader. The academic institutions are pioneering areas of thought in the way that we think about these different areas and as it applies to national security issues, global issues, all right? It absolutely is a great center, not just in preparing the folks who may come in to a career service within the Intelligence Community, but as the take on responsibilities across the government, across the nation, as they become active, productive citizens.

Okay, "I've heard you talk about integrated mission management or integrated performance management. How does open source intelligence fit into this framework?" I touched on it maybe too briefly as I went through, but as we look at taking all of these elements that we have and getting after critical targets. It's not a matter of just asking the SIGINT folks and the HUMINT folks or the military folks or – you know, saying, okay, what can you get out of this and let's figure out how we tie it together. That's more of a collaborative piece. I'm talking about integrated planning for a different level of performance. When I say integrated performance, I'm talking beyond collaboration. I'm talking we're purposefully sitting down and saying, let's come up with a new idea, a new way to blend all these pieces and tie it in. And it's not a matter of thinking about that and then going, oh, and what did open source say?

And so one of the things that we've done is we've taken some of the open source folks who were on our team and embedded them with our teams who were driving our integrated performance plan. So they are embedded as part of the team, looking at the new strategies for going after these targets and how we tie those pieces together. It needs to be represented front and center at the cutting edge of the way we're thinking about going after the problems, and the team is doing that.

Okay, "How do you envision incorporating open source geospatial info into IC product?" That's one of the opportunities that I highlighted there right at the end. Think about the range of images that are out there, that are available out there today, and what that can do for us – what it's already doing in some sectors but what it can do for us in the way that we pull information together and mash it up with other information. The picture is often – and has many times been said – worth a thousand words. Sometimes pictures are created to give you the thousand words

that aren't necessarily true. So it's not just a picture for the picture's sake; it's the picture and how it combines with all the different pieces of information that you have – that you have available within that open source universe and we have available within the Intelligence Community enterprise inside that sources and methods line, if you will, and how we bring that together and use that for new insight.

We – you, right, need to think about what those opportunities really mean. I know that there's some technological innovation going on in trying to improve some of the capabilities that are out there, both in terms of capturing and transmitting things from cell phones and different video and how we move those things through. They have great commercial value and they should be invested for that purpose, and many people are investing for that value when you think through what that means and how we take advantage of that both in the open source domain, all right, and in the classified operational domain.

This one is my favorite. It is blank. I am flipping through these because I obviously mixed them up. Back to the zealous staff. Okay. "Is anything being done to help train all source analysts?" Yes, absolutely. You heard Sabra mention before the training that is going to go on just in the margins of this conference. But Doug and what Doug is doing with the Open Source Center has a huge training initiative that he has been building and working on.

We have been supporting a number of different training initiatives across the board. And in the vision for the way open source moves forward, that whole point of meeting people in the open source community where they are. Some of them recognize a need, but wouldn't necessarily identify themselves with the open source community. But meeting them where they are and defining what they need to be able to help build that piece out is a critical piece. So you may not want to depend on the Intelligence Community. You may be concerned about an Intelligence Community taint on your element of the government because you don't want the intelligence thing hanging over it.

Nevertheless, you need an ability to do that. We want to encourage you in developing that capability. All right. There is no monopoly on the tradecraft. Just teach it. And the better you are at it, the better product that comes out of that, the more we gain together. And so it is a matter of bringing the different aspects of the community along and developing them, right, and developing their overall capability, and then making sure that it is tied together.

Okay. (Chuckles.) I am going to paraphrase this question because it is a little derogatory in a couple of places. This question here is looking at – look, we have got a lot of folks in the room who are true believers in open source and what open source can do. But there is a lot of folks, maybe some that look like me, that feel like open source has less value because it is unclassified. All right. You know, you can look at it – and I am sure that there is probably a thesis involved for somebody who wants to study what happens when you have a secret, and the value that somebody puts on a secret, and then they begin to think about – well, this has got to be of extreme value because it is secret, as opposed to this thing that was open.

Most of the time what we put as secret, we put as secret not because of what it said, but because of the way that we got the information. We are protecting a human being. We are protecting a

source. We are protecting a method. That is why it is secret. Right. The data itself, right, is not usually the reason why we classify it. Okay. But it is easy to fall into that give me the good stuff. The good stuff is the truth. I have said it I don't know how many times. And open source has stood, will stand, and will lead in the test of time – my prediction – relative to truth and timely truth, right, in the pursuit of our national security objectives. It is today. It will continue.

We have got to make the most out of the resource, get the most value out of it that we can possibly get. And I believe there is a lot more here building on top of what has already been tremendously successful. It will come. It is. And for those who feel like it is not of value because it is unclassified – they will learn or their time will come and go. Evolution will take care of it. With that, we can be guaranteed. (Chuckles.)

I have time for one more. Don't know the answer to that one. Dan might. I will give that back to Dan. Maybe he can answer it later. Okay. This is an interesting one. And I need to be careful answering it, but I want to answer. "Does your vision of this new universe of open source info diminish the need for OPSEC-ing counterintelligence, and there is" – somehow I knew there would be more on the back. I was actually looking for a name so I could talk to the person offline. "And does any of this imply a diminished role for operational security and counterintelligence?"

Yes, my vision does include, right, what it means relative to OPSEC and counterintelligence – both in terms of that leveling playing field that I talked about right up front, and in terms of what that specific in situ reaction is to certain events that may be going in on the ground or the way that they are being interpreted because people can come to the right answer for all kinds of wrong reasons. And it doesn't really matter to me from a counterintelligence or operational security perspective that they got there for the wrong reasons, right. What I care about, right, is the protection of the people who are engaged in the operation and the protection of the operation itself when I am taking about OPSEC and CI.

Do I think that means that there is a diminished role? Absolutely not. All right, the back half of the question – is there a diminished role for operational security and counterintelligence? Absolutely not. It is a maturation of the game. It is how we use all of these things as intelligence professionals to achieve what is required for the nation. Again, all right, thank you. Thank you for being here. Thank you for the work that you do. Thank you for our zealousness relative to open source and what it can do. Get more zealous. All right.

But be patient. Your colleagues may not always get it right. It may go slower than you want it to go. It seems like it is always going slower than we want it to go. But remember the higher calling is truth. It is the highest calling we have. And be bound to those who are bound to truth. Thick and thin. Ben Franklin put together – I can't tell you how many because I read it and I can't remember the number – but he put together a number of resolutions, things that he wanted to have included in the Constitution. Came time to vote for it, not a one of his got picked up. He voted for it anyway. Somebody asked him why? And he said, it seemed to me that the whole import of the thing was more important than any one piece. Same principle. Same principle.

Press on. Press on. Be bold. Be creative. Encourage one another. And let's achieve new and extraordinary things on behalf of this nation, our citizens, and our allies in the pursuit and the security of democracy and freedom. Thank you. Have a wonderful conference.

(Applause.)

MR. BUTLER: Glenn, thank you. As one of your zealots on your staff here, really enjoyed your remarks. And I can tell you working closely with Mr. Gaffney, if we don't walk into the room excited every morning at 8:00, we walk out very excited by the time the meeting is over.

(END)

**To break the ice, I began this speech with a poorly chosen jest. I had no intention of diminishing the vital role our Congressional partners play in the work of the Intelligence Community. As the Deputy Director of National Intelligence for Collection, I know firsthand how seriously Congress takes its oversight responsibilities. I am committed to building and sustaining this important partnership*. - Glenn Gaffney

**Remarks and Q&A by the Director of the Central Intelligence Agency**
**Michael V. Hayden**

**DNI Open Source Conference 2008**
**Washington, DC**

---

MR. DOUG NAQUIN (Director, Open Source Center): Good morning, again.

To recall yesterday afternoon's community panel session, I noted that as we developed our capabilities over the past few years, both in the Open Source Center and in the community writ large, we needed to secure a voice at the proverbial table or tables so we could begin to have those conversations that would institutionalize open source as a recognized program as well as, as a discipline.

One person who has been instrumental in getting open source a voice at those tables is our next speaker: first, as Principal Deputy Director of National Intelligence under our first DNI, John Negroponte; and now as Director of the Central Intelligence Agency.

Michael V. Hayden has insured the Intelligence Community does not lose sight of an environment that we've seen over these two days is growing and morphing continuously in terms of its potential to improve our knowledge of and insight into the world in which we operate. As much as anyone, Director Hayden has taken the community from acknowledging open source is good to actionable footing.

As a former military attaché in J-2, he is deeply familiar with the value of open source on the ground, and as a former Director of the National Security Agency, he is certainly no stranger to the challenge of volume.

So without further ado, it is my distinct pleasure to introduce Mr. Michael V. Hayden, Director of the Central Intelligence Agency.

(Applause.)

DIRECTOR MICHAEL V. HAYDEN (Director, CIA): Well, thanks, Doug. Good morning, everyone. It's a pleasure to be here. You get 39 years of being only able to wear a blue tie, and you see what happens, huh? (Laughter.)

As Doug suggested, I'm no stranger to the open source discipline and actually quite a fan of it. As you mentioned, I'm a career intelligence officer, so I'd like to start today with maybe an observation that could surprise some of you. Secret information isn't always the brass ring in our profession. In fact, there's real satisfaction in solving a problem or answering a tough question with information that someone was dumb enough to leave out in the open. (Chuckles.)

Doug mentioned I was an attaché in Bulgaria – a long time ago, about 20 years now. Part of that job is immersing yourself in that society. Someone once gave me – the description of a good

attaché is someone who has become so immersed in the society that when he wakes up in the morning, he can sense that something is different today. So in order to be able to do that, in order to immerse yourself, you read the press even if it's the state-run press, you watch television even if it's state-run news shows. You make all kinds of official contacts that you can possibly make. Most of that stuff is a little dry, but in essence it gave me a sense for norm; you know, it gave you a sense as to what the center line was.

Now there was a lot of information there, always freely available, and I collected it in open and sometimes not-so-open ways. But the key was to actually know what to look for and then be in a position to absorb it.

One of the things I did as an attaché – and I realize this is a little bit different than maybe the narrowly defined definition of open source, but I think it has powerful echoes, so I want to share it with you. As an attaché, you are an overt collector. And this was a communist country, a closed state in which attaches were fairly closely watched. But again, you wanted to immerse yourself in that society to learn as much about it as you possibly could.

So one of the things I took to doing is, rather than driving on collection trips in the U.S. government Volvo that we had, I took to taking trains. And so I would get up early in the morning, try to slip out of the house without being observed. I'd take the streetcar down to the train station, buy the ticket that day, get on the train, and then travel across Bulgaria from Sofia to the Black Sea, and then turn around and come back.

Now, that was an attractive route for me because one of the more important things I had to observe was Bulgaria's armored brigades, of which there were five. And many of you probably know tanks are heavy, and they like to move them by rail. So guess where all five tank brigades were. They were all along the main east-west rail lines.

So I would go into the car and immediately go to the dining car and figure out some way that I could stay there beyond the 45-minute limit that was posted at both ends of the car; not because the Bulgarian breakfast food was particularly attractive – (laughter) – but because the dining car had windows on both sides, and that I could observe both sides as we traveled out.

So we get to Varna or Burgas – okay – and my goal there was to be – if I could possibly be invisible, I would have been, but I can't, so I just try to keep my mouth shut, speak as little Bulgarian as I could – ordering things and so on – and, again, trying to be as inconspicuous as possible.

But on the return trip, I change the M.O. On the return trip, I'd done all my observation. On the return trip, I wanted to – back to that verb I used earlier – absorb, but this time I was going to absorb not visually, but socially, and so I would walk the length of the car – multiple cars – looking for that couchette that had the empty seat with seemingly interesting people in all of the other seats.

I can recall one instance where I was walking by a couchette with six seats – five full, one empty. The five individuals in the seats were Bulgarian air force academy cadets – (laughter) –

and I just looked at the seat and said – (in Bulgarian) – is it free? Da. Got away with that without too much of an accent, sat down, pulled my hat down over my eyes, closed my eyes and just sat there.

They were practicing their aviation English. Now the international language of aviation is English, and so if you want to be an aviator, you've got to – you know, you've got to have some working knowledge of English. And so they would be saying some things in Bulgarian and coming back in English or saying some things in English and coming back in Bulgarian. And one of the phrases – one of the phrases they put out was "runway." And there was a long pause because whoever they were asking this of didn't know the answer. So from the – beneath the brim of my hat, this voice – mine – simply said, pista (ph) – (chuckles) – which is the Bulgarian word for runway or racetrack and so on.

And it was one of those Rod Serling kind of moments for those poor cadets. (Laughter.) I identified who I was, so as not to make them vulnerable or at least not to do something they weren't prepared to – well, only volunteered to do, talk to an American. One of them vaporized in an instant. He was gone from the car and I never saw him again. (Laughter.) But the other four stayed there and we spent the rest of the time going into Sofia just talking about life and death and military service and how's the academy and what's your curriculum and what do you intend to fly and how long – how many flight hours do you get? (Laughter.) What's the saddle depth of an SS-21? (Laughter.)

I was doing, back in the mid 1980s, socially, absorbing information that wasn't, in any real sense, protected, information that was available, would we but get ourselves up against it and be able to, again, use that verb, absorb it. In today's world, that information that would have been available 20, 22 years ago, only by this social discourse, is now available in what we call open source, out there in the electronic media in which our species has decided to put almost all known knowledge. And so that experience as an attaché has given me an appreciation of that which we can learn, information readily available, unguarded, not classified, if we would but get ourselves in a position to access it.

I should also add too that those five armor brigades that I wanted to look at from Kniajevo and Sliven and Yambol and Kazalak, okay, they were actually pretty big. They were actually pretty easy to see. Today, the job we have in the Intelligence Community is a lot harder and bit different. The things we want to discover are not out there as the size of an armor brigade. Collection, analysis, dissemination of information is as important as it has ever been. And so your conference here, covering such a broad array of topics including – and I'm happy to see virtually every stakeholder in the open source enterprise here – makes abundantly clear that the rich potential, far reach, and real impact of open source intelligence has finally been embraced.

Now, it's something I appreciated even before that tour in Bulgaria and I've tried to carry it forth ever since. A little over three years ago, as Doug suggested, a small group of us sat down to figure out what the new Intelligence Community might look at under the newly created Director of National Intelligence John Negroponte. John was at the DNI and I was his deputy. We set up a shop just a few blocks from here in the Old Executive Office Building and literally taped blank sheets of butcher paper all along the wall of the temporary office we had been given. And I

mean – you know, we used the pages, blank as a metaphor. This was not a metaphor – (chuckles) – okay? The pages were blank. And how did we want to structure this community?

There's a lot to think through. But it didn't take us long to identify the way ahead for open source. In fact, we saw the establishment of this center, the Open Source Center, as one of the three most important objectives for the ODNI in its first year. The other two? The National Clandestine Service at CIA, second, the National Security Branch at FBI, and, third, a more autonomous Open Source Center for the Intelligence Community. We considered a couple of options for creating this center. But at the end of the day, we decided that voting on the expertise and the capacities of the Foreign Broadcast Information Service and placing the center in CIA made the most sense. FBIS represented the strongest foundation on which we could build, with capabilities that were already out there, ranging from media and Internet collection to research and analysis to advanced I.T., database acquisition and training. And keeping it in CIA allowed the Open Source Center to focus on mission while CIA handled most of the housekeeping chores that would come about from any such organization.

So the aim from the start has been to build and strengthen those capabilities that already existed and then extend their reach. And as I said, we made the Director of CIA the executive agent for open source. I'd be responsible for the center's success, not just in such traditional roles as collector and analyzer and disseminator, but in a new, broader role of community leader working to expand the open source discipline. Let me make sure we understand that distinction. The Open Source Center was designed to be a production line in terms of the creation of knowledge of use to American policy-makers. But it was also designed to be an advocate, a spokesman, a facilitator for the open source enterprise for the open source discipline beyond the fence line, beyond the confines of the Open Source Center itself.

I don't offer this bit of history as some sort of a lesson in the IC wiring diagram. I want you simply to recognize that open source intelligence is widely seen as both an essential capability and a formal asset in our national security infrastructure. As the DNI's strategic plan puts it, and I'm quoting here now, "No aspect of collection requires greater consideration or holds more promise than open source." Here's why. Those working in this discipline are at the nexus, right now, of two intensely powerful dynamic forces: the media and information technology.

And while the Internet has revolutionized human interaction, there is still an awful lot for us to learn about it and the opportunity that it now represents. Finally, the questions our customers ask, whether it's a policy-maker or military commander or law-enforcement official demand answers, many of which are only available through open source research.

So when I became Director of CIA, one of the first things I did was to make Doug a direct report to me. So Doug, in the org chart, is up there with the DI and the head of the National Clandestine Service, the Director of Support, and the Director of Science and Technology. And early in my tenure I think Steve Kappes and I – Steve is the Deputy – had gone a bit public with the number of installations, the number of partners we visited. Steve and I have been to more than 50 liaison partners in about a two-year time period.

In addition to that, we made a special effort to visit the outposts in the open source enterprise as well, and I think I've got four of those already in terms of notches on my belt. One stop that meant a great deal to me was designed to be a courtesy call. I was in Key West, not on business. (Chuckles.) And there is an open source facility there that looks at that island about 90 miles just off the southern marker buoy there.

It was going to be a 20-minute courtesy call. I was there for three hours because, talk about time on target, the people in this little cinderblock shack on the extreme southern reaches of Key West knew so much about what was happening in Cuba. And for me as the Director of CIA to sit with them and watch Cuban soap operas and have them tell me what they were extracting from watching these soap operas was quite remarkable.

They gave me a videotape, DVD, of a program that they had captured from the Internet. And it had a Cuban soap-opera star starring in it, and there are only two other players. And his name is Nicanor (sp) and he's making a fine brew of coffee and there's a knock at his door. And it's two individuals from the security service to install the microphones. (Laughter.)

We're here to install the microphones. He says, what do you mean, microphones? And it goes for about 17 minutes of some of the most subtle satiric commentary on a totalitarian state I have ever seen. He mentions that – they have to decide where to put the microphones and they can't put them in the kitchen because it's too noisy and the bedroom air conditioner interferes with it. So, finally, they say, we have to put the microphones in the bathroom. (Laughter.)

So he says, when I criticize the government, I must go into the bathroom? (Laughter.) And he said, why don't we put another microphone over here? And then they begin to criticize him. What kind of person are you? There are only a limited number of microphones in Cuba! (Laughter.) There's a family down the street that criticizes the government day and night. They have 11 kids and they're only allotted one microphone.

It gave me a new appreciation for life and thought and the situation on the island. And, again, back to riding trains to Kazanlak, it's out there; it's available, but you have to access. And you access that truth in a way that's different from running agents against a foreign government. Now, given that importance to this discipline, Doug sits at my staff meetings each time they occur, and that's three days a week. Open source has a seat at the table, a seat at the table with every other core discipline that comprises the Central Intelligence Agency. We think it's a key component of our own strategic blueprint, which we call our strategic intent; that's how important we think this is.

Now, as I indicated a few minutes ago, my job as executive agent for the Open Source Center is to help it achieve those two primary goals: one, a highly effective collector and producer in its own right, the production line; and, second, to be a catalyst for the larger community, for the open source enterprise about which you heard Doug talk about yesterday.

So how are we doing? Well, one irony of working the open source side of the intelligence business, not unlike every other part of the intelligence business, is that the better we do, the less

we can talk about it. We are often addressing requirements or questions that are sensitive by nature. The information is unclassified, our interest in it is not.

Open source, by the way, is now routinely packaged with the other ints in making our products out of our DI. And I can assure you that on a recurring basis, you see open source material – cited as open source – in items in the President's Daily Brief. It's also true that, from time to time, there are items in the President's Daily Brief that are exclusively derived from open source and carry the logo not of DIA or NSA or CIA, but carry the logo to the President of the Open Source Center.

It contributes open source intelligence to national security in unique and valuable ways. Take recent events – take this jump-ball, Russia-Georgia and now think about how open source could contribute to that. How about what's going on in Pakistan? Think how open source can contribute to that and I think you have a pretty good idea of the kinds of things that open source can offer all of us. It's invaluable. We couldn't claim to do all-source analysis.

How can you be all-source, which is what we claim to be, if Doug and his folks are not part of our team? And that's a baseline that helps us to find, by the way, what's truly secret, what is not accessible in these ways, and allows us better to focus our espionage energy on those things.

Open source also helps us understand how others view the world. Without that understanding, we'd fail in our obligation to provide insight, not just information, but insight. Last spring, I was out at the Kansas State University as part of their Landon Lecture Series. And one of the points I wanted the students to take away from my time with them was how crucial it was for us as a nation to understand others, to understand others' viewpoints, friends and adversaries. We can't be myopic, see things only through an American lens. It's arrogant, but it's worse than arrogant; it's dangerous. The lecture out at Kansas State focused on the growing complexity of the world and the fact that international relations in this century will be shaped by a greater number and more diverse set of actors than they were in the last century. And the overriding challenges presented to those of us responsible for national security is that we now must do a far better job understanding cultures, histories, religions, and traditions that are not our own, or at least are not as represented even in our immigrant nation as much as our traditional cultures have been.

Open source officers have an important role in giving us that window. They expose us to perspectives we might not otherwise see. They broaden our understanding of the world. That's fundamental to our mission. Now, let me talk for a minute about goal number two, you know, the advocate, the sponsor, the facilitator, the responsibility to lead the community in unleashing the full potential of open source.

We can be proud. We've made progress here as well. Some examples – Open Source Center now provides the White House Situation Room with 340 real-time feeds from televisions broadcasts around the world. It provides data that highlights to our commands like EUCOM through a customized Internet portal. It's formed new collaborative relationships with foreign partners.

Remember the comment I mentioned where Hayden and Kappes went out there and visited 50 liaison partners? In several of those instances, the takeaway, the thing we brought home, was a new relationship between their open source enterprise and our open source enterprise as well. We're taking advantage of expertise across the spectrum from NGA headquarters in Bethesda to the Foreign Military Studies office at Fort Leavenworth, Kansas, to the Asian studies detachment at Camp Zama, Japan.

Open Source Center is expanding its training from officers across the community. Half of the Open Source Academy students this year work for organizations other than the Central Intelligence Agency. Perhaps most importantly, the center is making more intelligence-related content available to more people in government than ever before.

Fifteen thousand people, state and local, Congress, policy-makers regularly use opensource.gov. Now, we want to build on that momentum, and that's what drove the action plan that I know Doug's already talked to you about. It's strategic in nature, but he and I have talked. This isn't about moon-shots or dreams; it's about practical, near-term, incremental objectives. I think we've set the path and now it's simply time to execute.

Now, one of the things we're going to do to help Doug execute is to change governance a bit for the open source enterprise, not the center, but the open source enterprise. So today I'd like to tell you a bit about the creation of a new community-wide governance board that will guide us as we move forward. The Open Source Board of Governors will consist primarily of open source producers and stakeholders throughout the Intelligence Community. And what we want to be able to do is to lead an integrated approach to exploiting openly available information. The board of governors will set strategies and priorities for the open source enterprise based on the input from all who want to ensure its success.

We see this board of governors as a forum where consensus can be reached on how best to use our collective resources today and in the future. It will consider things like IT strategy and IT policy. How do we wire up together? The centralization of services, services of common concern like training or content-acquisition, things like standardization, standardization of tradecraft. The idea is to set direction and priorities in a way that allow each of the players, each of the elements of the open source enterprise to develop and make the most of their capabilities.

We've had this for the past year for one of the other functions at CIA. In addition to being the executive agent for the Open Source Center, I am the national HUMINT manager. In that hat, we have a national HUMINT board of governors in which anyone who's collecting information from our species has a seat at the table. And we have been able, through consensus, to develop a set of priorities and standards that we will be able to use across the board in human intelligence collection and reporting.

Well, why can't we do that in open source as well? The open source board will meet quarterly. The first session will take place before the end of the year and at that meeting, we'll set a work plan for the coming calendar year with key milestones and decision points.

Now, yesterday, as I know all of you know, we marked a solemn anniversary, seven years since the attack on our homeland. That one terrible day prompted action across our community on many levels. And I think the IC, the Intelligence Community, can be proud of the work that it's done in the last seven years. Together with partners across our country and across the world, we have kept the United States safe.

But we owe it to our people, the American people, never to be fully satisfied with the job we're doing. We owe it to them to constantly ask the question, how can we better do this? How can we better achieve our mission? There is abundant evidence that we're asking that question and challenging ourselves now more than ever in the open source arena.

So I'm delighted to be here today. I'm even more delighted to see you here today representing the organizations of which you are a part, but maybe more fundamentally representing the enthusiasm that is now out there for this incredibly important discipline.

Thank you then for your energy and your dedication. It inspires us as we continue to serve our fellow citizens to the best of our ability. And with that, I'd be happy to take any comments or questions you might have in the time remaining to us. Thank you.

(Applause.)

MS. SABRA HORNE (ODNI Senior Advisor for Open Source/Outreach): Thank you so much, General Hayden. We have four questions for you that we've taken from the audience. I'll start with the first one. "This conference sponsored an open source analytic contest, an unclassified mini National Intelligence Estimate, if you will. Why doesn't the IC publish unclassified NIEs that could be subject to the peer review of the open source community?"

DIRECTOR HAYDEN: Okay, what do the other three look like? (Laughter.) I don't know if all of you know this, but even the classified NIEs are subject to peer review. There are outside readers for even the most highly classified National Intelligence Estimates. So that's very important. So in terms of the discipline, even at the highest levels of classification, we do get outsiders to come in and give us a view. So I think that's very important.

I guess the second observation I'd make is that the NIEs are kind of the capstone documents. In fact, in some cases, they're criticize them, looking at Mark here, too capstone, too ethereal. But when they hit the sweet spot, when they bring in all of the threads of information in a digestible body for a policy-maker to actually think and decide on something that's quite important. So I guess what I'd underscore to you there – it's all source. It brings them all in so that the policy-maker can have all of the data that we have available to him in one place.

Now, that is not to undersell the independent analysis that's done in the unclassified world in which we, frankly, shamelessly, try to leverage and exploit in our own classified work.

MS. HORNE: "With respect to the phrase 'Open source is good,' do you believe open source is a double-edged sword? We need to always understand how adversaries can use our open source information against us. And what is being done about this problem?"

DIRECTOR HAYDEN: Yeah. Every intelligence discipline has the challenge you just described. Vince Fragamini (sp) was my deputy when I became a brigadier and I was the EUCOM J-2. And Vince was a career Navy Intelligence Officer. He had run their intel school down at Dam Neck before he came out to Stuttgart to be the J-2. Vince had a great phrase: live by SIGINT, die by SIGINT. (Laughter.) And it wasn't designed to be critical of SIGINT, it's just that SIGINT has the tendency to be out there on your breaking-edge news so you get the SIGINT report and Vince had another phrase: when in doubt, put it out, okay? (Laughter.) But then he would always remind me: live by SIGINT, die by SIGINT.

And I guess what I'm trying to describe for you is the problem of deception is present in every intelligence discipline, whether you're listening to someone, whether you're observing someone or something, or whether you're meeting with someone personally. And it doesn't have to be deception in terms of being intentional. This guy may be giving his impression of a meeting. How many of you had that guy talk to you, okay? The guy gave you an impression of the meeting which is at total variance with everyone else who was in the room?

Well, when we intercept that conversation, that becomes intelligence and we report on it in the same way in which we would be looking at that individual's remarks were he giving them at a press conference following the aforementioned meeting. So this problem of sorting through is present in all of our disciplines so I think what I'd suggest to you is, open source, just like every other stream of intelligence available to us, has to be vetted and has to be bumped up one against the other in order to find out the best version of truth.

MS. HORNE: "We've spoken of the importance and key role of open source. Within the CIA, the unclassified resources, infrastructure, and support has lagged behind the classified. How will the CIA put the unclassified and open source infrastructure on equal footing?"

DIRECTOR HAYDEN: It's challenge, you know, truth in lending among friends, these are not easy budget decisions, but we have made the commitment to strengthen this discipline. And I should add, too, this discipline's budget is set off for special scrutiny, set off from the rest of CIA's budget so that it is visible and observed not just by me, but by people north of me in the organization chart.

Now, we recognize that this does require investment. Somewhat like the SIGINT enterprise, which I was familiar with in my time at NSA, you really need an awful lot of computational power and IT and storage to handle the kinds of volume we now get in American SIGINT and which Doug now has to deal with in American open source reporting. So it requires investment. We're committed to that, but it's a balancing act; a little more over here means a little less over there. We just have to do the best we can.

I should add, too, we do recognize we're digging out of a deficit here. This is probably one discipline in which we have underinvested and we have to play some catch-up.

MS. HORNE: And, finally, "How do we encourage more experiences like your Bulgarian open source experience?"

DIRECTOR HAYDEN: One of the things we're doing – and we're very serious about this – we're trying to shove our analysts out the door, off of Langley, and push them forward. So a significant fraction of our analytic workforce now does its work – I mean, it does what it would be doing at CIA Headquarters, but it's not doing it at CIA Headquarters; it's doing it at forward locations.

Now, a lot of those would be in Iraq or Afghanistan in direct support of what's going on there. But there's also an awful lot who are not there, that are in other locations and the idea there is, well, to step back and put this into a second context. Half of our analysts have been hired in the last six years. So I go to Michael Morell or John Kringen and before him and say, we need more experience in our analytic workforce.

And I'm accustomed, as a former GI, you know, I know how long it takes America's Army to build a battalion commander; it takes 18 to 19 years, then someone is a lieutenant colonel and he's ready to command a battalion. So I go to Michael or to John and say, how long would it take to build us an analyst with 20 years experience? (Laughter.)

And the answer they come back with is frankly unacceptable. (Laughter.) We have found, pushing analysts forward into the area in which they report, the things they think about, accelerates this experiential curve. And why does it accelerate the experiential curve? Because the first newspaper they read in the morning is a local newspaper in the local language; the last thing they look at, at night before they go to bed is the local news in the local language. They know whether things are comfortable or uncomfortable, the population is tight or relaxed because they're on the metro with them, I mean, all of those things that an attaché can absorb, we're trying to do that for our analysts as well.

So I think, in its own way, perhaps indirectly, it's doing that kind of acculturation that I underwent when I was serving in Sofia back in the 1980s.

Thanks very much.

(Applause.)

MS. HORNE: Thank you, General Hayden, for your comments. And we especially appreciate your appreciation and advocacy for open source.

Thank you.

(END)

**Remarks and Q&A by the Christine McKeown**
**Office of the Under Secretary of Defense for Intelligence**

**DNI Open Source Conference 2008**
**Washington, DC**

---

DAN BUTLER: Good morning. I'm Dan Butler, the acting assistant deputy DNI for Open Source. Welcome again to the second day of our conference. It's my pleasure today to introduce our speaker – our keynote speaker from the Department of Defense from the Office of the Undersecretary of Defense for Intelligence. Ms. Christine McKeown, our speaker, is the associate deputy undersecretary of defense responsible for analytic concepts and strategies in the office of the USDI. That includes being responsible as the DOD analytic mission manager. She was the DIA rep to the National Geospatial Intelligence Agency. She's been a senior executive at DIA since 1998, and her experience, as you can tell from reading her biography in your program, is deep and broad. She has a breadth of experience in plans, programs, operations and strategic analysis, with particular emphasis on the Middle East and South Asia.

She's been a terrific partner with us in the Office of the DNI, particularly since she assumed this new position and really began to focus in on the importance of open source intelligence for the Department of Defense enterprise. When Christine moved into this role, one of the first things she did was she recognized the importance in our intelligence community, in our national security bureaucracy of codifying important requirements, and codifying those in a strategic context. And for the first time ever, the value, the importance of open source intelligence was included, thanks to Christine's efforts, in the Defense Intelligence Strategy and, subsequently, in the Defense Intelligence Guidance.

Christine is an important leader in the Department of Defense and our national security community. She's an important force within the open source enterprise or enterprises. She's a fantastic colleague, and I'm very pleased to introduce her today as your keynote speaker for the Department of Defense, Ms. Christine McKeown.

(Applause.)

CHRISTINE MCKEOWN: Good morning. How's everybody doing today?

AUDIENCE: Great.

MS. MCKEOWN: Boy, these lights are really, really bright up here, aren't they? Okay, Dan, thanks very much for that really kind introduction. I'm really pleased to be here today, and I'm glad that while Dan talked about my experience at least he didn't talk about how long I've been doing this, which is actually a pretty long time.

Well, it's really a pleasure to be here today and speak to all of you at this DNI Open Source conference, and representing the Department of Defense and my boss, the under secretary of defense for intelligence, Lieutenant General James R. Clapper, U.S. Air Force retired. I think

General Clapper would probably prefer to be here with all of you rather than doing the pressing national security business that he's involved in the Pentagon today that prevented him from being here.

I know that many of you here in the audience know General Clapper, and for those of you that don't, and for truth in advertising, I have to tell you that I wouldn't place at all in the Clapper look-alike contest. For one thing, I have a lot more hair than he does. (Laughter.) But in the sound-alike category, I believe that I'll take at least an honorable mention today – up to you to judge – because I believe that both of us would deliver the same message to all of you, and that message is the importance of open source to the Department of Defense.

Now, just yesterday I had the opportunity to attend the memorial dedication at the Pentagon for the victims of 9/11, a very touching ceremony and a very nice ceremony. It was especially touching to hear from former Secretary of Defense Rumsfeld and some of the other defense speakers who were there. The memorial officially opened to the public last nigh at 7:00, and I hope that all of you at some point in time will have the opportunity to visit the memorial. The one thing that it did for me, sitting there and attending that ceremony yesterday, was to realize again the value and the importance of everything that we do every day in the Department of Defense. And so if there's one thing that you take away from my comments today as I talk to you this morning, that is I want you to keep in mind that the Department of Defense values open source and values what each and every one of your are doing.

I thought I would start out my comments this morning talking a little bit about the Office of the Under Secretary of Defense for Intelligence. The under secretary really has two primary roles within the Department of Defense. He's the principal staff assistant or advisor to the sec def on matters relating to intelligence, and this includes oversight of the entire defense intelligence enterprise and ensuring that the broader department receives the support that it needs from that enterprise. The under secretary is also dual-hatted as the director of defense intelligence within the Office of the Director of National Intelligence, and this dual-hatted position came about following an agreement in May 2007 between Sec Def Gates and Director of National Intelligence McConnell to create that position.

When General Clapper was confirmed as the second under secretary in April 2007, he adopted organizing principles within the office similar to the DNI, with a strong focus on collection and analysis and mirroring within the USDI the functions being performed by the DDNI for Collection and the DDNI for Analysis. I was asked to take on responsibilities as the senior defense official for all things analytic and to provide oversight and guidance to all defense intelligence analysis and production.

Now, defense intelligence is a critical component of the greater U.S. intelligence enterprise – no surprise to most of you in the audience – and as a subset, this enterprise consists of a variety of different organizations, and I'll walk you though a couple of those this morning. They're combat support agencies such as the Defense Intelligence Agency, defense organizations such as the Defense Security Service, service intelligence centers such as the National Ground Intelligence Center, counterintelligence and security elements, and joint intelligence components for both the joint staff and the combatant commands, or COCOMs.

Now, this enterprise really needs to fit seamlessly into a larger network of activities that serve the entire U.S. government and develop people and systems that can integrate easily into that larger network. Without this, all of us are less efficient with our resources and more prone to duplication of effort – something any of us can ill afford to do anymore.

So, to help better ensure that integration, the undersecretary developed a defense intelligence strategy that really highlights four strategic goals. I'm going to focus on one of those now because I see it as the one that's most intertwined and related to the open source activities you've been talking about for the last two days, and that goal is to extend the full advantage of the U.S. intelligence enterprise to all defense users to ensure timely and accurate decisions and the availability of defense intelligence to the broader U.S. intelligence enterprise. The defense intelligence guidance associated with this goal in the open source realm specifically emphasizes support to the combatant commands, and I quote, "Components shall strengthen open source intelligence collection and analysis and integrate open source into the all-source analytic process, based on mission-related collection and production requirements." Our intent is also to extend defense intelligence capabilities and information to other elements of the U.S. intelligence enterprise.

So, in establishing the four goals in the Defense Intelligence Strategy, and this one that I've just mentioned, our attempt is to be in sync with the DNI's inclusion and emphasis on the national open source enterprise. First, by acknowledging open source exploitation as a foundation for all intelligence disciplines, the DNI has shown a spotlight on this discipline of vast but, I would argue, still underrated potential, and also by defining the National Open Source Enterprise as an enterprise of enterprises with separate but interlocking domains for foreign intelligence, defense, homeland security, and diplomacy, each of which is driven by unique missions and policies. DNI efforts increasingly are focused on areas where these four different domains intersect and expand through collaboration and the sharing of people, tradecraft, and technology.

I'd like to turn now to some specific initiatives that we've undertaken within the Office of the Undersecretary of Defense for intelligence. I mentioned that the undersecretary himself has directed that open source be addressed as a high priority for defense intelligence, and our office has provided the impetus, personnel, and resources to create, at DIA, the Defense Intelligence Open Source Program Office. This program office offers a venue for DOD intelligence components to voice their concerns, prioritize and develop resource plans, and collaborate together to develop solutions to common DOD open source problems.

Our office is also working to raise the priority of open source funding initiatives for defense intelligence through the budget process. We're emphasizing and supporting the proliferation of open source expertise and training at commands, and we're working on giving analysts access to the open source equipment, and tools that they need at their desks to exploit information to be used in their analytic products.

We also have invested in an exchange of open source officers between the DNI Open Source Center and our office. I have a USDI officer embedded at the Open Source Center who serves as the DOD program manager, leveraging the potential for an enhanced collaboration between the

open source center and the combatant commands. And Doug Naquin, director of the Open Source Center, has recently appointed an officer to serve on my staff as General Clapper's personal emissary on open source, and to work on DOD policies and DOD instructions and initiatives to meet the needs of the defense intelligence community.

I'd like to turn now to a second but equally important role that open source plays within the Department of Defense, and that is providing customer support to all spectrums of the department, from operating military forces in Iraq and Afghanistan, to combatant commanders and to the most senior policy-makers within the Office of the Secretary of Defense and the secretary himself.

I'd like to take a few minutes to highlight some success stories in leveraging open source at the commands in particular, and I'm going to start out with AFRICOM. The Open Source Center is dedicating the most comprehensive open source support to AFRICOM of any combatant command. This concept has been developing as AFRICOM has been standing up this year, and it will serve as a model in developing support to additional DOD components in the future as resources permit. AFRICOM's commander, General Ward, personally uses a tool developed by the Open Source Center to inform himself every day about developments in his AOR, and he has praised this tool highly. The media tracker is an analytic tool that graphically displays varying African reactions to the command.

I had an opportunity earlier this year to meet with Vice Admiral Moeller, who happened to be here in town for a visit and was meeting with some of the African intelligence community analysts, and he also personally cited the importance of open source in the business that they're doing as they stand up AFRICOM.

The Open Source Center is working closely with AFRICOM to build its cadre and staff. They've maintained a continuous presence there with the stand up of AFRICOM for the past eight months and are poised to begin deploying a team of fulltime personnel to the command – a senior representative, an open source officer, a geographer, and a librarian. And about a year ago OpenSource.gov developed a special portal containing AFRICOM-related open source information. The center also plans soon to commence production of a daily open source product on Africa.

Next I'd like to turn to the Southern Command, or SOUTHCOM, in Latin America. The Open Source Center forward deployed an officer to SOUTHCOM about a year ago this month. This was the first of the combatant commands to receive a permanent open source officer, and that officer has improved current and in-the-works analytic training on innovative open source tools. Because of the demonstrated success at SOUTHCOM, the Open Source Center is now considering forward deployments elsewhere, and AFRICOM, that I already mentioned, is certainly an example of that. Now, it's my job to make sure that the other commands – CENTCOM, EUCOM, PACOM in particular, are also getting the support that they need from the Open Source Center.

During the past year at SOUTHCOM, the embedded open source officer's knowledge of SOUTHCOM priorities has been leveraged to help assist them tailor collection and analytic

efforts, and to address open source gaps for the command. The center created a Bolivia portal on the America's page of OpenSource.gov, featuring open source materials that were useful to U.S. government personnel in theater and elsewhere during floods late last year.

Next I'd like to turn to the Pacific Command. The Open Source Center and the Asian Studies Detachment at Camp Zama in Japan have formed a partnership that has resulted in broader dissemination of open source information on targets of common interest and the development of mechanisms to expand expertise and eliminate duplication of effort. There have been periodic analytic exchanges between the detachment and some of the bureaus in Okinawa, Bangkok and Seoul, as another example.

I'd like to talk now about some specific examples. The Asian Studies Detachment was cited as providing relevant and timely open source products throughout Joint Task Force Caring Response, which was a humanitarian relief effort and assistance operations in Burma following devastation from a tropical cyclone. And the assistant chief of staff for intelligence, headquarters Marine Forces Pacific, stated the following – and I quote – "Open source support to JTF Caring Response has been nothing short of superb. I never thought I'd see the day when open source was able to provide that level of tailored support, and I was wrong. At the JTF headquarters, your products were the backbone, the must-read for the entire chain of command, as well as the basis for daily intel briefs."

Next I'd like to turn to the European Command. This spring the Open Source Center learned that the commander himself wanted tailored open source support. In response, the Vienna Bureau set up a tailored page on OpenSource.gov, addressing EUCOM customers' priorities, and to tailor support further, the Europe program now produces and disseminates and one-to-two page daily open source product call the EUCOM Daily Headlights, and feedback from leadership officials at EUCOM and analysts at the command has been very positive.

I'd now like to turn to the Army and the Foreign Military Studies Office. I had the opportunity in late August a few weeks ago now to visit the Foreign Military Studies Office in Fort Leavenworth, Kansas. I observed, in progress, the Open Source training that the Army conducts once a month that complements courses offered by the DNI Open Source Academy. The course has trained more than 700 intelligence community and military open source analysts. It is accredited by the Army and also by the Department of Defense, and validated by the National Open Source Committee as fulfilling the requirements for foundational training in open source.

The Foreign Military Studies Office also has a border security team that reports two to three times a week on military and security issues from Mexico, Central America, the Caribbean, and Canadian perspectives, which is based wholly on foreign media sources. This effort complements efforts at the Open Source Center and the products are then replicated for all of you on OpenSource.gov. This team and the reports that they're doing are widely used, and they constitute more than 40 percent of the content in the Department of Justice's National Intelligence Center. They have a Counternarcotics Publications Quarterly. And the reports have provided tipping information for federal law enforcement agency investigations and apprehensions.

I would be remiss today if I told you that everything is working well, because it is not. We still face a number of challenges in the open source arena, not the least of which is moving open source out of the closet as an afterthought, and to making it an integral "int" discipline within all of our strategic planning and implementation. I ask all of you this morning, is open source standalone discipline or not? Are we treating it as a source of first report or are we still turning to, and more importantly, funding other ints first before investing in open source?

Within the Department of Defense, we face some specific and unique challenges. The single-biggest challenge within the department stems from the vast quantity and diversity of components that we represent. Our customers range from the pointy end of the spear in Iraq and Afghanistan to senior decision-makers in the Office of the Secretary of Defense, and we must make sure that we are not misleading them on our ability to deliver open source information to them.

Another major challenge is that each command has unique requirements in terms of embedded open source support. I talked about this earlier and I believe we need to work closer with the Open Source Center to develop a proof of concept on how we can do that support and tailor it to each command's specific needs. We also have an insatiable appetite in the department for open source information, and that appetite is exponentially expanding. The Open Source Center is doing everything it can to meet the overwhelming number of the department's requirements, but there are still many that are not being addressed, and the net result is that sometimes during crisis, such as happened recently during Russia and Georgia, because of timelines between the areas where these crises are going on and timelines back here in Washington, we don't always have time to reach all the way back here to Washington and find ourselves working directly through bureaus.

Now, perhaps our expectations within the department are exceeding the Open Source Center's ability to deliver. This is an issue we need to work on together so we can find ways of dealing with the best proliferation of Open Source materials, made possible by the Internet, and going beyond traditional print and broadcast media.

I'd like to close after just talking a minute about the way ahead. The challenges that I've articulated this morning are going to dominate the horizon for all of us during the foreseeable future, and securing adequate open source funding in a time when we all believe that there is – we know that there is increasing competition for resources, it's going to be tough. Currently our primary emphasis within the department is on the Defense Intelligence Enterprise and the combatant commands, but I recognize we must also stay tuned to the needs of the broader department and to the broader intelligence community as well. Under the auspices of the undersecretary of defense, we are doing our part to grapple with these challenges and ensure success, not only for the department but also for the entire U.S. government. Together we need to focus on those areas that will maximize the benefit to the greater open source enterprise while facilitating the work of all of you who are developing capabilities.

And in closing I'd like to remind you of my bottom line up front, which is to keep in mind that the Department of Defense values open source and we need the assistance of each and every one

of you. Thank you for the opportunity to speak with you today. And I don't know if I have time to take one or two questions before I turn the podium over to General Hayden.

So just give me a minute and I'm going to take a look through these questions and see if I can take one or two or if there are a couple of them that – okay, so someone – oh, this one says it's marked for the CIA director, so maybe that one – I don't have to answer that one. That's a good thing. (Laughter.) So I'm going to leave that one up here for General Hayden when he comes up.

Okay, well, I'm going to take this one because this is an easy one, and then we'll see if there's a hard one I can take. Here's another one that's marked for Director Hayden. "You mentioned that the Department of Defense is committed to the exploitation of open source. Please provide the DIA point of contact who can help address the problems and restrictions that prevent DOD organizations from effectively exploiting open source." Well, I'm going to give you a couple of names, and if anybody wants to talk to me afterwards or meet any of these individuals, let's see if we can work that out.

Ellen Tudesco is the DOD program manager for the Defense Intelligence Open Source Program Office. I know she's here today. Pamela Dobson (sp) is my USDI employee who's embedded in the Open Source Center. I know Pamela is here as well. And Wanda Meyer-Price (sp) is the new open source officer who will be coming to work in my office at the Pentagon, and Wanda's here as well. So if you need any additional contact information, please come speak to one of us afterwards.

Here's a question about EO 12333. "Has EO 12333 finally settled the relationship between the DNI and the secretary of defense?" I don't know whether I would call that an open source question, but I would certainly say that the signing of EO 12333 is probably – everyone exhaled a sigh of relief. There was a joke going around Washington that if people had had to coordinate on the original EO 12333, nobody would have done that. So I think most of us are glad that it has been signed and now we can move on to focus on business.

And I think with that, I'm going to finish and, again, say thanks to all of you for being here today. Thank you for everything that you do on behalf of the open-source community and good luck with the rest of your conference today.

(Applause.)

(END)

**Remarks and Q&A by the Director of the Open Source Center**
**Mr. Doug Naquin**

**DNI Open Source Conference 2008**
**Washington, DC**

---

SABRA HORNE: Good afternoon, everyone. Welcome back from lunch. I hope you've had a wonderful, relaxed morning talking with your colleagues and peers about incredibly exciting open-source ideas, because those of us who are zealots believe that's what we should be doing.

So we're excited to have a wonderful presentation coming up, the "Building of the Open Source Enterprise."

But before we do, I have a few administrative things to ask of you, please. Those of you in state and local law enforcement, if you're carrying firearms, we do need you to check these items at the door, so please get up en masse before we all get in trouble.

Secondly, in regards to the Q&A sessions in the panels, we do want us to be respectful of our colleagues, so remember that a question is short, to the point, and ends with a question mark. (Laughter.)

And finally, we have heard the deafening roar about the Open Source challenge. We hear that you cannot wait any longer to hear the results of this wonderful contest. So we would like to introduce to your our two fabulous selected entrants for the open-source challenge. This was actually a really incredibly exciting event for us. It took nine days, nine hard, long days of work on the part of a lot of people. Could we queue that slide, please? The next slide. Thank you. Well, that – we'll go straight to that slide. We had wonderful judges who helped us in the process, but we did end up with two excellent entries that ended up being by far the best that we saw. They exhibited creativity. The solutions were right on point. They were very interesting concepts about how they utilized open-source resources. And we felt like they stood head and shoulders above the rest.

So we would like to offer our hearty congratulations and bragging rights to, first of all, lead POC on the first project, Robert Hybel (sp) including Michael Beddler (sp), Shannon Ferrucci, Raymond Waisco (sp), Andrew Bracefield (sp), Chris Hypner (sp), Daniel Summerville (sp) from Mercyhurst. Congratulations. (Applause.)

And also, we had a wonderful submission from iJET. The lead was Eric Boger (sp), also Andrew Chester, Bradley Perry, Kay Felingham (sp) and Bruce McIndoe. Congratulations to you all. (Applause.)

Next we'd like to welcome Doug Naquin from the Open Source Center. You are all quite familiar with Doug who is the leader at the Open Source Center, one of our most wonderful open-source capabilities within the intelligence community. Last summer, you heard from Doug speaking about the wonderful capabilities that OSC brings to bear within the community and far

outside its reaches. However, now we'll hear from Doug as chair of the National Open Source Committee, the governance body for the IC's open-source capabilities.

Thank you, Doug. (Applause.)

DOUG NAQUIN: Thank you, Sabra. First, an announcement. Will the people who won the award please see me after my presentation for possible job opportunities?

Actually, I had a speech all written out and planned, and had to tear it up because the bottom line was open source is good, let's go have a drink. So I spent the morning after Mark's presentation rewriting my speech.

Actually, my task this afternoon is twofold. First, I'm pleased to introduce a new community action plan, an approach to coordinating the exploitation of open sources across several domains: foreign intelligence, defense, homeland security and diplomatic that constitute what we henceforth called a community.

Second, we will segue from my presentation to a panel of intelligence, defense, diplomatic, and homeland security representatives who are the designated open-source leads for their domains.

Now, to provide context, we are now in the third year of the DNI Open Source Center's existence, and more significantly, in assuming a communitywide perspective as to how we can bring open sources to bear more effectively in supporting the variety of organizations, foreign and domestic, charged with protecting our nation's security.

A little less than a year ago, I was invited to speak to a CIA retirees' association about how open source, as an intelligence discipline, has evolved over the past decade. When asked what I wanted to accomplish over the next year – which would be this year – I noted the specific objectives that DNI, OMB, and Congress had defined and support. But I said, the most personally satisfying accomplishment for me, at least in terms of lasting impact, would be to raise the level of discussion around open source, to get beyond the open source is good stipulation and the accurate, perhaps clichéd, characterizations like source of first resort, or quotes like Allen Dulles once said, "Eighty percent of what I need to know comes from open source."

I wanted to help tee up and witness a serious conversation among those who make the actual decisions for the intelligence community about exactly how open sources could and should play into the overall – and integrated as Glenn talked about this morning – intelligence strategy. To address the strategic questions about what is open source's recognized comparative advantage and how we might capitalize on that advantage, what should our next $1 million go toward? And the $1 million after that? What strategic approach should we take: centralized or decentralized? When should the Open Source Center act as enabler for other nascent or autonomous open-source efforts – what we call the teach-to-fish approach – and when should we act as another's end-to-end open-source provider? This is what I mean about raising the level of conversation.

Now, I give great credit to the DNI, DNI staff, and the director of the Central Intelligence Agency, who you'll hear from tomorrow, for creating the conditions to have this conversation. Three years ago, we were still trying to convince people that open source had intelligence value. Now we just have to take advantage of these conditions and institutionalize this conversation so it happens regularly and independently of whether the DNI or the DCIA personally happened to be a champion of open source.

Now, when I spoke to the – now, this conversation is important, and why is it important that the intelligence community be the appropriate venue for this conversation? So I'll see if this clicker works. Okay. Three key points about this slide: one is context. I'm often asked why would an open-source center be the intelligence community? Well, it's really the question of what do you want to support. If you wanted to support corn production, you might put it in the Department of Agriculture. The question here is you put it in the intelligence community because the context is terribly important. Our job, as you can see from the slide, one thing you'll get – you'll see a lot of Venn diagrams today, so you should be confident that all your IC leaders have taken fifth-grade math.

You'll see that our value in the intelligence context gets greater as we move toward the right. So no longer do we just worry about the outer edges of the light blue there, and say we collect a bunch of stuff and we leave it to others to make sense of it, that if we're really going to have intelligence value, we need to start pushing those arrows to the right. There is an open-source element to each of those "ints." If Zawahiri gives a speech, it's unclassified HUMINT. And I can go through examples of we get – buy maps on – cadastral maps of Baghdad on street corners, it's unclassified GEOINT. Also, as you heard this morning, open-source complements these other "ints" by providing tip-offs, verifications, denials, other three-dimensional aspects to an intelligence issue that when combined with these other "ints" has tremendous value. But the further we can push that arrow to the right, the more value that we have. That's why the context is so important.

Second key point is economy of resources and risk. The further we move this to the right, the less we have to spend resources, or the amount of area in the black. Those resources tend to take more resources on the black than does the blue. So the smaller we can make that black area, it doesn't mean you spend fewer resources on the black, but the resources we do spend on the black become much more effectively applied. Risk is the same way. The more we can rely on open sources, theoretically and actually, the less we create risk for the more adventuresome or/and more clandestine areas of intelligence.

Third is impact. Open sources no longer operate solely on the outer edges as fodder for others to analyze, as I mentioned earlier. Many more questions today lend themselves to open-source research and analysis than even five years ago. And two examples were the ones that were used in the open-source challenge. Those are bona fide national security questions that I'm sure somebody has asked, or will ask within the next five years.

When I spoke to the Open Source Conference last July, my role was slightly different than my role is here. Last year, I spoke solely as the head of the DNI Open Source Center, and my focus was on the steps we were taking to build OSC as a hub or catalyst for a larger and integrated

community enterprise. While I'm always happy and proud to talk about the progress OSC has made in this venture, my role today is more to look forward and talk about steps we are taking to adjust community open-source governance so we can focus our collective efforts to make steady and tangible progress against the goals the DNI staff established in 2006, that little red book that Dan talked about this morning.

Specifically, in June, I was asked to assume responsibility for chairing the National Open Source Committee, affectionately called the NOSC. This entailed as the first order of business the development of a strategic action plan. Some might refer to that as an implementation plan or a business plan, that's fine. I use strategic action plan because while the focus is on action and the year ahead, we wanted to ensure that we did not lose the strategic intent behind the action.

So this summer, anchored by a two-day offsite of NOSC members, we put together a succinct but straightforward document as to what the community's goals and objectives are for the next 12 to 18 months. These goals in turn should help drive our investment priorities. And the plan itself is available on Intelink U..

I'll talk about the plan's goals in a minute, but I'd first like to highlight the two underlying principles this plan reflects. Okay. You can't see that really well, but there's another Venn diagram. Trust me. First, while we continue to refer to a National Open Source Enterprise, we've come to realize that in a community that includes foreign intelligence, defense, homeland security and diplomatic missions, we are really talking about an enterprise of enterprises. Each domain, for example, can, and in some cases will, stand as a separate enterprise to align with unique mission requirements and policies.

At the same time, the NOSC will focus on what I call the sweet spot, that spot, that area of yellow, common to all the enterprises or where the experience or expertise of one can benefit the many. Generally, this area entails issues of policies, standards, information technology, cross-agency workflow and training. But that direction remains at the discretion of the DNI. The driver behind the concept of an enterprise of enterprises is to provide as much a common foundation as possible without, one, expecting one solution to meet the needs of all; or two, expecting all to adjust their needs and policies to accommodate one solution.

Second, we are all about integration. On the one hand, there's the integration among those who work in or with open sources across our broad community, greater coordination, acknowledgment of the principle of comparative advantage, and even recognition of centers of excellence will allow us to contribute to the best of our agency's abilities while avoiding necessary duplication. On the other hand, and perhaps even more important, is integration with the other intelligence and perhaps less open disciplines.

While a lot of good open-source work stands well on its own, if you recall my early Venn diagram chart, the value of open-source work increases dramatically if we can focus our efforts so our work complements or enables other disciplines. Those of you who have been following the Internet even at a surface level over the past couple of years know that the volume and variety of openly available information has dramatically changed the landscape of our potential.

But that potential can only be realized if we are, one, focusing on the right things at the right time; and two, delivering our products and services to the right people at the right time.

So getting back to this year's plan, let's have a look at the goals themselves. Now my finger went too fast. All right. One, universal cross-domain access. People do their work in different domains with different classifications. That's a fact. They also want a variety of material, abide by a number of varying policies, and want to go to as few places as possible to deal with an ever increasing volume of potentially helpful material. This is why an architecture that focuses on managing and sharing open-source information is high on our list of priorities. We also believe we can apply much of what we learn on the low side to other domains.

One of the things that we have is that a lot of folks in the intelligence community are focusing their efforts on what we call the high side, trying to – so nobody's paying attention to the low side, which gives us a target rich environment.

Integrated mission management and impact. This goal addresses directly what I call the "so what?". Here we get beyond the "open source is good" cliché and to measurable and meaningful impact. To maximize the impact, open source must be integral to the community in its overall planning and assessment processes. We have made strides in theory in the past couple of years thanks to DNI staff, particularly collection. But we can do more, especially as our enterprise of enterprises matures and grows.

Next, proliferation of open-source expertise. Open source exploitation is prevalent throughout the national security community. And embedded open-source specialists apply unique expertise and support of their respective organizations' missions. This goal acknowledges that a profession specializing in open-source expertise is needed. One of what I call the three ironies of open source holds that as more and more people have access to more and more information, the more important it becomes to take a disciplined approach to skills, tradecraft, methodology, knowledge, and education.

I have experienced first hand that the best way to convince someone they can benefit from open-source expertise is to give them an open-source expert – just one. It doesn't take long for people to see what they've been missing or that they can do better for what they've been buying.

First, we as a community need to develop those experts.

Second, we need to get them or the associated skills training out to the units that need them. For all the technology that we devote to managing the volume and variety of material with which we must deal, the most effective open-source exploitation remains predominantly a human endeavor. Just ask anyone who has had the benefit of working with the trained research librarian or area specialist with one or two foreign languages, counterintelligence training, writing skill and basic knowledge about how networks, operating systems, and various software packages work. They do pretty amazing work on a daily basis.

Last is open-source enterprise governance. Now, governance here is really a misnomer. The NOSC will not presume to tell agencies how to plan, program, or execute their missions, or even

prescribe how to use open sources, rather we will be successful, if we facilitate the right discussions and decisions above us at the strategic level – and I won't say below us – but as well as in the individual agencies. This is what I mean about having the right conversation at the right level. Thus a governance process we are attempting to establish is mostly about communication, coordination and visibility, and not directing people or resources.

If we are successful in establishing a true open-source community that transcends agency and component boundaries, I believe we will not only be doing right by the government on open source, but we will be demonstrating one of the underlying principles of the Intelligence Reform and Terrorism Prevention Act. I further believe that if this can happen anywhere within the national security community, it can happen in open source.

Now, at this juncture, I would like to turn my attention to our panel of community representatives who will talk more about what we mean in managing the sweet spot. So if they could – if my panelists could join me up here, I will introduce them.

First, on the defense side, we have Ms. Ellen Tudisco who is the chief of the Defense Intelligence Open Source Program Office, DIOSPO. She sets defense standards for the collection and sharing of open-source information and serves as the principal advisor to the USDI on the integration of open source and to defense all source analysis.

Next to her is Mrs. Barbara Alexander, who currently works on collection requirements at the Department of Homeland Security. Mrs. Alexander has a broad background in analysis, strategic planning, and programming, information technology and other intelligence community issues acquired over a 25-year career as an intelligence officer for the Defense Intelligence Agency.

Next to her is Dr. James Bell, who is acting director of the Office of Research, Bureau of Intelligence and Research, Department of State. Dr. Bell oversees foreign public and elite opinion research in support of U.S. diplomacy and national security priorities. He also co-chairs an interagency sub-PCC directed at coordinating opinion research in support of U.S. public diplomacy and strategic communication.

And last but not least is Kim Robson. Kim Robson is a National Geospatial Intelligence Agency senior executive serving at the DNI Open Source Center as our deputy director for community integration, where she leads our enterprise partnership program focusing on extending open-source capabilities across the intelligence community.

All right. Now, I have some questions that will get the ball rolling, and then I hope for the session to be interactive and that we at the same time can start taking questions from the audience. So we'll start with Ellen.

Ellen, on DOD. Defense is such a large organization. How do you see DOD addressing open source as a community: centralized, decentralized, or somewhere in between?

ELLEN TUDISCO: Well, Doug, I'd like to start with just a little bit of history. Defense has a rich history in using open-source information and managing it collectively. The Defense

Intelligence Information Support Program has purchased and shared content with DOD and other community members for over 20 years. Defense open-source advocates, users, and practitioners have met in various forums since the late 1990s. Many of these individuals now champion defense needs as members of the National Open Source Committee and its subcommittees. Even a few have served as members of the ADDNI for open-source staff.

Where we're different is how we integrate open source into all source intelligence products. Our defense analysts require access to open source across multiple information domains, from strategic to tactical in order to support national security policy, warning, acquisition, and military operations. So our task now is to make all the investments required to link and interact in an even more robust fashion with a broader open-source enterprise.

Defense is very passionate and vocal about using open source and delivering it to effect. We use it for informing classified intelligence analysis, understanding the socio-cultural dynamics of foreign environments, enabling public affairs activities, facilitating strategic communications, strengthening foreign partnerships, and supporting allied and coalition efforts. Most important, we have witnessed the operational relevance of bringing timely open-source information to the battlefield. We have seen that open source delivers timely information that allows our service men and women to accomplish their missions and to come home safely.

Currently and by default, we take a federated approach to open source that deepens our common purpose among many different defense members. Our Defense Open Source Committee, or DOSC, mirrors the National Open Source Committee with a focus on defense missions and priorities. It's the forum for sharing open source best practices, solving common challenges, and advocating the tools and resources that Defense needs to hone its open-source capabilities. Through this self-governance mechanism we have approved open-source training, developed and taught at the Army's Foreign Military Studies Office as the defense standard.

The DOSC's support for the development and testing of the Open Source Collection, Acquisition and Requirements management system has been key to getting it towards initial operating capability on the 1st of October. We feel that OSCAR is a critical building block for open source that will leverage collection across defense in the broader enterprise and government. OSCAR will develop metrics that measure the depth and breadth of open source's mission and impact and its role in understanding global developments.

DIA, Defense Intelligence Agency, by direction of the undersecretary of defense for intelligence established the Defense Intelligence Open Source Program office in November, 2007. We are charged with developing policy and plans to guide open-source activities.

While open source is not a new discipline within defense, our biggest challenge is defining the programmatic structure to make it coequal with the other collection disciplines, intelligence disciplines. The combat and commands and service intelligence production centers maintain organic open-source capabilities to fulfill their commanders' critical information requirements and priority intelligence needs.

To sustain and to advance this defense open-source capability, we must establish a resource framework that provides the Congress the visibility it needs into our programs, accomplishments and successes to fund this critical defense intelligence requirement. An initial step is to resource vetted professional librarians who can integrate open-source expertise with all source intelligence analysis as well as open-source collection managers trained in OSCAR and the multidiscipline intelligence cycle.

Another goal is to identify current open-source expenditures on data and content for cost savings and efficiencies. We assess that Defense has deep open-source knowledge and experience in the area of science and technology. Out S&T centers, particularly the National Air and Space Intelligence Center, constitute a core capability for the national open-source enterprise.

The National Center for Medical Intelligence developed the information management tools used to create the National Virtual Science and Technology Library. Through this library, the National Defense Intelligence College will make Defense S&T information available through a single portal to authorized users. Within the federated model for open source, Defense must be recognized and resourced as a national repository and disseminator of military science and technology information.

Lastly, the USDI has designated the Defense Intelligence Open Source Program Office as the DOD lead for open-source efforts. In order to oversee this program authoritatively, and to champion effectively DOD's requirements to Congress, this office must be positioned at the Office of the Secretary of Defense. Executive agency at the OSD level will enable defense to unify its open-source plans, policies, and programs and to promote integration of open source across the National Enterprise and with the other collection disciplines.

MR. NAQUIN: Barbara, we see where DHS has developed a strategic plan for domestic open-source enterprise. I just saw the purple book. You stole our color. What are some of the challenges you face in establishing this enterprise? And how do you think the National Enterprise can help?

BARBARA ALEXANDER: Okay. Thank you, Doug. But you're colorblind. It's not really purple. It's our little blue book. And we at DHS are really delighted to present it. It's debuting here at the conference hot off the presses. It was picked up at 5:00 o'clock this morning. One of the key ways that the National Enterprise has helped us is indeed in helping publish the book. It was through the auspices of the DNI staff for which we're really grateful.

Let me talk for a minute about the strategy, the vision, and then answer your questions about some of the challenges we're facing and what we want to do in partnership with the national community.

The strategy, which I hope you'll all pick up – it's at our kiosk and in some of our training sessions – recognizes the imperative for open source in the department. Tomorrow's keynote speaker is Undersecretary Charlie Allen, and he's going to speak to the role that open source plays in the homeland security mission.

It's critical as we deal with a department that is not part of the intelligence community. We have pieces of DHS which belong to the IC, but the preponderance of our 210,000 employees are members of the law enforcement community. And this is critical as we keep this understanding of our constituents and our stakeholders at the forefront of what we do. They depend on open-source information on a daily basis, because they don't work in a SCIF. They don't work at the TS-SCI level. And so it's absolutely vital to helping in defending the nation and meeting their operational needs.

Our customers range from our department policymakers to our operational components, to state and local fusion centers and private sector partners. So you can see the expanse of the mission set that we have and can begin to intuit the importance of open source in supporting their unique missions and unique needs for open-source information.

The open-source information that we provide to them, homeland security open-source information, is different from the open-source information that has a foreign basis that's provided by the Open Source Center or by the other members of the IC and their open-source activities. Our DHS authorities allow us to provide domestically relevant open-source information that the rest of the IC is prohibited by law from providing. And so we, in our program, are attempting to be responsive to the homeland security issues and the needs of our particular stakeholders.

Our vision, our little blue book, is consistent with the direction of the National Open Source Enterprise. In fact, we patterned our strategic vision against the goals and objectives that were laid out in the little red book. There's no sense in reinventing the wheel, and even more importantly, we want to work together in partnership with the national community. We recognize our participation in what Doug has wisely called the enterprise of enterprises. It's a great term and we're using it all the time.

We actually engaged our colleagues on the NOSC, the National Open Source Committee, when we were developing the strategy, asked them for their input. We engaged with our congressional partners and presented our draft to them and solicited their advice recognizing the expertise that the congressional staffs have in this area as well. We're committed to working together to get best practices across the community. And it's helpful that so many of us have worked together for so many years.

The vision not only is consistent with the NOSC, but it recognizes I&A, intelligence and analysis, as the center of gravity for open-source intelligence for homeland security, law enforcement, and the first preventer communities. It commits us to developing a framework in governance for our DHS open-source activities, building a trained workforce and representing the department's communities on the NOSC, so you see again the interaction that we have.

It recognizes the criticality of civil rights and privacy issues, and it directs our DHS open-source enterprise to train our workforce all across the department and with our partners in these critical areas that are somewhat unique in the homeland security environment. It lays out the goal of information sharing for our products, and it seeks to integrate the existing information dissemination platforms that we have in the community to facilitate collaboration. It commits us

to capitalize on emerging techniques and methodologies and tradecraft and technology. And all of these are areas I think where we will turn to the national enterprise to help us as we continue to flesh out this activity.

What this is doing for us is providing the framework upon which our implementation strategy then is built, and allows us to keep focused as we develop the open-source program.

We've made some significant steps already. We've, as I said, engaged with the enterprise and the NOSC. We've developed an investment plan which we've presented to Doug as the chair of the National Open Source Committee. We have a structure identified for governance within our Homeland Security Intelligence Council structure. We've done a lot of training at our state and local fusion centers.

I'll put a plug in for some of the training that's ongoing in the breakout sessions. If you're coming from a state and local fusion center, I encourage you to stop by and participate in these information sessions. We've done 16 with mobile training teams, and Undersecretary Allen is committed to training all of our state and local fusion centers over the next year or so. We also have developed online training modules for open-source information which are getting great reviews and are highly acclaimed.

We have a lot more to do. We have a lot of challenges. Part of it is that the department is new. It's only five years old, and so our open-source program is nascent but it is growing by leaps and bounds. In fact, we are getting more requirements for open-source acquisition than we have the resources to address, and so that's one area that we're going to be looking to the national community for assistance. We have already received resources from the assistant DNI for open source, and we are beginning to use those to fill some of our critical positions. And we're working closely with the DNI on sharing methodologies and tools and information platforms in order to again leverage what is already existing, and use our scarce resources wisely.

Another challenge, again going to the fact that our stakeholders are not part of the IC, is helping to be that facilitator between understanding what the intelligence community is, and for the members of the IC explaining what the homeland security community is. And we're trying to be the bridge between those two.

So what are we expecting from you? As I said, leveraging the expertise and the capability that has been built up over the many years with the Open Source Center. We have a great relationship with our partners on the committee, at the subcommittee level, and we are leveraging the tools that the DNI is putting is putting into place for the National Open Source Enterprise. We want to raise the level of expertise at our state and local fusion centers with the analysts there so that they understand the best use of open-source techniques.

And as appropriate, we want to be able to engage the Open Source Center and the rest of the national community on foreign open-source information, which actually has a homeland security nexus, so we're building the bridges between those two things in support of the homeland security mission.

MR. NAQUIN: Thanks, Barbara.

Now, Jim, in supporting his diplomatic mission, the State Department operates in a way that straddles intelligence and diplomacy. How does open source fit into this overall?

JAMES BELL: Thanks, Doug. I don't have a blue book. I don't have a red book. I have no book. (Laughter.) So I'm at slight disadvantage. But I do appreciate the opportunity to sit on this panel, and I really appreciate the diagram that Doug shared where we're seeing these four domains with the sweet spot in the middle.

I appreciate it because for the people on this panel, but especially I can speak for myself, INR, where I'm an office director, does exist in two worlds, in two cultures: one is the intelligence culture in the intelligence world, and the other is the world of diplomacy and it has its own culture. And I liked what Barbara was saying about bridges, because that's how I would describe the role of INR at State – as a bridge or facilitator. Bridging that cultural divide that sometimes can be challenging but I believe, personally, that there's actually a lot of advantage to be gained from that kind of bridge.

And having an organization with one foot in the intelligence world and another in another mission, in this case diplomacy in the case of INR, actually brings a lot of advantage for some of the reasons – precise reasons that Barbara alluded to is that we can facilitate communication between those worlds, and bring intelligence to bear, in the case of INR, on diplomacy in a way that is much more meaningful and more effective if we do our job right, and link the intelligence community more effectively with what the consumer's interested in.

In the case of diplomacy, and when it comes to foreign intelligence, one of the largest audiences of consumers, groups of consumers for intelligence, foreign intelligence, are diplomats. So that bridging concept I think is very important, and I think this domain concept is very, very useful.

Now, more directly to answer Doug's question, I'd like to start, as Barbara did, with a little discussion of what is the mission of INR. At INR, we see our mission as directly supporting policymakers and diplomats in order to facilitate the effective conduct of foreign policy. It's that simple. That's our role. We directly support policymakers and diplomats.

Within that mission, what is our focus? Our focus is strategic intelligence, providing the fullest possible situational awareness to policymakers and diplomats so they can do the best job possible of realizing policy priorities and responding to world events.

What is our method? In INR, we emphasize all source analysis, and I know that's a term that's been out there for a while. It was on one of the screens that Doug shared. Within all source analysis, one of our roles, and a key role, is to integrate open sources with other sources to provide timely accurate intelligence to diplomats and policymakers.

So for us, open source is key. Now, INR is both a consumer and a provider of open-source intelligence. And so I'll talk first a little bit about the consuming and then a little bit about the providing.

In terms of consuming, why is open-source intelligence important to INR? And I think we can all imagine reasons why open source matters, and some of them have been mentioned already in this session; I'm sure other sessions of this conference will address them in greater depth. I'm going to run through them very quickly. But I want to emphasize maybe one or two that I think are especially important when I think about how INR can support diplomats and policymakers in the domain of diplomacy.

To begin, open source enriches analysis. It's another source of analysis. And importantly in terms of enriching analysis, it provides an opportunity to triangulate analysis, as I call it, back from my academic days, trying to understand from multiple angles and perspectives what it is we're seeing, understand more fully what is out there, what is happening on the ground in a particular place, at a particular time. You're never going to get a comprehensive picture of every dimension, but a fuller picture is definitely something we should strive for. Open source can help us in that regard.

Besides enriching and triangulating analysis, I agree that open source has elements referring to, can have the ability to provide up-to-date information you might not be able to get anywhere else. And we value that also in the diplomacy mission that we support.

Now, more specific to INR and our support to diplomacy, I feel there are a couple of advantages that really matter. One is that by relying on open source effectively and strategically, we can share analysis more widely or with a broader audience of policymakers and diplomats, and that's something that we take very seriously in INR. We want to get intelligence, intelligence that bears on real world problems, policy priorities to the widest audience possible at State.

Not everyone at State has access to TS-SCI. A lot of them don't. They need information that they can use in their work every day, and our ability to provide them with intelligence that is accurate and timely, but can be used by them wherever they are around the globe, is very critical to our mission. Open source helps us in that regard.

And aligned with that, by providing open-source analysis or using it strategically and effectively to support policymakers and diplomats, we are talking to them at the same level of classification that they live in, which is unclassified most of the time. They need to be active in a public domain. They need to be able to cite and refer to information that is not restricted in terms of access to really achieve the goals that they're charged with achieving. So open source is another advantage in that regard. It relates to the nature of our consumers at the State Department in the diplomacy mission.

So those are some of the key aspects of the consuming side.

When we think about inputs that INR can provide to open source and the open-source community, intelligence community, there're really three areas that I would emphasize, and they all are related to open-source analysis because, again, what INR sees as its key mission is strategic all source analysis. We are analyzers. We are synthesizers. We are the people that translate intelligence, raw and other forms, into meaningful information to provide that decision

advantage that is the theme of this conference because intelligence needs to have that translation going on, and that's the key role of analysis as we see it in INR.

In that regard, there's three areas, as I mentioned. Analytic outreach. This is something that INR has engaged in for many years already, and we see it as something that's directly related to the open-source enterprise and a role that State can play in building the enterprise of enterprises, and building open source in the community.

Recently, the director of national intelligence issued a directive making INR the lead executive agent for analytic outreach in the community, building on the foundation we already had in this regard. And we see this contributing to that mission as well as open source. This means reaching out to academics, experts, NGOs, others who have expert knowledge, insights into key policy issues, key events going on around the globe, and encouraging those people to participate and bring their knowledge to bear on these problems in conjunction with analysts in the community, analysts at State, to provide the best possible intelligence.

What these experts are doing in the public domain is open source. It's out there. They have public roles. We're not asking them to change that dimension. We want to benefit by applying it more directly to particular issues we're interested in. This exchange of ideas enriches intelligence community in terms of what it's trying to achieve, enriches the people at INR, and our support to the State Department policymakers and diplomats improves because of it. So analytic outreach is a key mission, and we see INR as a center for excellence in this regard within the community and look forward to that mission.

In addition, what I'm directly responsible for, monitoring public opinion overseas, both through monitoring public opinion polls as well as commentary in the media, meaning op-eds, mainly, looking at how issues are framed, and more importantly the information environment, the broader strategic environment, in which issues and policies are unfolding or are being reacted to, and understanding that fuller situational awareness so that we can provide that to policymakers and diplomats.

Monitoring public opinion is a key part of that, something that we do in a unique fashion compared to any other part of the IC. We have this role, and we're really happy of the way we've been able to collaborate with the Open Source Center providing that information to the whole community, and the collaboration between the Open Source Center and INR has been a tremendous benefit to us in that regard.

And finally, another key component of our open-source role as a provider is humanitarian crises. We have people dedicated to respond to these kinds of crises synthesizing and integrating information from both the public sphere and the intelligence world to understand completely what's happening when there's a natural or other kind of disaster in the globe, people are displaced, what's going on, on the ground? How can we get a full situational awareness of that? How can we respond most effectively as a government to that kind of situation?

So consumer, provider, we see ourselves as part of that enterprise of enterprises. I think it's a great model, and I really, again, appreciate the notion that we respect that there's different

domains, but they benefit from these bridging organizations like INR and the other ones on the panel to bring these two domains together.

Thanks.

MR. NAQUIN: Thanks, Jim.

Okay. Lastly, Kim, you spent most of your career at NGA, but the last year and a half, you've been deputy within OSC. So from that perspective, and not just because you work in OSC, why do you think the intelligence community, and specifically OSC and CIA, are well positioned to support the DNI in this leadership role?

KIM ROBSON: Well, first, I think it's important to recognize that open source, like all disciplines, derives its value from being delivered in the context of the problem that we're trying to solve. And I believe the intelligence community is uniquely positioned to search and analyze open sources in the context of our nation's key intelligence issues. It's the intelligence community's job to really understand the global intentions, capabilities, and capacities. We observe what's happening, assess why it's happening, and we make assessments as to what will happen next. But this information is only relevant if it helps our nation's leaders make better decisions and act on those decisions.

So at the Open Source Center, we have over 40 years of experience structuring open-source strategies and analyses to target the key strategic and tactical intelligence questions in the IC context. It's that experience that makes us the logical choice to lead the community. And Doug used an example earlier, and maybe a little extreme, that if our largest national intelligence issue was corn production rather than counterterrorism for example, than the nation might be better served by having the open-source leadership in the Department of Agriculture, where they have the context for corn production. But it isn't. The IC is the right context for the highest intelligence priorities, and so it is the right place for the open-source community leadership at this time.

The Open Source Center is also the only open-source organization in government today that really has the critical mass to lead this large enterprise of enterprises. OSC has a global IT infrastructure that's providing a stable foundation upon which to build the broader open-source enterprise.

We also have a worldwide workforce that has very mature business processes. We also have extensive tradecraft experience and a capacity to train and to help other people train. Further, we have the depth and the breadth of the foreign language experience that I've not experienced anywhere else. And we have expertise in working through very complex legal and policy issues that are extremely important that Barbara is working on today as well. And we can take those – the experience that we have and apply them to the next level of problems.

OSC's approach to leadership and view of the National Open Source Committee is for OSC to lead strategic government's activities, while also helping the other organization to grow their expertise, working under their authorities, and supporting their unique missions. This approach

achieves more residual value than by asking any single organization with finite resources and a very focused mission to provide everything as a service to everyone else. So combining the collective talents and efforts of the community has had a unifying effect and it reinforces the attitude that we're all in this together.

From my vantage point, the model is really working well. I have seen an unprecedented increase in open-source awareness and in capabilities across the enterprise, and perhaps, most importantly, open source is starting to be institutionalized with formal plans, explicit budgets, and policy guidance across the various enterprises. NGA has now developed a geospatial open-source strategic action plan. As Barbara mentioned, DHS now has its own strategic plan. This year's Defense Intelligence Guidance specifically calls on open source. So all of these things together means that it's really – it's becoming real. It's not a hobby anymore.

We've also seen major successes in providing economies of scale for the community. The Open Source Academy has provided more training in the past year to community personnel than we had in the previous five years combined. And we're positioned this year to provide even more training and increase those numbers for the community.

We also have over 16 separate commercial databases that are now licensed for the entire intelligence community and through our opensource.gov platform we're brokering data from 100 separate organizations across this enterprise of enterprises, making it available to anybody who has access to those systems.

As a community, we're unifying and we're working well together. Our new strategic action plan is successfully focusing our efforts at the center, as well as the efforts of the broader intelligence community.

I think our biggest challenge right now is to rationalize all these different policies and all the different priorities and missions across the enterprise, and then figure out what is that sweet spot, really focus on that and try to work together in those areas.

But in spite of the challenges, I think the outlook is really positive. The governance structure is solidifying and our community strategic action plan is in place. We have the attention and commitment of our senior leadership, and we also have a team of dedicated senior executives and open-source practitioners who recognize the value and opportunities that open source is creating. And we will be able to create the decision advantage with this construct.

MR. NAQUIN: Thanks, Kim.

Now I think we can open it up to any of the questions that may have been filtered down if anybody has been collecting any. Or we can take them from the audience if you have for either me or any of the panel members.

Q: Thanks. I'm John Newhagen from the University of Maryland. And maybe I'm the last guy in the room to get at, but it seems to me that what I see emerging is more than just saying that you should be going to non-traditional information source, is that – what I see is a kind of an

emerging methodology. Maybe it's the result of an increase in complexity for the information environment. So you can –

MR. NAQUIN: Right. It was so much easier. When I came on – entered on duty, open source was primarily newspapers, radio, and – actually I'm not – I think TV had been invented. But it was radio – (laughter) – and newspapers. And I was primarily translation and we didn't have to worry our pretty little heads about anything else. And now you have blogs, vlogs, chat rooms, YouTube. I have a chart – virtual worlds et cetera. So the world of open sources is much more – much more complex.

From a center standpoint, we addressed this exactly a year ago by establishing what we call an emerging media group. Now, I know it's not emerging. It's here. But the idea is that we were not able to accommodate this new media within our traditional structures. So we did what a lot of companies did. We created a separate organization that could in fact become its own spin off organization if it got enough critical mass. And the effort was to focus not only on exploiting these new media, but on what are the types of questions we can answer that we couldn't have answered two years ago looking at traditional media, plus what methodologies do we have to develop to actually get some kind of foundation or baseline.

So we're addressing, for example, video analyses now. That's not – we should call the new media, but it's a type of analysis that we've never really done, at least within the Open Source Center, that is much different than analyzing word or text. And so those methodologies are coming out of this new group and we won't be able to move this fast I think as the media are, but I think we're at least positioned now to address these much quicker than we were a year ago.

But it is – the other thing – the other point I'd mention, that we're finding as a result a new media, is not just the content of the media. It's what the media are doing in terms of the way people interact with each other. And I think there was a session earlier today on social networking that I wasn't able to be there, but I was told that was fascinating. But it's exactly – it's not just the implications of say blogs in a particular country, but what is the network behind the blog. Who is actually accessing? Where is it center? Where are the activities – it doesn't actually have to be in that country to have a tremendous impact in that country. So all these have implications for intelligence, not just the content, but also what it means in terms of the interaction.

We're addressing this, but it is difficult to keep pace with the way that the media evolve now. I'll acknowledge that.

Maybe you want to –

MS. ROBSON: I'd like to also add that the methodologies of the tradecraft are changing and I also think that the methodology in how we're interacting together across the various communities are changing as well. And I believe that the model that we are implementing right now very successfully is the model that the 9/11 Commission had in mind when they issued their results. We are really working together. We are not competing with one another. We recognize that this is the way it was supposed to be and intended to be.

MR. NAQUIN: Yes, we often go out with the call, does anybody know anything about this? And we're looking for that expertise no matter where it resides. And sometimes it's in academia. Then we just have to – we're staying legal with regards to working with academia. But we are definitely following what I call the "I'm not proud" approach. It's – generally we're looking for best expertise resides or the best capabilities and then bring them to bear. And we can do that on the unclassified domain a little bit more easily than we can in others.

Q: Hi, John Vaughn (sp) – (inaudible) – Solutions. I've been an open-source analyst for the past three years now, and I have realized the more technical I become, the better I am at my job. My question for you is do you feel the skill sets and the background required to be an open-source analyst is evolving and what might that look like.

MR. NAQUIN: Absolutely. I have talked about this at some length. I won't go too much into the history, but just in the past decade, when we hired open-source professionals, we focused on three areas. One, librarians; two, geographers; and three, people with language – foreign language critical thinking and writing ability. This was our vision of an analyst. What we found is that depending on areas of specialization, that's not enough. We've kind of not – we've not relaxed the foreign language requirement and we've not relaxed the critical thinking, but we've had to start adding things like technical expertise, knowledge of – I'm not saying detailed as the computer scientists, but counterintelligence has come into play big time in terms of basic training.

There're some things you do so many times a day, depending on what you're looking at, that you want to do at other times of the day. Very intricate kind of foundation activities that you need to know even if you're doing just open-source analysis. We're in a process of revising our performance standards right now for open-source officers to accommodate this increased this for technical analysis or technical skill and that to reach a certain level of proficiency they will probably need to demonstrate that type of skill, not only in how they use the tools, but in the variety of media to which they must deal. So the geospatial information, video information, we want our folks to be able to integrate all media types into a product as opposed to, I just have to write this thing in two pages and I send it on and the video guy takes it, he does it. It's the power in the future is we're going to start with a picture and support it with text, as opposed to starting with text and supporting it with eye candy.

And so you have to have some technical skill to do that, at least that's our experience.

MS. ALEXANDER: Let me just add to that. I was an analyst many years ago, as my kids say, back when dinosaurs ruled the earth. And my focus was foreign intelligence information. We used state. We used finished products. Open source was maybe when I got "Corriere della Sera" once a month coming in on my desk or the orange-covered FIBUS (sp) and anybody who remember what part of the world that was, can see me and I'll buy you a drink or something. But that was it and what we're seeing in open-source analysis is a huge expansion in tradecraft, I think.

I'm awed when I talk to our young open-source analysts about the research planning that they do, the ways in which they are using not just the first bit of information that they gather from the internet or from other sources, but that leads them to something else and leads them to something else. Within the homeland security mission, for example, one source of open source is in tattoo parlors, the designs that are on the walls. Well, that leads you to understand the demographics of a gang perhaps in a locality.

So the – it's almost – to me looking at the analysis that occurs today – a broader, more imaginative, more use of curiosity to get all of the pieces of the puzzle together to provide a finished product.

Q: Yes, you mentioned OSCAR. How do you see that fitting in with the four different enterprises? For anybody.

MS. TUDISCO: I'll take that on and gladly let others chime in, too. We in Defense see that as a real building block, as I mentioned, because Defense being a very hierarchical, structured, disciplined organization, everything we do is driven by requirements. And so the idea is to articulate those requirements in an accurate concise way that can be acted upon in the open-source world. So this requirement system will give us the vehicle to do that. It'll give us a vehicle to reach out to other areas of competency and capability that lay outside of our own realm in defense, and to grab that information and use it as others can tap us for our areas of expertise.

So we don't go fishing for information just because we want it. We have a requirement. So everything that we do is what we call requirements driven. So this system will put that in place and it will, in a way, just as much as we need to give ourselves structure in the programmatic world, it'll give us structure in the collection and acquisition and analysis worlds by having a structure to house it.

And, frankly, to recognize it, to put it out there, as it already is, as a profession, as Doug said. A profession needs its own house and its own structure, if you will. So we think that'll be good. Plus, on the back end, you've got the products that come out of that requirement system that can then be identified and shared with anyone who needs them. So I see it'll be very good for us to measure what we're requiring, what we're getting, and how we're using it, and then who is using it because any consumer is going to be interested in somebody else's product. So I just see it as a really necessary building block to put a little more form to the process that already exists.

MR. NAQUIN: Anybody else on that one?

MS. ROBSON: Well, I can – just one thing that I envision with OSCAR is that all the members of the community have access to it. So when somebody comes in with a specific need, everybody will have the opportunity to see what that need is and to weigh in on whether or not they could provide that capability. So it's really a collaborative view into what the needs are across the community and lets people actually – if somebody from PACOM comes in with a need and NOSC has a product, then they can come in and offer to fulfill that requirement.

Q: (Off mike, inaudible) – the question – I'm – (inaudible) – from George Mason University. The question relates to the differences between open-source intelligence and other types of intelligence. There are clearly many advantages to open source, but there are very significant differences, especially with respect to credibility and how this affects the methodology, whether the analytic methodology and whether there are efforts to update this formal analysis methods and also training of analysts with respect to a much higher attention to be given to the credibility of sources. And how this could be determined? And how this could be shared because credibility is a complex issue to assess and because it is open source maybe it should be shared once it was established.

MR. NAQUIN: I think there are several questions in there. I was wondering whether I was going to get asked the question. No matter what conference I go to, it's – well, that's not reliable. Open sources aren't reliable. And I'm kind of perplexed by the question because why is it any less reliable than any other – any other source of intelligence because it's unclassified. There is a vetting process that goes, whether it's – (inaudible) – whether it's imagery, and open source that addresses exactly the type of question. The foundation of open source, whether you call it information or intelligence, is the source analysis. And I'd better get this right because I got several analysts in the audience and they'll kill me if I get it wrong.

So the idea is that part of what drives our value is our knowledge of a source. So when we hear or see something in the open press, the first thing we ask ourselves, who owns the paper, who runs it, what's the possible – what are the possible games being played in terms of why this information is there or not. All that analysis goes into a source before one word is put down on paper or one judgment is made. So we know the various sources in the newspaper, what their circulation is, who has access to them, how many people actually have access to the internet in certain countries. So we know if it's having impact or not. All that is what I call that foundation analysis that goes before anything is provided.

That said, it doesn't necessarily have to be true to have impact. So if something's false and 15 million people get access to it, there's some impact that we have to be ready to address and assess. So this question of credibility in source analysis is key, but I don't think it's any different from an open source than it is in the other intelligence discipline.

Every discipline has a way to do that source analysis or that source vetting or understanding if it's reliable, not reliable, or somewhere in between. So that's key.

In terms of the question about sharing, that's one of the advantages of open source generally, is that it is more widely sharable than other sources of intelligence. The second irony of open source or the three is that the better we get at it, however, the more we are pressed to classify it because the better we get at it provides an advantage. And when you get that advantage, you don't necessarily want to share it with – I'm not talking about within the government necessarily, but widely outside the government. So that's kind of a conundrum that we have to address. If we get really good and starting to answer really sensitive questions, or whether we're right or wrong, we're tackling sensitive requirements, that's going to push us or could quickly push us to the realm of classification.

By and large, you'll find in the Open Source Center we are relative liberals in the case of information sharing and we look for reasons why we can't share before we find reasons why we can.

I'm not sure I answered all elements of your question, but that source analysis piece is really critical to us and it –

Q: (Off mike, inaudible) – here, in the case of open source, you don't really have the luxury of time. There is a lot of information. You may want to use all those you cannot vet the source. And I think these should be taken into account in developing these analytic methods.

MR. NAQUIN: You're absolutely right. There are caveats that we apply to new sources that we've never seen before. Somebody posts a blog. A lot of it tends to go up, right. And we do a lot of analyses before we drive any conclusions. But if we have a newspaper that's been published for 50 years, we kind of have some sense of its reliability. So the other good thing about open sources is that we can redefine all sources in a way that there are several different media types that can address the same question that could triangulate, as Jim talked about, even within the open-source realm. It's not often exact science, and with new media it's posing us all kinds of new challenges and problems, but also a whole lot of new opportunities.

MR. BELL: Doug, can I just add that basically we're ultimately talking about good analysis and how to do analysis well. And I think the intelligence community as a whole is really focused on that, analytic standards and training people. And open source is a particular set of technical skills, but it has to meet those same standards of analytic integrity and sourcing as part of that. And I think we're cognizant of that and I think a lot of effort is being put into making open source a reliable form of intelligence. That's what we're about.

Q: Sergeant Bill Lewis (sp), 101st. Barbara, you spoke about mobile training teams. What type of training does your teams provide and do they provide any training in hotspots such as Afghanistan?

MR. NAQUIN: Yes, we do. We provide a lot of the mobile training. So we provided training just this summer to units in Afghanistan and Iraq. And I can't say where, but in the Middle East that was easily accessible. Our challenge is just capacity. So we would if we could try to offer them once a week, but we generally try to hit regional and hotspots particularly. That's kind of our number one priority. And then, if you want to see me after, we can give you some opportunities – some of the next opportunities that are coming out.

MS. ALEXANDER: Our training teams have been focused on our state and local fusion centers. They've been for the homeland security information. And then, as I said, we've developed an online training, again, focused on the specific needs of the homeland security community. We have worked closely with the Open Source Center in developing modules. And Open Source Center personnel have gone with our folks to these fusion centers for some of the training. There's a variety of techniques that are taught, methodologies. I mentioned the use of research planning, things as basic as RSS speeds and how to incorporate the tools and techniques that are available to help analysts go through the variety of information in that platter of information that

crosses their desk. So it's a two-day course that we've been having at the fusion centers and we're also working with our components in the department and our headquarters analysts. So it is focused on the homeland security aspect.

MR. NAQUIN: I think we can help you out. Richard?

Q: Hi, Richard – (inaudible) – from NGA. One of the concerns I have is that all morning along I've heard behind the scenes we need more resources, more money, more people across everyone who talked this morning. When I look at the analysis and I look at what's been finished and produced, I see that it is getting classified at very high levels. If people don't know that the most of the information came from open source, or a lot of it did, so as we start looking in the future about getting those resources, the impact of open source to our products is not really evident. For the hurricanes in the last couple of weeks, we've done a lot of work looking at open source for the hurricanes, for natural disasters to save people's lives. Yet when those reports are finished, nowhere does it mention that it was from open source most of the information was derived. So as an enterprise, as we move forward, how are we going to ensure that our leadership understands that much of what they're seeing is open source?

MR. NAQUIN: Well, that's kind of – it's almost a philosophical question. I can say with some confidence that my leadership and also the customers do realize the extent to which open source contributes to the overall mission. We also are fairly – not fairly, very good about metrics in terms of looking at things like impact and access and who's using it, so we can actually make these cases to folks as they come through and they ask, so what, what are you doing?

That said, when it comes to resource discussions and decisions, that's why I said earlier, having that conversation and sitting at that table at the right time is crucial. And it's going – it's getting better. I've been in this business on the open-source side a long time. It seems remarkably improved in the last three to five years, but it's not going to happen over night. It's going to take this continuous – we've got to show impact. We've got to show value. We've got an investment. Now, we've got to show the so what. We're showing it. I think that'll sustain it or keep it coming. But we're seeing ways to show the value and to measure it and to kind of say this is what's you're getting on your return. And that's been helping. I don't know on the defense side.

MS. TUDISCO: (Off mike, inaudible) – some comments too. DIA has really embraced the DNI analytic tradecraft standards. And through that approach, when we create a finished intelligence product, we can identify the source streams. And open source is right there. So I think the next step will be use the tool, develop the tool that will parse that out and measure the volume and the contributions and so on. And then, as I envision it, OSCAR will take us from the requirement to the end product. And so you've got visibility and accountability for what we're doing with open source and how it's contributing. And then perhaps we can tie those products and analyses to a decision that decision makers made. So therefore, I think that will give us a better audit trail as well.

MR. NAQUIN: We have time for one more question.

Q: Carlson – (inaudible). Sir, you bring up a very good point when you mentioned that it doesn't necessarily have to be true in order to have an impact when it comes to open source and different things. And I guess my question is to what degree has open source learned from their experiences. You see a lot of attention being given to the negative press coverage to something like the Haditha case or Hamdaniyah, some of these cases bring up – kind of bringing military justice issues. And I guess my question to the panel here is to what degree does open source owe the national community sort of the responsibility to sort through misinformation if indeed it is out there? Thank you.

MR. NAQUIN: Well, it depends where the misinformation's coming from. If you're talking about – we look at – again, it depends on the context. If we're getting a certain perspective, we want to understand, number one, what is the foundation for the perspective itself, and what is the context upon which it's delivered. What is the timing in which it's delivered? And then we can kind of come up with some possible judgments, but we're usually very careful about – (inaudible) – on them in terms of why this might have come out when it did, why it did, and the tone it did. And we do that by understanding the source and years', sometimes decades' worth of background information on how that source operates.

If it's one of these new sources, we're much more circumspect about what kind of conclusions we draw and we have to develop a whole new baseline for a whole new source. So in terms of what we can – we're often asked questions along the line of why do they think this way or what changed their mind. And of course, you can't actually get into the mind or definitively say they changed their tone because of this, but you can provide some context upon what might have been triggers for a change of behavior or for anomaly. And that's generally what people look to us for are the anomalies. They don't need to be told, oh, yes, the French still don't like us, but what they want to know if the French start liking us why what happened.

So those are the types of things that I think we have the most value. Other than that, people tend to want to draw their own conclusions based on their own context that they establish.

So we're a little bit careful of getting too subjective and we try to keep in the realm of – as trade – as much ties to a tradecraft as possible.

I think that wraps us up in terms of time. I really appreciate you attention and attendance and also thanks to the panel. Appreciate it very much. (Applause.)

MS. HORNE: All right everyone, we're heading to our next sessions at three o'clock and don't forget that at 4:15 we do have the "Meet the Speakers" session in the exhibition, where you can mingle and chat with those folks that you've heard from all day. Thank you so much.

(END)

**Remarks and Q&A by the DHS Under Secretary for Intelligence & Analysis**
**Mr. Charles E. Allen**

**DNI Open Source Conference 2008**
**Washington, DC**

---

SABRA HORNE: Welcome back to the second day of the DNI Open Source Conference. We hope you had a wonderful day yesterday, and we're excited about our big day today. In a few moments, you'll hear from Mr. Charlie Allen from DHS. We'll also get to hear from General Hayden from the CIA today. We have a privacy discussion featuring Mr. David Shedd, Jeff Jonas, Richard Willing, Alex Joel, and Jonathan Zittrain. So it's going to be a big day.

We also have an announcement that we want to make regarding the Open Source Works, which is a CIA agency doing amazing open-source work. You'll hear about that later today.

A few housekeeping details: We wanted to let you know about the question-and-answer process. You all should have received some note cards earlier today. They're also available outside. Please write your questions on these cards and folks in the aisle will collect them, and we'll be able to deliver those to the speakers at any moment.

All right. We have up now – I'm going to introduce Ms. Barbara Alexander, who is the director of Collection Requirements for DHS I&A. She is also the director of Charlie Allen's Open Source Capabilities within DHS. She's had a 25-year career in intelligence, and we're thrilled to have her part of the open-source family. We also want to note that yesterday was the release of their strategy, "The Vision for the Domestic Open Source Capability." So welcoming now, Barbara Alexander. Thank you. Enjoy the day.

(Applause.)

BARBARA ALEXANDER: Good morning. It's my distinct privilege this morning to introduce someone who, for many in this audience, needs absolutely no introduction. Under Secretary for Intelligence and Analysis and the Chief Intelligence officer for the Department of Homeland Security Charles E. Allen has had a distinguished government career spanning over 50 years. He joined the Central Intelligence Agency as an analyst in 1958, and he's worked on almost every geographic area in the world.

When Charlie says, I know that subject well, which is a frequent comment at morning staff meetings, it's a reminder to those of us who worked for him that he has been an astute observer of world issues for a very long time. He has served as the National Intelligence Officer for counter-terrorism and the NIO for warning, and the assistant director of Central Intelligence for collection, all positions that have postured him well for the critical role he now holds, as he supports the Department of Homeland Security's mission of defending the nation against all hazards and all threats.

He knows all the domains that we've been talking about at this conference. He served as the deputy program manager on a multibillion dollar compartmented program at the Pentagon. He's had overseas assignments, so he understands the State Department and the diplomatic role. He reinvigorated the Open Source Steering Committee as its chair in 1999. In the three years that he served in DHS, he has developed a DHS Intelligence Enterprise. He built an architecture that encompasses the department's components, and the state, local and tribal partners across the country, and with our foreign partners.

He has developed the analytic cadre of the Office of Intelligence and Analysis, focusing our analysts on the priorities of the department. He has ensured that intelligence supports the operational activities of DHS. He has expanded I&A support to the state and local fusion centers, taking resources out of hide to ensure information of intelligence value is reported to the intelligence community and to our other stakeholders.

He has worked with the director of National Intelligence to secure a place at the table for DHS as a full participant in intelligence community forums. And he's developed the DHS open-source enterprise vision and strategy that will provide unique support to homeland security constituencies with actionable open-source information in a manner that is consistent with civil rights and civil liberties.

I Googled Charlie when I got ready to do this introduction. This is open source, after all. Wikipedia – I know, not one of the most reliable places – but Wikipedia refers to him as an American public servant, notable for his roles at DHS and before that, at the CIA. And Bloomberg.com, in a March 2006 post recalls that the then-Director of National Intelligence John Negroponte called him the most experienced intelligence professional in the U.S. government.

I would say that there are many public servants, but there are very few legends. Charlie is a legend and an inspiration to all of us who work for him. He knows more than anyone else the decision advantage that intelligence brings. And you'll hear from him, I know, the value that he places on open source, as we defend the homeland.

I am pleased and extremely honored to present to you Undersecretary Charlie Allen.

(Applause.)

CHARLES ALLEN: Thank you very much for that more than generous introduction. I really am grateful to be here, and grateful for this opportunity because over some decades, open source has been the watch word of what I have tried to exemplify here in the intelligence community over, I guess, five decades. And I'm very pleased that you have had excellent speakers before me, such as Glenn Gaffney, Joe Hayden, John Clapper (ph). And I'm obviously grateful for the DNI and the Open Source Center, as well as – we're very proud, as part of the department, to help sponsor this conference.

Open source has always served as an essential foundation for both current reporting as well as strategic analysis. Allan Dulles said that 80 percent of the information required for the guidance

of national policy could be found out in the open – in the library, as he put it. I never really talked to Allan Dulles, but I saw him when I first came as a very young officer to the Central Intelligence Agency.

In 1947, in a New York Times interview, George Kennan, who was X in the "Foreign Affairs," the father of our containment policy against the expansionism of the Soviet Union, said that he believed that 95 percent of the information needed for national policy decision-making could be found in the open.

Joseph Nye, who is well-known to many of you, former chairman of the National Intelligence Council for whom I worked directly for 18 months, and of course, he is former dean of the Kennedy School at Harvard, he stated that open-source intelligence provides the outer pieces of the jigsaw puzzle without which one can neither begin nor complete the puzzle. If you know Joe Nye, and I know him well, he always has great elegance in the way he puts things, no more elegant writer, and I think that captures it very well.

I've long been an ardent advocate of open source. In the Cold War, especially in the early years, in the '60s and '70s, we literally wrote many president daily briefs based only on the substantive knowledge of the analysts, and reading Tass, Izvestia, or Pravda. There were no classified sources with that, only the knowledge of the analyst. I wrote many current intelligence items, as well as PDBs, in various areas of the world based on only open source – my own substantive knowledge of that country.

That sometimes comes as a revelation to people at senior levels. In the 1990s, I had an unnamed, very senior official of the intelligence community who held a huge responsibility. He said, I found out that you could actually put open source into a president's daily brief, which was an enlightening moment of revelation when I just smiled and thought of the decades of how many Kremlinologists used only what was published over Radio Moscow or in the Soviet press in order to write and inform the president and the National Security Council about open source. Sorry to give you that history, but it's important.

When I was the assistant DCI for collection, I really worked to bring open source into the areas of collection. As Doug Naquin would know, open source, represented by FBIS, was at every meeting of the National Intelligence Collection Board. I chaired that board for 10 years. It was an excellent board. It still operates today under Glenn Gaffney. Let me tell you, I always demanded more from open source, and those who attended from the open source, from FBIS, and what is today the Open Source Center know that, where I press them to do more, because I know the nuggets are there.

In my current role as the under secretary for intelligence and analysis, we know that open source is indispensable to supporting Secretary Chertoff, the DHS leadership, but equally importantly, and probably more importantly, to help us support our state and local customers – our tribal, our territorial customers – and also to be used in supporting our private-sector partners. Ultimately, the central source of open source in intelligence was recognized in 2006 by the DNI when he designated open source as a source of first resort. That was Ambassador Negroponte.

That is not to say that open sources are the end-all or the be-all of intelligence, but it is the source of first resort. It can free up a lot of other equally critical intelligence disciplines to go after the truly – the hard targets and the critical information gaps. When we have an issue developing at Homeland Security that may be a threat or threat-related, a threat to the homeland, we always go to open source. And when we have a breaking crisis, yes, we call our partners that have classified information, but I always instruct – I say to the watch and warning staff, call the Open Source Center. See what they have. What's in the press?

Open source serves as an important role of validating classified or sensitive source reporting. We see a development occurs, and we see if it's controlled press, we see what the press says, which from official reporting, validates it or may put a spin on it from the host government, and you read it. You read it. And I was reading open source this morning. I come to work at 5:30, and I was reading with my watch and warning staff issues coming out over Radio Caracas – very interesting stuff relating to Hugo Chavez and some of his actions. So I always turn to open source as I turn to classified sources.

Open-source support to the homeland; it's vital that you understand it and understand how we use it. The need for timely, accurate, and actionable open source in the post-9/11 world requires a change in the intelligence community's legacy thinking. And DHS has the unique responsibility for making open source the source of first resort for homeland security constituencies. Given our mission, we must provide high quality open source to an unprecedented stakeholder group, from the president of the United States, the local police department, the first responders, as well as the private sector. Our private-sector stakeholders own 85 percent of the infrastructure of this country, and they need support and assistance and we are providing that.

While the intelligence community has long had an established open-source capability directed against foreign threats, no comparable open-source capability existed on the domestic side. DHS must assume the leadership role for domestic open source as a means of protecting the homeland and supporting the first-preventer community, which serves as the tip of the spear for homeland defense. In this role, DHS can provide decision advantage, as Barbara said, to the homeland security community in new and innovative ways.

Through the fusion centers, we have an unprecedented relationship and communications mechanisms with state and local law enforcement. As many of you know, I am putting DHS officers within the fusion centers across the country. At the end of the year, we will be represented in 35, and by next year, in the next year, we'll be in 50 fusion centers. Through fusion centers, we have really an unprecedented relationship and communications mechanism with state and local law enforcement. We can provide critical understanding of foreign events, which may threaten or have an impact upon the homeland, local jurisdictions or private-sector infrastructure.

On 29 and 30 June of 2007, when we had attempted attacks near Piccadilly in London, and when we had the crash of a SUV into an airport in Glasgow, our state and local officials wanted to know, well, what does this reflect? What were the techniques being used in this IED that – the IEDs that failed to go off? Open source provided a lot of information instantly. Yes, usually

official reporting comes in, but it's followed – it comes behind the press. We were able to get a lot of information out, out to all the state and local fusion centers, and we did this jointly, obviously, with the FBI, which goes out to its law enforcement partners.

Open source will never provide all the answers, but it can provide the value of adding enhanced situational awareness in a very tailored and a timely and informative way that the products can be, in turn, disseminated widely to an audience and our audience rarely has clearances in the broadest sense. We have cleared hundreds of people at the local level, but this can be translated all the way down to people who will never need a clearance to give them a sense of what's occurring, to give them a sense that there's some new technique or tactic or procedure being used by extremists in conducting attacks, say, overseas. You'd be surprised how valuable that is at the local level.

The goal here is not to create a new stovepipe, but rather to augment the classified intelligence, to produce the best possible intelligence. In 2007, I established the DHS open-source enterprise with the mission of supporting homeland security constituencies at all levels of government with timely and accurate and actionable open-source information in a manner that protects the constitutional rights and the privacy of U.S. persons. I want to briefly take this opportunity to share with you the significant progress we have made in developing our domestic open-source program.

First, you will find at this conference copies of the DHS "Domestic Open Source Strategic Vision," and I hope each of you get a copy of it. It just sets out very succinctly how we envision open source and what we're going to do about it. This vision sets out our major goals and I think it's fully aligned with, and complementary to the goals set forth in the "National Open Source Enterprise Strategic Vision."

Secondly, our vision clearly establishes DHS's intelligence role as a focal point for open source among the homeland security law enforcement and first-preventer communities. It underlines the lead role in developing robust open-source capabilities in DHS and throughout the state, local, and tribal homeland security organizations along with the need – and this is very important – to develop a skilled and highly trained cadre of open-source professionals.

The DHS vision also emphasizes our role in providing actionable intelligence that is responsive to the unique information needs of the state and local law enforcement communities and establishing an effective open-source information-sharing capability. If there's one thing I think we do well in homeland security intelligence, is to share information, and it's expanded almost exponentially over the last two years.

It also sets a key objective: the need to leverage innovative trade craft and technology. And I want to make it clear that our strategic vision is accompanied by an implementation plan that outlines specific activities and actions which need to be taken, many of which we're already beginning to meet. So it's not just a vision; there's an actual implementation plan that makes a difference.

Let me talk about some of our successes and upcoming activities. In training, we have created a two-day open-source training program which has been delivered to good reviews, to 16 state and local fusion centers over the past year – totally unprecedented. We're scheduling the delivery of that training to all state and local fusion centers throughout the next year, and we'll also be providing this training to DHS analysts and DHS component organizations, such as customs and border protection, immigration and customs enforcement.

We did not just stop there. We have created the first of its kind online open-source training program, which is available for you to see at our DHS kiosk here at the conference, which will make open-source training continuously available to even a broader set of homeland security and law enforcement personnel.

We have also created a DHS open-source website on the DNI's Intel-U which our metrics showed to be one of the intel links most popular and accessed sites. They're interested in what goes on, in what we send out, particularly what we share with our partners, because it's not just the Feds; it's what's outside this Beltway from the homeland security perspective that really counts. DHS intelligence is producing a number of daily serial open-source reports which are routinely featured on the website and available to state and local partners.

We intend, over the next year, to expand our information-sharing efforts by creating an open-source portal on homeland security state and local communities of interest to ensure the optimal delivery of information across homeland security and law enforcement communities. This is called Homeland Security Community of Interest, or (HSLIC ?). This is a COI that's available to 45 states, the District of Columbia, and up to 4,000 analysts participate in this information-sharing program on a weekly basis through teleconference.

And collaboration to make certain that the domestic open-source enterprise is fully inclusive and coordinated – we're establishing a DHS open-source governance process that will ensure state and local and intelligence community participation.

We continue also to be active in the DNI's National Open Source Committee. And thank god it's active, and it wasn't in the perilous state it was in when I essentially rescued it in 1998, and '99 and 2000.

We're also formalizing our relationship with the Open Source Center in order to leverage open-source capabilities in support of DHS's open-source program. We're very grateful to Doug Naquin for his support.

We understand that the open-source universe is always expanding, evolving, and we have to work hard to stay ahead of the trends in this environment – everyone does – if we're going to harvest its full potential to meet homeland security needs. To that end, we will initiate a DHS Open Source Innovation Center which will model the best practices of similar activities in the intelligence community and the government, taking full advantage of public and private-sector trade craft and technology advances. We think this will significantly enhance our capacity to deliver relevant open-source analysis to our stakeholders.

So let me, in conclusion, be clear about one thing. We know better than anyone that we have much more work to do, and I think everyone does, and that there are many more challenges. But I am absolutely committed to creating the most robust domestic open-source program possible and to ensure our state and local partners have the absolute best and most timely and relevant information possible.

I believe we're well on our way to meeting the goals that were laid out in our implementation plan. I do know we have a lot of work to do, but I think we all do. I think we're living in a new world. The new world order is very different and the issues with which we have to work are very different as we look at homeland security, and we look at all aspects of what that really means.

Never have I enjoyed more working with our state and local partners, and with our first responders, whether they're in Orange County, California, or whether they're in Miami-Dade, down in Florida. We could go on, and I could give you many examples of how I think we're beginning to transform events, how we're sharing information, how we're sharing intelligence.

Thank you very much. I'm very happy to see this conference is so well attended. (Applause.)

Any questions?

MS. HORNE: We have time for two questions.

MR. ALLEN: Two questions, okay.

MS. HORNE: I thought I'd read them to you.

MR. ALLEN: Yes, ma'am.

MS. HORNE: "Has homeland been defined – as defined by Congress, does homeland security program include Canada because of the common frontiers, NAFTA agreements and the rehabilitated NORAD?"

MR. ALLEN: Well, homeland security, obviously, is deeply concerned with our northern and southern borders. The country, Mexico and Canada, are both great partners, as we know, in NAFTA and other agreements, working together on information, and the sharing of that information and on intelligence that is very crucial to us. We, at Homeland Security, both in intelligence and non-intelligence areas, have very rich relationships with our allies, both north and south. We think very highly of the need to continue to share information.

Canada is extremely important to us, part of the Commonwealth, part of a longstanding, obviously, intelligence relationship that goes back many decades, and information-sharing is certainly something – open source is something that we want to collaborate with our Canadian partners and we think very highly of what they do and we're going to work ever more closely in the coming months and years ahead.

MS. HORNE: And the last question: "What will the open-source environment look like 10 years and beyond?"

MR. ALLEN: You probably ought to ask a 20-year-old that question, rather than I. I think it's going to grow so exponentially that it will defy definition; the speed, the power of computing and the power to move data in every aspect possible. So I believe that the universe is going to expand beyond belief. And I do really believe that not only Allen Dulles, but George Kennan, had it right. I think Allen Dulles actually said much earlier in his life how valuable the public library was in providing what is needed to inform decision-makers about events and how to react to them.

I think we're going to be able to react very, very quickly to crises. We're going to see them, and I think the whole new discipline of open source – I do recall some people in even as late as the 1990s in the intelligence community being dismissive of open source. I hate to say that. That's very painful, at a time when I just could see it taking off as part of what was becoming the Internet. I won't mention who those people were because the names are rather prominent ones.

But dear lord, we cannot begin to value sufficiently open source 10, 20 years from now. We're going to have – going to be the best informed and we have to stay on the cutting edge of this as a country. This is our forte, our ability to handle information. Other countries are doing a lot in this world on open source and data handling. I think this country has to be the best. I actually do believe in American exceptionalism. Not everyone does today, but I do. Thank you very much.

(Applause.)

MS. HORNE: Thank you very much, Mr. Allen, for your comments, but especially thank you for your vision and your leadership.

(END)

**Panel: Managing the Balance Between Privacy & National Security**

**DNI Open Source Conference 2008**
**Washington, DC**

**INTRODUCTION:**

RICHARD WILLING,
PUBLIC AFFAIRS DIRECTOR, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

**MODERATOR:**

DAVID SHEDD,
DEPUTY DIRECTOR OF NATIONAL INTELLIGENCE
FOR POLICY, PLANS, AND REQUIREMENTS

**PANELISTS:**

JEFF JONAS,
CHIEF SCIENTIST, IBM ENTITY ANALYTICS,
AND DISTINGUISHED ENGINEER, IBM

JONATHAN ZITTRAIN,
PROFESSOR OF LAW AND CO-FOUNDER, BERKMAN CENTER FOR INTERNET AND SOCIETY, HARVARD LAW SCHOO

ALEXANDER JOEL,
CIVIL LIBERTIES PROTECTION OFFICER, ODNI

SABRA HORNE: Next, we will hear a wonderful discussion about privacy, open source and technology. Mr. Richard Willing from the Office of Public Affairs at the Office of Director of National Intelligence.

RICHARD WILLING: Good morning. As Sabra said, I'm Richard Willing, Director of Public Affairs at the ODNI, but a year ago, I was on the other side of the footlights working as a reporter, covering this conference for USA Today, producing what I now know as open source. Back in the day, in my then-current vernacular, I thought it was just clips or scraps, or some of our detractors said fish-wrap. I'm glad for the upgrade.

Newspapers, even online papers, are painfully low-tech. They do come with some privacy protection, so the disincentive of lawsuits, which even if not won are painful and expensive to defend, as well as market pressures that keep high-end papers like The New York Times from running lingerie ads with teenagers at least more than once.

But the technology that sort of drives this rich harvest of open source is no respecter of privacy when knowledge is the concept at all. Birth, death, property records – they're available to

reporters for fashioning their profiles, to analysts for making links, to covert officers for building covers, and then they're tossed around the Internet by anybody and everybody like an old infield ball. Genetic profiles are placed online so that families can match up. They're also available to law enforcement, intelligence, private authorities as terrific identifiers.

Back in the day, a young reporter – okay, it was me – had to spend a lot of time in the Detroit Federal Courthouse going through old transcripts to find the true name of a disgraced lawyer who had managed, after his discipline, to have his name changed in all the filings to John Doe. These days, it would only take capturing the original web page which is relatively easy to do, even if deleted. When embarrassed lawyers, by the way, file false light and invasion of privacy suits – when reporters do things like that to them, those go online, too, forever. So open source gives and open source takes away.

Yesterday's presentation had several signal examples of the collateral damage that can occur when the demands of technology collide with the needs of the individual. The newspaper in Florida that posted a six-year-old story about an airline bankruptcy over today's date, the stock went down 75 percent, I think we were told, in a matter of hours before it could be called back and corrected.

The technology called image metrics, I believe, that constructs a perfect video replica of a human being, make it say anything it wants online, this is putting words in people's mouths, something reporters are accused of doing. This is creating the whole plumbing. I saw today that YouTube is going to police jihadist and other videos that advocate violence. So this is a moving target. Actually, that story is on page D1 of the Washington Post, but full disclosure, I read it online at 6:00 a.m. this morning.

But we're the government, you say. We've got sovereign immunity to protect us from lawsuits. Why shouldn't we have the same access to the technical world that the famous, iconic, lone, white male blogger sitting in his undershirt in a corner of his parents' basement has? Part of the answer, I think, is what we're here to talk about, but part of the answer, I think, is the laws and regulations. We operate under FISA, the Privacy Act and that 1978 law I can't remember that set up and polices national security letters of agency directives, executive orders like 12333, charters, ICDs, that database of federal judicial officers I created, their home addresses and phone numbers. If I bring that over, continue to hold that, is that a problem? If they're U.S. persons and I retain, collect and disseminate it, it might be.

We've got a distinguished panel this morning to kick off this debate and ask the appropriate questions and suggest some ways in which maybe the technology itself and certainly regulation, and maybe just a little bit of good old common sense, can help get us to an end state where we get the maximum use out of open source while minimizing the intrusions into personal space.

Our panelists include Jeff Jonas, IBM distinguished engineer, big thinker on all matters technical who's just completed the U.K. Iron Man on Sunday, which means he's run 26.2 miles, swum 2.4 miles and biked 112 miles, all in one day. There's meaning there, and I'll leave you to tease it out.

Alex Joel, our civil liberties and privacy officer at ODNI is also on board.

And in the spirit of the day, Jonathan Zittrain – or least electrons confected to form a perfect simulacrum of Jonathan Zittrain – he's going to appear via video conference from Cambridge, Mass., where he leads the Berkman Center for Internet and Society at Harvard Law School.

The panel's moderator is David Shedd, a true national intelligence officer whose ODNI career is coterminous with the life of our office. He started as chief of staff in May of '05 one month after the office was stood up. He has been the acting director of the intelligence staff, and since May of '07, has been the deputy director for policy, plans and analysis. He's truly the ODNI's man for all seasons.

David?

DAVID SHEDD: Well, the first disclaimer is I'm not Jeff Jonas and I'm not the Iron Man. Jeff, great to have you here – Alex as well. I will take on faith that Jonathan is out there.

I thought we would open with a framework in terms of government and the treatment of civil liberties and privacy as it pertains to the issues of the handling of open source. And for that, I've asked Alex to give a bit of a précis in terms of a better understanding for the audience in terms of what that entails.

ALEXANDER JOEL: Sure. Thanks, David. I'm Alex Joel, the Civil Liberties Protection Officer for the Director of National Intelligence. And when people think of open source, obviously, we're talking about publicly available information and even though it's publicly available, it doesn't mean that it isn't protected. In the intelligence community, we operate under the rule of law. We have the Constitution. We have federal statutes. We always have to remember that we do operate under those principles.

But I want to talk more specifically about Executive Order 12333. We talk that about executive order a lot in the intelligence community, but just to remind ourselves of what that means – and it was recently revised as we know – part one of that order lays out the roles and the missions and the intelligence agencies and the director of National Intelligence. That was really what was revised in the recent exercise that we went through.

Part two lays out the protections for United States persons, and that wasn't revised in a substantial way in the recent revision. And we call those the U.S. person rules, and those are very critical for Americans to understand. First of all, just to remind ourselves, a United States person is very broadly defined in that executive order. A United States person is not only an American citizen and a permanent resident; it's also a corporation and corporate in the United States, and importantly for our discussion today, it's an organization that's substantially composed of Americans and lawful, permanent residents. So it's an unincorporated association.

What does that mean on the Internet? What does that mean in the open-source world? That can be somewhat difficult to ascertain. It's also difficult to know when you're dealing with a United

States person or not in open-source electronic environment and the new technologies that we're talking about. So that's something to think about.

So the executive order talks about protecting information concerning a United States person in terms of collection, retention and dissemination. And the basic rules are: You can only do collection retention and dissemination pursuant to procedures that are approved by the attorney general and the head of your agency. Now, that sounds very bureaucratic, but practically what that means is there are 17 elements in the intelligence community. Those elements operate under their own rules. So you have to worry about well, what elements am I a part of, and what do the rules of my element say? You have to make sure that the collection activity you're doing pertains to your mission.

So just because it's publicly available and the information is about Alex Joel, it doesn't mean that I can go out and collect information because it's public and it's about me, Alex Joel, because I find Alex annoying and I want to keep track of him or I'm curious about people in my neighborhood. It's publicly available and I want to keep track of them, and I want to maintain a database about people in my neighborhood and share it around the intelligence community, because, hey, it's publicly available. No, it has to relate to the mission of your agency.

Beyond that, the executive order says use the least intrusive means feasible. Well, that's good for the public information community, the open-source community, because, hey, it's publicly available. That is not an intrusive technique, and so that's what we're all here to discuss. Open-source information is, of course, defined as publicly available. That's one of the main categories of information that Executive Order 12333 authorizes the intelligence agencies to collect.

And so, one of the main questions we ask ourselves, when we're going out and collecting information, is, is it authorized by the attorney general guidelines for our agency? Is it related to our mission? And is it publicly available? And so that's one of the things we're going to talk about. And then, of course, is it U.S. person information? We're going to ask that question as we go.

One of the other questions we need to ask is do we need to disclose our affiliation with an intelligence community element? We talk about that in terms of undisclosed participation. One of the reasons that Executive Order 12333 exists, the main reason, is the abuses that came out in the Church and Pike Committees era in the 1970s. What they wanted to avoid was – one of the things they wanted to avoid – were intelligence community agencies penetrating domestic organizations without disclosing that they were, in fact, members of the intelligence community.

So the executive order requires you to disclose that you're a member of the intelligence community, unless you have authorization not to disclose that you're a member of the intelligence community, and that has to be pursuant to these guidelines that are approved by the attorney general. That doesn't mean that you can't join your local health club without saying, hey, I'm with the CIA or something like that, but it does have implications for how you behave online, join these forums and things like that. You may have to think about, hey, wait a minute. Is this a U.S. organization and do I need to disclose affiliation? So those are one – that's one of the questions.

Another question you have to think about is am I doing this in a way that would be perceived or is in actuality monitoring First Amendment-protected activity? Is this a blog? Is this a political blog? Am I doing something here that could be viewed as monitoring something purely for the purpose of collecting information that's protected by the First Amendment? Again, if you're doing something related to your agency mission, and not for the purpose of just, hey, this is somebody who's protesting the war or protesting administration policy, then that should answer that question.

We should always ask ourselves, is this lawful activity, of course. Let me give you an example. Just because it's publicly available, you might think, well, it's open source. It's got to be lawful, but if, for example, you see something on the Internet – and I see this all the time – you see ads for, hey, buy this service, buy this data; it's publicly available. Well, if it's financial records information, if it's credit records information, driver's license records information, health information, those are warning flags. Those kinds of sensitive records could well be protected by a particular federal statute. So just going out and buying things that claim to be publicly available information, doesn't make it publicly available information. So we always have to ask ourselves whether a particular law applies.

And then the final thing – well, two other quick points if I can jump in here. We have to worry about accuracy of the data, and we'll talk about that in a little bit. So I won't dwell on that here. And an important point from an executive order perspective and from the framework of our activities in the open-source community is, is the activity that we're engaged in open-source collection? Is it open-source intelligence activity or is it human intelligence activity? Is it signals intelligence? And I know that sounds bureaucratic, but from a privacy and civil liberties perspective, that's very important, because if you're doing open-source intelligence, well, that fits in this framework. You're doing publicly available information kind of work.

But if you're really engaged in something else, if you're doing something that really is human intelligence or signals intelligence, maybe you're actually doing something with fancy technology and something else that maybe that's electronic surveillance. Maybe that's covered by the Foreign Intelligence Surveillance Act. Maybe that's something that intrudes on the Fourth Amendment. That should be done by another agency and other folks within your agency that should be pursuant to a court order.

So that's the general framework. I know I threw a lot of ideas out there that we can discuss further.

MR. SHEDD: Thank you, Alex, for that framework and the setup to the kind of discussion that we want to have that's fruitful in the connection to open source and the intelligence community.

To kick off the discussion, I'll turn to Jonathan first with comments to the first question or issue. The intelligence community has been criticized in the past for relying too heavily on secret or classified sourced information for overlooking the wealth that's out there in the open-source community in terms of the traditional way of doing the intelligence community business. We have, as I think you heard from Charlie Allen, already made great strides in recognizing that

open sources are valuable, and publicly available sources can, in effect, better ensure protection of privacy. The size of this crowd is obvious proof of the tremendous interest in this.

So I guess my opening question is, as the intelligence community continues to embrace the world of open source and open sources, how can we use technology to actually help protect privacy along the lines that Alex has already outlined in terms of the framework? Jonathan, would you like to open with a comment on that?

JONATHAN ZITTRAIN: Yes, and I have the same faith that you can hear me that you had the faith that I was out here somewhere.

MR. SHEDD: I gave you the thumbs up. We can.

MR. ZITTRAIN: Excellent. First, I think I agree with your premise, and the premise that we've heard so far this morning, that open source has somehow been the little sibling here. It hasn't been seen as exciting and sexy, as classified or blue-border kind of stuff. And I'm glad to see that changing.

I guess there could be two reasons for that. One is the more banal reason that it's just if you don't have to lock it in safe, how valuable can it be once it's on your desk? I think we can get over that. The other is that maybe it has been thought of as almost too easy to collect, as too easy pickings. If all you have to do is surf the web all day, that somehow just doesn't fit your conception of doing hard work to uncover those difficult secrets that can be the difference between life and death or a successful intelligence operation.

So on that front, I think one thing we might offer is the observation that there is lots of hard work to do to make sense of open-source information. It may not simply be a question of reading the newspaper every day and then surfing your favorite websites, but rather, there are some sophisticated tools, some of which we see in academia, some of which we see in the NGO world, some among entities like RAND or CENTRA, and some within the government itself, that can take otherwise innocuous data and create a mosaic out of it that actually has stuff leap out.

In the early 1970s, they had actually pioneering studies – of course, at the time, run on mainframes – called block modeling, where they could take records within the Centrex phone system of an organization as to simply who called whom – the LUDs as they would call it in "Law and Order." And with that, they could actually crunch some numbers and figure out who was planning a revolt within the organization, who were the ones who were most respected that may be on their way out and really get some insights about it.

Now, that kind of data doesn't have to be pulled with privileged access somehow to the Centrex switchboard, but it's the kind of thing you can do by crawling Facebook or other social networking sites, and get a sense of who was linked to whom, who was clustered in what groups, things that by just surfing Facebook, you wouldn't find, but by the application of a tool, you might not.

I think that then starts to raise some privacy questions precisely because it's so valuable. When I make a friend on Facebook, I don't expect that that's going to be part of some deep insight about me once aggregated with my other friends, or even more important, my friends' friends. When I make a purchase on Amazon, I don't expect that a similar mosaic will happen. I remember once encountering an Amazon page for the Official Lego Creator Activity Book, and you know how Amazon will suggest other things that say, below on that particular page, perfect partner; buy the Creator Activity Book with "American Jihad: The Terrorists Living Among Us Today." That was perhaps some bad mosaicking by Amazon's engine, but it certainly made me think that maybe I should get another book other than the Lego Creator Activity Book and step slowly away from the page.

So there will be ways in which, as these technological tools come to judgments that we can't easily review ourselves, these are inferential systems that cannot explain their own leap of logic, but can simply say, on the basis of everything, I conclude that X is related to Y or that A is part of a group of B.

You do have some risk of guilt by association and it raises the question – and I'm not sure I have an answer to – of how might you allow people to help participate in straightening out their information and reviewing their information. It's simple if you're in the credit report model where TRW or Experian has something on you that's carried over into the Privacy Act and FOIA models of being able to say, I'd like to know what the FBI, say, has on me, and perhaps slightly redacted, I'll get the file, and then I can make a fuss or otherwise petition to have it corrected.

But figuring out how to actually draw the public in and involve them, either in correcting their new information or in creating new open-source information for the purpose of helping the intelligence community might be another frontier worth exploring.

The Texas Border Patrol in the state of Texas set up a set of webcams along the American-Mexican border and gave the public a standing invitation, if you've got nothing else to do today, why don't you stare at this stretch of land and if you see anything interesting, send us an e-mail. They had several million people register for the site. It generated approximately 80,000 e-mails during a 60-day test period. These e-mails actually did say, hey, wow, there's a truck. And it does make you wonder, wow, are soap operas today that boring that this a preferable alternative?

And the answer from the Internet is with a denominator this big, with that many people using the Internet, there will be some significant critical mass of people pretty much willing to take up any task. And figuring out how to harness those eyeballs and those brains to a task that they might self-consciously know is for the defense of the country or the furtherance of intelligence objective might be another project. Why don't I leave off with that? And thank you.

MR. SHEDD: Thank you, Jonathan.

I'll turn to Jeff here for his thoughts, particularly as it moves into the area of technology and ensuring privacy in terms of that, building off of Jonathan's comments.

JEFF JONAS: Yes, so to set that up, I think that today, as people are looking at open source, since there's not enough people to look at open source, you have got to use computers, and you're trying to make the most sense of it. And I think one of the problems that we have is that if you just look at open sources, open sources don't correlate with other data. Your ability to make sense of it, accurate sense, of it isn't so good.

So when I look around, I see people who have whole programs on open source and whole other programs on biometrics, and whole other programs on demographics and structure data. And I think the future is going to be that this data is going to be commingled to make more sense of the open source. So then the question is what data is going to be commingled under what policy?

So as I think about that, I think about immutable auto logs which are this notion that as people use systems, especially nontransparent systems, how they use the system, what they look at, what they record, collect, redact, delete is recorded in a way that cannot be altered. It's like etched in stone. Even the database administrator can't come and undo it. So accountability and oversight people can take look at how – if a system was used within policy and law.

I think another kind of technology that's going to be key, especially as you commingle open source with bad guy list, is what I call tethered data. In other words, if a piece of data changes up the food chain – for example, hey, they're not supposed to be on the list; hey, we had the wrong passport number for this particular person that shouldn't be entering the U.S. – that data needs to move through the system so that the places that that's been reported can correct the change.

And I think data anonymization, where you are changing data into a form that is non-human readable and non-reversible has still yet the ability to be matched, so that people can very narrowly discover what's common between different programs without having to over-share or move all their data.

MR. SHEDD: I want to go back to Jonathan and segue into the question of looking into the future. Where do you think technology is going – and you've already touched on a couple of examples of it – and build on that, and then we'll come back to the privacy civil liberties question as we look into the future in the collating of information and the engines that drive that.

So, Jonathan, would you comment as to what you see into the future?

MR. ZITTRAIN: Sure. There's a recent Supreme Court case in the law enforcement, rather than intelligence context, that is of some interest. The police had used essentially an infrared heat-detecting gun simply aimed at the outside of a house to find, yes, there were people growing pot inside the house. The people then objected and said that that was an intrusion into their privacy that required a warrant and other process before the police could do it.

The Supreme Court holding was interesting. It said that essentially, the police are allowed to undertake the use of technology without a warrant so long as the technology is publicly available. With infrared heat guns not yet widely publicly available – although you can find them in some obscure catalogue – the police would need a warrant. Once it gets to the stage

where you can walk into your local RadioShack and pick up one of these things, and get it free with your battery purchase, at that point, the court says, why would we restrict the police to something that the general public could be doing so handily?

And that's a really interesting line for the court to be thinking about on where to draw the limit on open-source kinds of collection, because I think as the premise of your question suggests, the technology is getting better and better, and more and more publicly available.

So to me, when I look at the next generation of privacy challenges, I look to say, what will be publicly available? How will we be generating, as members of the public, data about each other, judgments about each other? So a couple of examples – I think it's entirely possible in the near future that we'll use our handheld digital assistants when we walk into a café or a bar and we don't know anybody there, we can ask our PDA, are any of the 50 closest friends of my 50 closest friends within 50 feet of me? And if, in fact, they are, let me know and we can make introductions; or more generally, introduce me to people that have enough of a reputation within the system that we're sure they're not an axe murderer, but that otherwise, you would calculate I like.

And you can even see having a TiVo-like thumbs-up, thumbs-down control where after you meet somebody, you give them the thumbs up or the thumbs down, and that feeds into the system to help the system make better pairings for you later. I think it would get to the part where you might turn to your friend or roommate and say, I'm going out to the pub tonight. Would you mind lending me your reputation instead of my own? Mine is a little rusty. I promise I'll give it back to you in as good condition as the way you gave it to me.

This then creates a database of sorts that has open-source elements to it. It's meant to be aggregated and sifted and used, but that if you suddenly imagine the government making use of it, it would be raising some serious privacy issues.

And similarly, I look to nascent technology, still in their first couple of years, like Flickr, where, who would have thought that if you gave people an invitation to share their most recent holiday photos with everyone on the web, and by the way, while you're at it, why don't you tag them with who's in it? You couple that with technologies that allow for facial recognition. There are sites like Riya or MyHeritage.com that allow for this. It means that if you are in a tourist's photograph in the background – it wasn't even your friend taking the photo – that goes up onto Flickr and may be automatically tagged with your identity.

And suddenly, without having to have any surveillance infrastructure of a covert variety, we can start asking these database questions like where has Jeff Jonas been spotted within the past five weeks? And boom, an army of the world's tourists has indicated exactly right where he is, or we can say, who was walking into or out of this consulate or this meeting in a mosque or a synagogue or a church, those kinds of questions. And figuring out whether we should say, well, it's all open source. That's part of what anybody could ask, does that end the inquiry? I think that is a great question for us to ask ourselves before we're in that world.

MR. SHEDD: Before I turn to Alex for a context set inside the intelligence community of the implications of technology in the future and open source, Jeff, do you want to build on what you started to talk about and now what Jonathan has said that it's really fascinating?

MR. JONAS: Yes, I started thinking about – the ACLU came out with something called "How Many Minutes to Midnight?" It's a doomsday clock to a total surveillance society, and it was six minutes to midnight and I'm looking at that thinking, I don't know, could it really be six minutes? So I decided to think about this a little bit. And my conclusion, much like we've just heard is that to me, I believe a surveillance society is not only going to be inevitable and irreversible, but the most interesting thing, it's irresistible. Consumers are doing it. You want GPS and everything so you can find Starbucks, find your kids, and find your 50 best friends, and you're going to publish that on here so you can find your 50 best friends. You're going to want RFID and stuff. You're going to want them in your glasses so you never lose them again.

So the notion that there's a lot of sensors today, we've seen nothing yet and consumers are driving it. And more and more data is being more and more widely available, and it's how the data gets mashed up is going to create extraordinary intelligence for companies and for governments.

MR. SHEDD: Let's talk about the government piece. Alex.

MR. JOEL: Okay. Well, that will be easy.

(Laughter.)

MR. SHEDD: You only have three minutes.

MR. JOEL: Okay. Thank you. (Laughter.) So there's been – a lot of different ideas just were presented here. A couple of things that Jonathan said initially were very interesting that I just wanted to quickly address. A couple of the issues he raised initially I just want to quickly go back to – actually had to do with accuracy of the data and with the actions that you take with respect to the data, if I could go back to some of the initial comments that Jonathan made which were very interesting, and I kind of quickly went through those.

So when you think about what you do with open-source information and then the action that you take based on that open-source information, I think those are important considerations for any government agency to think about. So you have to always – and I think that's one of the important innovations or developments in the intelligence community for the Open Source Center and for all of the open-source activities that are happening.

I think it's a terrific development in the intelligence community that we have the Open Source Center, that the open-source disciplines are developing, and are so, in fact, developed across the intelligence agencies, because we are treating open source not as something that people do casually on the Internet on the side and just are surfing, but are treating it as a separate and independent discipline, intelligence discipline. So we are treating it with a lot or respect, with a lot of care and understanding that this is not something that we can just sort of throw into the

hopper, but has to be integrated with everything else that we're doing as intelligence professionals, and we understand the implications of that information.

And of course, from a privacy and civil liberties perspective, we also have to understand the implications of that information on the rights of Americans and on the rights for a United States person, and how that affects the individuals that we are dealing with. And obviously, in terms of the action that we take on that information, we also have to be cognizant of that. We are taking that information in and putting it into the processes that we use in the intelligence community for analytic purposes.

We don't take that open-source information, and purely based on something that somebody posts on Flickr, or YouTube, or something like that, immediately take that as reliable and use that to take action on a person. We, of course, are analyzing that information in context as part of an open-source discipline. So I think that's an important point to make, and we need to continue to make that as we go through our policies and our open-source training and guidance.

Just quickly on privacy-enhancing technologies, my office, along with a science and technology group within the DNI, has sponsored two separate projects to explore the full spectrum of privacy-enhancing technologies, including the ones that Jeff has mentioned, and IBM and other companies have already pioneered different forms of privacy-enhancing technologies. It's a whole spectrum of them. They're very interesting and they offer quite a bit of promise in this area, but no single technology is foolproof. You have to look at the spectrum of them including audit logs, tethered data, anonymization, the kinds that were mentioned.

I do want to emphasize there is – I know that technology poses a unique challenge for us in the publicly available information area. This is, I think, the real crux of the issue, because as technology pushes more information into what we see on the Internet and what seems to be increasingly publicly available, we have to remember what the definition of publicly available is for the intelligence community. It's information that is available upon request or by casual observation to any member of the public, and we have to distinguish that from what we would consider to be surveillance activity.

So this is something we're going to have to continue to develop and think about through policy guidance and training. And I know it's difficult and we have to continue to develop this further for our open-source community, but I would distinguish that from directing a heat-ray sensor gun. I know that this was not the device specifically in the Kyllo case that Jonathan is talking about, but we're not talking about directing surveillance at a particular person. I would consider that to be surveillance.

And so we have to think about these – it's open-source information. It's something that you acquire because it is available to any member of the public, not because you are directing a particular surveillance technique at a particular person. That would be one distinction I would draw.

The other distinction I would draw is that you, of course, have to relate what you're doing to an authorized mission. So it has to be something that you are authorized to do as part of your

agency. So remember, when I went back to that framework that I was talking about, is this an open-source activity? Is it related to your mission or are you now drifting into a human intelligence activity? Are you developing a human source? Are you actually going out there and conducting something that is really in the realm of human intelligence? Are you doing something in the realm of electronic surveillance? So we're going to have to talk about that some more as we go forward.

MR. SHEDD: I'd like Jeff's perspective.

MR. JONAS: I'd just add one piece of that, is in the scale of publicly available, it's like sitting behind you on your desk is a phone book, or 411.com, and that scale goes to property ownership. I was in Dubai recently, and I'm in a conversation with a lot of people I don't even know over dinner, and somebody is sitting there and pulls up my house and what I paid for it, and says, oh, you live on a golf course. Well, I guess that means that's publicly available. I mean, it helped demonstrate that.

I think a real trick, and this maybe synthesizes what I've learned by having a lot of conversations with the people in the private community, is if you were to shorten it down to the shortest possible sentences, but they all would want is avoid consumer surprise. So it's what is consumers' expectation? And the trick, the real trick, is if you want to catch a few bad guys with low signal, you need to observe a few things they didn't think you were observing. And there lies the tension.

MR. SHEDD: Jonathan, could you elaborate from a private-sector side to what Alex has talked about in terms of the limiting aspects for government in getting access and collating that information as open-source information from your perspective and your study?

MR. ZITTRAIN: Well, the general rule on the private-sector side of things has been highly sub-sectoral regulation. So if you are in the business of renting out video cassettes, you have certain duties imposed by federal law arising from a certain set of privacy invasions that came about during the confirmation hearings where judge – perhaps to be Justice Bork – that no one else in the world has. There are some spotty state-level responsibilities for health protection and then some through something maybe with HIPAA which almost casually as an afterthought imposes some restrictions on data use and dissemination for electronic health records and credit reports.

But for the real aggregate stuff that we're talking about that's kind of the cutting edge, I don't see a privacy framework for that that limits what the private sector can do, which then brings us back to the question, well, gee, if the private sector can do it, why can't the public sector?

There have been some interesting incidents that may point to stuff that will confront us in the future. I remember there was one particular virus that had started infecting a number of machines. There's millions of viruses, so, so far, nothing that interesting, but one person got so frustrated with it – this person had technical skill – that he actually wrote a new virus that hacked into the machines that it could find, looked to see if the old virus was there. If it was, it cleaned it out and then it went to sleep. So it was sort of – it had a kind of Batman theme to it: breaking the law in order to do good.

It raises an interesting hypothetical to me, one that has been bouncing around the cyber law community, such as it is, for over 10 years now. So it was a law student at Yale actually who brought it up first, where he hypothesized, what if you could write a worm that would go out on the Internet, find a way to go into each machine, and simply report back, and only report back, if it found the fingerprint of a file – imagine it's a file that is highly classified that no one outside of government has business possessing – and only if you see the fingerprint of that file on the machine do you report back where you found it. If, in fact, this file has been compromised, whoever has it is a spy operating against the U.S.

I'd be curious to know, Alex's and Jeff's views as to whether in the quiet of the fifth floor at Langley, would you run the worm and see what came back, or would you say, uh-uh, got to – that's a huge search, couldn't possibly do it.

MR. JOEL: Well, we can't confirm or deny that kind of operation. (Laughter.) Well, I mean, any kind of – that's a search of someone's computer so, obviously, you would have to have a warrant for that kind of activity. So anytime you send out something that looks into a computer inside the United States like that, that would be beyond open source, obviously. That's the sort of easy answer.

But the real question I think you're asking is, can you develop technologies that can find a way to address policy challenges in a way that is also protective of privacy? So can you devise something that is designed to find the needle in the haystack while also protecting the hay, and that is so foolproof that can meet Fourth Amendment concerns, meet privacy concerns, and things like that. And I think that if you do that in a transparent way through the – in partnership with the appropriate legal checks and balances, I think that technology can offer solutions in that regard.

And that was part of the exercise that we went through with the two technology projects that we have been sponsoring. We're trying to look for solutions to do that, essentially find the needle, protect the hay, kind of things that we've been trying to figure out.

MR. SHEDD: Let's dedicate the last 15 minutes or so to some questions from the audience and I'll start with this one, and it's open to the three panelists. "Are there strategies to include private and non-private organizations in the process of contributing to open-source database? And along those lines, can these organizations start in centers of excellence, in universities and so forth, if, in fact, the government doesn't want to go down that path in terms of processing of open-source information?"

MR. JONAS: That's consistent with the theme that I have is that I think that there could be a much deeper conversation between technologists and policy folks and people in the privacy community. And I think maybe one of the best examples of this is Tim Edgar, formerly ACLU is now in ODNI. I think that's remarkable and I think anytime that you can extend your conversations into organizations like CDT, conversations with people like David Sobel, now at EPIC. Is he at EPIC now? EFF? Oh, he's at EFF, that's right. And then there's organizations

like IAPP and conferences like CFP, Computers, Freedom and Privacy that I think are really good ways to get that conversation going.

MR. SHEDD: Jonathan, do you have a view or comment on this particular question?

MR. ZITTRAIN: Well, I think it would be fantastic for there to be public-private partnership in helping to pioneer open-source technologies, methods and even dealing with the databases themselves to contribute to a better understanding of the world. I can't help but give an example of that that's very close to home. I'm one of the founders of something called the Open Net Initiative, which has tried to document Internet filtering around the world by national governments.

In 2002, the public had reason to know that China filtered some stuff on the Internet. If you were surfing and you lived in China, there were sites you couldn't get to, but we didn't really know how much and what and all that kind of stuff. So we began by placing a long-distance call simply from Cambridge, Massachusetts, to Beijing as if we were in a Beijing hotel wanting to get online with a modem, and then we played 200,000 questions and just asked for one site after another and saw what we could get to and what we couldn't. That created a database that I think would count as sort of collecting open-source information that moved the ball forward. It worked until the dean got the phone bill, which turned out to be substantial.

But our move now, several years later and several million dollars later of funding from good sources like MacArthur to actually send people into these areas to run more reliable tests and get out before they get arrested, is to actually solicit the public at large to run a small tool on their own machines, so that when they encounter a block at a website, they can click a button to report it and say I can't get there from here. And aggregating everybody's reports as to where they say they can't get to and where the report is coming from, we can create a real-time map of what's filtered around the world.

Very useful information, useful for policy-makers, useful for universities and scholars, and something that the public at large, I think, the same people who might run that old screensaver, SETI@home, which would crunch numbers having to do with radio telescopes looking for intelligent life out there when the machine was idle, I think that spirit might be able to apply to open-source collection and reporting project like that one that are very fertile for these partnerships.

MR. SHEDD: Thank you. Maybe for Alex as a startup: "Please provide a concrete example of an open-source intelligence exploitation activity that you today would consider illegal, absent an approval, FISA court or some other form. And then as that ties into the worldwide net and the web itself, how is the privacy protection enforced outside the United States?" And that's probably a very short answer to that one.

MR. JOEL: Well, I think I've given a sort of couple of examples in my talk already. So for example, if someone, even though information is publicly available, has decided to start maintaining records on individual Americans for no authorized purpose within their agency just

because they find it of curiosity, and they start sharing it around within their office and maintaining files on Americans, I would find that to be improper.

If they start collecting information on Americans because of First Amendment-protected activity and solely for that purpose, they don't like the political views of a particular group and they start collecting information solely on the purpose of those political views and for no other reason, I think that would be problematic.

If they purchase information on the Internet without – and it turns out to be that those records are protected by, let's say, the Right to Financial Privacy Act, or those are credit reports, and they're protected by the Fair Credit Reporting Act, and they've obtained that information without going through proper channels, that would be problematic as well.

You have to be worried about things like if you hack into a website, that's not publicly available information, if you're sort of doing hacking kind of activities, things like that. You have to – of course, it has to be publicly available. It has to be available to any member of the public. That's the definition of open source, and that's what you're allowed to do under the guidelines.

It doesn't mean your agency can't access information through other techniques that are lawful and that are authorized for your agency; I'm just saying this is what open source is. In terms of – I think the question was what other form – is the question about what other foreign intelligence agencies are restricted from doing or –

MR. SHEDD: Or in the foreign arena.

MR. JOEL: In the foreign arena, the rules I'm talking about apply inside the United States and apply with respect to our activities as directed against U.S. persons. So they don't apply with respect to activities that are not directed for U.S. persons. We may have other restrictions based on international agreements with our other – and on foreign laws that we are concerned about, but the rules I'm talking about are for U.S. persons and activities inside the United States.

MR. SHEDD: "With respect to the government needing to identify itself online in terms of, again, if it's intrusive in any way, the question here is, isn't it all too easy for the government to use cutouts, contractors and others, to go what itself, as a government employee, might not go do?"

MR. JOEL: Yes. Well, we have the golden rule under Executive Order 12333. You are not permitted to do through someone else what you are prohibited from doing yourself. So that's the indirect participation rule under Executive Order 12333. It's common sense. So if we are prohibited from doing something, we're certainly not allowed to contract someone else to do that for us. You're not allowed to task somebody else to do that for you, not allowed to go do through a cutout or through a third party. So that is directly in the executive order, and that's carried through in agencies' procedures. So that's something that is a prohibition.

Of course, I'm not naïve, and so I know there are different permutations that people have to worry about, and you have to think that through in terms of how you conduct your activities at each agency.

For all the folks who are from intelligence agencies here, of course, you should consult with your office or general counsel, your own civil liberties and privacy equivalent to my office. We are going to be putting out guidelines – or guidance, not guidelines because that's put up by the attorney general – guidance for the open-source community. We're working on that project with the DNI open-source collection folks to sort of walk people through these issues because they can be difficult ones to deal with.

MR. SHEDD: Thank you. And one last question before we wrap up with the comments, and I'll start with you, Jonathan, because it is directed at you. You mentioned the use of politically available technology to conduct operations in your example that you provided. "What about the integration of publicly available products to conduct Internet information collection?" I think the question goes to the heart of building on that initial capability with additional technologies on top of that. Where's the end in sight in terms of using that technology for open-source collection?

MR. ZITTRAIN: I think it would be welcomed to use that kind of technology. Jeffrey has pointed out ways in which, what would otherwise be innocuous, might be a problem, if it's done for the wrong purpose, which only the person doing the collection or analysis would know. But that would otherwise – sure, if you can get some new technologies to help you make sense of something that's publicly available, more power to you. I even think to the fellow who found out, or at least had good reason to think that some of the gymnasts from China in the Olympics were not the right age, he just did some great gumshoe open-source work that once it was done, it could be replicated and others were amazed by it.

I guess the only cautionary thing I would think of would be – I think the line between passive collection, sitting in an office and reading the web or reading the paper, the standard, I think the old model of open source – you just kind of let stuff come to you or get delivered by the postal service – that that is starting to blend with things that involve some form of participation or push.

If you participate in a message board that is talking about jihad-related topics or something, a very fertile area, a public message board, you start to befriend people, in some ways, it's open source. It's completely right out there. On the other hand, the minute, I guess, you click enter or send, somehow you are engaged in some activity that is starting to raise issues that maybe mere passive observation wouldn't.

And how to figure out, well, jeez, how do I know if there are American citizens behind those aliases online, and therefore, I need to flag myself – by the way, everybody, I hate to end the conversation on the board, but I am from an intelligence agency, but please, as you were; let's talk about that. That raises some interesting questions. What's on American soil, what's not? Who's an American citizen or a resident alien or not? And you don't want to hamstring our agencies, and at the same time, you don't want to see the lines completely obliterated. They were there for good reasons, as Alexander points out.

MR. SHEDD: Jeff.

MR. JONAS: I see a future that's beyond search. I think the idea that everyone has to think of the question and pose the question is going to change. I think data is going to be getting commingled. It's going to be commingled in the network cloud, and intelligence is going to be pushed to consumers and to organizations about what it thinks you need to know. And I think that's – and I that's going to pose a lot of interesting challenges.

MR. SHEDD: Do you see the information in the social networks, for example, getting blended into that whole process as well?

MR. JONAS: Absolutely, for sure, and I think consumers are going to gobble that up. And I think companies are going to figure out how to do that and deliver more and more precise services as people try to continue to optimize their lives.

MR. SHEDD: Well, you've segued into some concluding remarks. Any other thoughts in terms of what you want to leave the audience with before I turn to Jonathan and Alex?

MR. JONAS: No.

MR. SHEDD: Okay. (Laughter.) Jonathan, some closing views in terms of the future and beyond where you've gone already?

MR. ZITTRAIN: I think that we have a generation of kids, so-called digital natives, who are true virtuosos with this technology and with doing interesting things with it and with a very different set of scruples about what counts as private and what doesn't. I think there's an advantage in that, and just as there's a time when you might put out the call for people with certain language skills, even if you're going to sit them down and do whatever FBIS has become – I forget what they call FBIS these days – yes, this would be a great time to start some new summer internship programs, get some high school kids, get some college kids through the ranks and I don't think they would see open source at all as a backwater. There's plenty of reason to think this is where a lot of the advances can take place.

MR. SHEDD: Thank you.

Alex, final word.

MR. JOEL: I feel like I've been a bit of a damper at the party, and I didn't mean to be. I will say the technology –

MR. SHEDD: I think you've actually provided reassurance.

MR. JOEL: Oh, okay. Well, I hope so. The technology is advancing at an exponential rate, and I think our rules and policies advance incrementally. And I will say human nature is the same as it always has been for centuries. Human nature is immutable. And I think you'll find that our

rules can be applied very flexibly and allow our intelligence community to meet the needs that we need to meet in order to make our national security mission successful.

So despite my having provided you with a framework that might give you the impression that we have the restrictions – we do have restrictions; they are important ones – you need to work with your office or general counsel and your civil liberties and privacy folks who understand what it is that you need to do to accomplish your mission at your office. And they do provide flexibility so you can continue to do your work and collect open-source information to meet the needs of the country. And I think you're doing it very well so far. And we're going to be able to continue to do it going forward.

MR. SHEDD: Well, thank you. And Jonathan, Jeff, Alex, thank you for your time, the thought that you've put into this. It is a brave new world and a lot of challenges ahead, but a lot of opportunities. And we will hire those high schoolers and young university students to carry it forward. Thank you very much. (Applause.)

MS. HORNE: Thank you, gentlemen, for that wonderful and interesting discussion. We look forward to furthering that discussion over the coming months and years.

We'll now move into our next session. Please, don't forget that we have a wonderful exhibition across the way and take advantage of that. We will ask you, as we prepare for the appearance of General Hayden with your help in facilitating that appearance. We'll need to clear facilities quickly to allow for that visit. So we'll notify you in the next session of how you can help us with that. So thank you so much, and enjoy the rest of the day.

(END)