Remarks and Q&A by the Principal Deputy Director of National Intelligence
Dr. Donald Kerr

2007 GEOINT Symposium
Sponsored by the United States Geospatial Intelligence Foundation

Henry B. Gonzalez Convention Center
San Antonio, Texas

October 23, 2007

BRIGADEER GENERAL MICHAEL G. LEE (Ret.): But probably the key and our hardest job is our next keynote speaker. A lot of the issues that we have are cultural issues; a lot of the issues are policy issues, and certainly the next keynote speaker is in a great position to influence that and help make some changes as we work through. And it's my great pleasure now to introduce the Honorable Don M. Kerr. Many of you know him already, but on October 4, 2007, Dr. Kerr was confirmed by the Senate by unanimous consent as the principal deputy director of National Intelligence, second in command to the office of the director of National Intelligence after Director Mike McConnell. He was officially sworn in on Tuesday, October 9, 2007.

Since July 2005, Dr. Kerr has served as the 15th director of the National Reconnaissance Office. Dr. Kerr was appointed deputy director for science and technology at the Central Intelligence Agency in August of 2001. From October 1997 until August 2001, Dr. Kerr was assistant director of the Federal Bureau of Investigations, where he was responsible for the laboratory division. Dr. Kerr's prior government service was with the Department of Energy from August 1976 through July 1979.

Dr. Kerr held several key executive positions in private industry. From 1996 to 1997, he was the executive vice president and director at Information Systems Laboratories. From 1993 to 1996, he was corporate executive vice president and director at Science Applications International Cooperation, SAIC. Dr. Kerr was the fourth director of the Los Alamos National Laboratory from 1979 to 1985. Please join me in a warm round of applause for the Honorable Doctor Don Kerr. (Applause.)

DONALD KERR: Thank you very much. Well, now that the truth is out and you know that I don't hold jobs very long, I'll try to tell you what I'm thinking about the one I just embarked on. It is really a privilege to come back to GEOINT in my new role as principal deputy director of National Intelligence. And as I settle into this job, I find myself thinking back to the beginnings of other jobs in the past. In some ways, they are all similar; there's a lot of information coming at you very fast; there are new issues, new people, and most importantly, new cultures, to learn about. But for me, one pastime in particular stands out.

As you heard, from 1997 to 2001, I was an assistant director of the FBI, responsible for the laboratory division in a period of what some of you might remember was a period of some turbulence. Ten months after I came on board, our embassies in Nairobi, Kenya, and Dar es Salaam, Tanzania were attacked by al Qaeda. My explosives unit was the one in charge of processing the bombing scenes for evidence that could lead to attribution.

That's when I first experienced the smell of decaying human remains on a large scale. It's something that you'll never forget. It was also my first real, face-to-face confrontation with the damage that terrorists were trying to inflict on our nation. After those bombings, we placed Osama bin Laden on our FBI "Ten Most Wanted" list. It was his first significant attack against our nation and its people.

My next similar challenge at the bureau was the attack on the USS Cole two years later. I was there within a few days and, again, my people handled the bombing scene, and also assisted in recovering the remains of the 17 sailors who lost their lives. Those were some of America's first glimpses of al Qaeda. Now that we have seen the full breadth of their intentions, both at home and abroad, we ask the question: What does it mean to be secure in an era of transnational threats emanating from stateless enemies?

To answer that, we really need to realize what a loaded word security really is. When I'm at work, and throughout my day, security is safety, as a barrier against physical or emotional harm. When I go home at night, security is privacy, as an expectation of freedom from unnecessary burdens. In the intelligence community, we have an obligation to protect both safety and privacy, and over the course of GEOINT 2007, as we talk about the hows of new technologies and tradecraft, I'd like to take a step back right now and talk about the whys.

Safety and privacy – it's common thinking that, in order to have more safety, you get less privacy. I don't agree with that. I work from the assumption that you need to have both. When we try to make it an either/or proposition, we're bound to fail. You can be perfectly safe in a prison; but you certainly aren't free. And you can be perfectly free in an anarchist society; but you certainly aren't safe.

The balance is one we've been working to perfect throughout my time in the intelligence community. That's of course a very hard thing to convince people of. Movies like "The Enemy of the State" and "The Good Shepherd" have poisoned the well of public opinion in some ways, and make people think we focus on safety mainly for governmental activities to the exclusion of all else. My takeaway message for today: We're not. You can – and we do – have both. We have always been a free people who can defend ourselves without giving up the liberties that animate us to action.

These two components of security – safety and privacy – are the crux of much of what we're doing in the intelligence community. And it's in that vein that I'd like to focus my remarks today.

Safety is the component of security that people probably think of most frequently. It certainly dominates my day at work, and you need only to pick up a newspaper to know exactly what I'm talking about. And in terms of helping to ensure our safety when it comes to crises like disaster relief and humanitarian issues, GEOINT is fast becoming the source of first resort.

This past August, in advance of Hurricane Dean's landfall, GEOINT provided a five-day forecast track for the storm, plotting out an hour-by-hour timeline of where the storm would hit, at which point it would turn into a tropical storm and then depression, and the necessary buffer zones along the away. Right after Dean hit, while most were still either evacuated from the area or still taking cover, GEOINT provided damage assessments, focused on the status of major roads, power plants, hospitals, piers and airstrips.

Even for earthquakes – like the Kailau Kona Earthquake this time last year in Hawaii – GEOINT was able to pinpoint damage in relation to military bases, wastewater treatment plants, and hazardous material facilities. From Typhoon Ioke to Tropical Storm Ernesto – tornados in Florida to floods in Ohio, GEOINT has provided street-level imagery, and with the value-added expertise of analysts, been able to tell which bridges are out, which roads are impassable, and where floods have overtaken land.

The value-added by analysts cannot be understated. For many of these disasters, NGA deployed its Domestic Mobile Integrated Geospatial-Intelligence System – there has to be an acronym for that, the DMIGS– a GEOINT ops center on wheels that allows analysts to deploy to a crisis location, and provide on-the-spot GEOINT analysis and production.

For all that GEOINT is and has become, though, it can only be part of the solution. From a policymaking perspective, I work to foster safety by protecting the nation from strategic surprise, and the tools provided by GEOINT are invaluable. But what we're best able to protect against surprise is through sharing what we know with each other, and encouraging greater integration and collaboration across the intelligence community, just the theme of this conference. For example, while NSA analysts are busy deciphering overseas signal intelligence from a known terrorist, NGA imagery analysts can be monitoring the movement of trucks that he has ordered – a lead perhaps provided by a CIA human source. It's all source collection and collaboration at its finest.

You, of course, would think that information sharing would be an easy sell. But, as many of you know, in some quarters of our intelligence community, you'll still find an atrophied mindset that everything we do should be secret from everyone else – even those with clearances. If 9/11 taught us anything, it is this: We have a responsibility to provide intelligence to others, whether it's FBI talking to CIA or the Coast Guard communicating with state and local officials. To allow for greater safety, we need to get better at managing secrecy. We still need to protect some of the most sensitive sources and methods, but we also need to learn how to develop, for example, imagery-derived products that mask the source and provide actionable intelligence. Fortunately, we're making progress in that work. And I'll share one example.

Earlier this month, we cut the ribbon – literally – on a center to help us better share information and make decisions across the entire intelligence community; we opened the National Intelligence Coordination Center, or as some call it, the NIC-C. It is a place to bring together all collection systems and agencies and will increase our opportunity to optimize deployment of our collection capabilities. It will help us with rapid adjustment in response to crises and give us a better way to stay responsive to tasking from the most senior echelons of our government.

The concept of the NIC-C draws directly on the recommendations of the 9/11 Commission and the Intelligence Reform and Terrorism Prevention Act. It will improve our ability to protect from strategic surprise, manage collection resources, and focus on the nation's top priorities. But I've just described something that lives at the top of the intelligence community. Is there anything for it to connect to? How do we bring this to action? Another theme that I should mention, and Admiral Murrett very kindly mentioned it earlier in his talk, a few of us comprised what we call the gang of four for a while. This was comprised of the directors of NSA, NGA, DIA, and the NRO meeting without adult supervision, trying to think about the most important things we could accomplish with the authorities and resources we had.

We started out thinking a great leap would be an integrated ground architecture. And we've now gone beyond that in our thinking because what we're really talking about was an integrated intelligence architecture. The major nodes in this architecture, not surprisingly, would be critical facilities like those Admiral Meret mentioned, NGA East, NGA in Saint Louis, data centers that may come into existence for the community; some of the key nodes that NSA has; not just NSA Washington, but the regional SIGINT sites. And of course, the NRO ground stations. There will be other nodes as well and importantly, the four of us control a lot of the connectivity that would provide the infrastructure to support this architecture. What we didn't have necessarily within our control was the ability to set standards that would allow for interoperability and interconnection. And to that end, we're now reaching out to the CIOs of the Department of Defense and the intelligence community.

And we're hoping that over the next year, we can bring some of this to fruition and have something for the NIC-C to talk to in terms of moving from a high level of thinking about our national priorities to being able to collectively task problems against the myriad of collection capabilities that this country has. So our vision is to be able to do that and the idea of the gang of four was, how do we enable that with the resources that we control?

Now, security through collaboration raises questions among some people. You have all heard the discussion of pre-9/11 and the existence of the wall in the Justice Department that separated law enforcement and intelligence information. The concern, of course, was that grand jury information, other privileged kinds of information, would somehow improperly escape into the larger world. And I guess, on the intelligence side, you could argue there were suspicions as well. They've all been well-documented. And we've started to bring down those walls as we require information sharing between intelligence, Homeland Security, and Defense agencies, and law enforcement. Some have grown uneasy. People are asking, just what is it they're sharing?

And that leads you directly into the concern for privacy. Too often, privacy has been equated with anonymity; and it's an idea that is deeply rooted in American culture. The Long Ranger wore a mask but Tonto didn't seem to need one even though he did the dirty work for free. You'd think he would probably need one even more. But in our interconnected and wireless world, anonymity – or the appearance of anonymity – is quickly becoming a thing of the past.

Anonymity results from a lack of identifying features. Nowadays, when so much correlated data is collected and available – and I'm just talking about profiles on MySpace, Facebook, YouTube here – the set of identifiable features has grown beyond where most of us can comprehend. We need to move beyond the construct that equates anonymity with privacy and focus more on how we can protect essential privacy in this interconnected environment.

Protecting anonymity isn't a fight that can be won. Anyone that's typed in their name on Google understands that. Instead, privacy, I would offer, is a system of laws, rules, and customs with an infrastructure of Inspectors General, oversight committees, and privacy boards on which our intelligence community commitment is based and measured. And it is that framework that we need to grow and nourish and adjust as our cultures change.

I think people here, at least people close to my age, recognize that those two generations younger than we are have a very different idea of what is essential privacy, what they would wish to protect about their lives and affairs. And so, it's not for us to inflict one size fits all. It's a need to have it be adjustable to the needs of local societies as they evolve in our country. Eventually, we can only hope that people's perceptions – in Hollywood and elsewhere – will catch up.

Our job now is to engage in a productive debate, which focuses on privacy as a component of appropriate levels of security and public safety. This is work that the Office of the DNI has started to do, and must continue and make a high priority. This careful balance we need to strike, however, is nothing new. With the advent of telephones, we entered a new frontier that required careful balancing between safety and privacy. We faced this challenge again at the end of the '70s in the aftermath of the Church-Pike Hearings. And now, in the era of new technologies, we have to work to continue to keep that balance, to earn that trust, and re-earn it every day through our actions. But we also have to be willing to reopen the laws and regulations that were based on technologies that existed 1978 and adjust them to the realities of 2007 and 2008.

Twenty-four years ago this morning, a yellow Mercedes-Benz delivery truck pulled up at the Beirut International Airport where the first battalion 8th Marines were headquartered. The truck, loaded with more than 12,000 pounds of explosives, was masquerading as the regularly scheduled water truck. The driver turned it onto an access road leading to the Marine base, circled the parking lot, and, accelerating, crashed through the barbed wire fence and into the lobby of the Marine headquarters; 240 U.S. Marines and sailors were killed.

At that time, it was called the largest non-nuclear blast ever deliberately detonated on the face of the Earth. The Hezbollah militants, like the al Qaeda terrorists whose work I saw first-hand in Kenya and Tanzania, were trying to do more than simply make a political point. They sought to inspire fear – fear that eats away at the sense of security that we all hold dear.

We didn't let them then; we won't let them now. The challenges we confront today – and seek to counter through our intelligence community using GEOINT – are nothing new to our nation. Our commitment to safety and privacy are nothing new to us and they are values that we must continue to protect as we learn to do our intelligence job better. To share information better, we still have to have an underlying commitment to these two principles.

And so, I wanted to share that with you today as, if you will, the non-technical piece of this discussion that we have to have. It's a debate we need to have in the United States. It's not necessarily best carried out in hearing rooms; it's certainly not best carried out in television environments where people just scream at each other. But I think it's going to take serious, long-term debate for us to all get it right. So thank you very much for your time and attention. I look forward to working with all of you.

(Applause.)

GEN. LEE: Thank you very much, sir. That was certainly, certainly that we're all concerned about as Americans and something that the general public, they don't want to talk about, but they are all concerned about it. I have a, I think, a very good question to start. There's been some controversy about the DNI's endorsement of a plan for DHS to take over the civil applications committee and expand its work to allow for greater domestic use of remote-sensing imagery for homeland security and the law enforcement applications. Is this enemy of the state for real? What's your take on this?

DR. KERR: Actually, I would call it a ringing endorsement of some great work that was done by the civil applications committee. Many of you had interactions with it. You know that this has served the scientific community well; it serves civil agencies of the government well, the Forest Service, for example, uses data to find the hotspots and fires of a lot of things related to disaster relief.

One thing by charter – and the way it was set up, it wasn't able to do well – was to provide access for law enforcement to some of those sorts of data. The proposal that's moving forward to move this capability under the cognizance of the Department of Homeland Security, it's, from simple activities three things: support the scientific community, continue to support the civil agencies as they do their job, and to study ways in which it could serve to link law enforcement under the appropriate responsibilities and equities, to provide them assistance as well.

That, in fact, was posed in the stand-up language as something to study and develop. Unfortunately, when it was first expressed to the press, it wasn't clear that that needed study and some thinking before it happens. And so I think what we're going to see is some careful discussion. But the point that everybody should take away is, the rules under which, for example, GEOINT, is used domestically will not change. They are still in place. Admiral Meret, in fact, will continue to be the release authority under appropriate legislation for all such data acquired domestically. And this proposal does not change that in any way.

GEN. LEE: Thank you very much. Next question, can you describe any progress with ICA number two?

DR. KERR: I'd be happy to, yeah. ICA number one was, for me, a somewhat problematic experience. And the reason was that it started in a rush; it was intended to try to inform a budget decisions process; and didn't really have a very fulsome analytic capability associated with it. I made the mistake of telling people that and, for my pains, was rewarded with the opportunity to provide quite a lot of analytic support to the second round.

And I think ICA two has produced a much sounder set of recommendations. And I have a lot better understanding of some of the collection systems because, in fact, the agencies responsible for them were tasked to do a lot of the analytic work in support of the ICA. That doesn't mean that they were given the opportunity to spin their results in all of the directions they wanted to. But it does mean that good systems engineering was applied in depth in areas where it was truly needed. And so, I think it's been a really good evolution in the ICA process. And I think it will be part of the Intelligence Community Activity for the foreseeable future.

GEN. LEE: Thank you very much. Sir, how would the DNI incentivize corporate behavior to have industry and government partner to obtain the maximum collaboration of solutions?

DR. KERR: One of the things that the DNI and I have actually talked about is that up to this point, the Office of the DNI has not had the kind of relationships with industry that might lead us to more informed decisions, more appropriate decisions, about roles and missions. It's not that we want to substitute for what the agency is responsible for executing program due with the industries that support them so well. But there are at time higher-level concerns that relate to policy decisions in Washington where, in fact, our ability to represent the entire intelligence community and its needs could be helpful to industry and to government both.

In times past, those would be issues like, would we ever authorize the R&D tax credit for more than one year at a time. Well, might as well give up on that; it's never happened. But there are other things that are the consequence of government decision that really define the industrial environment that you all work in and we need to be informed on that. And we're going to be looking for opportunities, in fact, to reach out more than has been the past ability in the early standup of the office of the DNI.

GEN. LEE: Next question. One significant barrier to effective and timely collaboration is the absence of a multi-level security system. What does the ODNI position in the list?

DR. KERR: I think we're interested. We'd like to see something that could be tested, made to work in our environment. We recognize that a multi-level security system is going to be, of course, largely software. It's going to be written by people like all of us in the room. It's going to have mistakes in it. And at the end of the day, our approach is not going to be so much talking about multi-level security, but in fact, as leaders of the community and managers of programs, what levels of risk are we willing to assume knowing that we're depending on a product of this sort?

So we have to have it in order to meet some of the expectations that are out there. But we also have to understand that risks will come with particularly the initial products. And we have to be prepared to, in effect, stand up and say, I was willing to take that risk because the benefit was so high.

GEN. LEE: Thank you. Having just come from being director of the NRO, what lessons did you learn?

DR. KERR: (Chuckles.) That's a really friendly question. (Laughter.) Let's see. The first point I learned is that not one point zero people are the same no matter what acronym they work under. Second, organizations like the NRO and others I've been associated with have great confidence in their abilities, great pride in their achievements, and so, great skepticism about the need to change and adapt to a new environment. And so, one of the things that I spent time on in my tenure at the NRO was trying to think about what role it would play as it evolved form its, if you will, very strong, Cold War set of beginnings, really worrying about first, targeting, second, arms-control monitoring and the like, to a situation we find today where systems that are the descendants of the early ones are being used to support the real-time fight.

That's a big difference; that's what's led to thinking about integrated architectures; it's what's led to trying to use lessons learned in the SIGINT world and bringing them over to the GEOINT world. The SIGINT world has been in the real-time business for a much longer period, so there are a lot of good lessons to be learned there.

GEN. LEE: Could you elaborate on the notion that privacy does not equal anonymity? What are the implications?

DR. KERR: It's a really good question because, in fact, it's a personal question that everyone, in a way, has to answer for themselves. But I think today, you know, I'm willing to call up, pick the vendor of your choice. I'm willing to share my credit card number and expiration date with a person I have never seen, have no idea whether they've been vetted or not. I've certainly been able to get past being anonymous in that transaction. And of course, you multiply that by all of the transaction that you're involved in every day.

I was taken by a thing that happened to me at the FBI, where I also had electronic surveillance as part of my responsibility. And people were very concerned that the ability to intercept emails was coming into play. And they were saying, well, we just can't have federal employees able to touch our message traffic. And the fact that, for that federal employee, it was a felony to misuse the data – it was punishable by five years in jail and a $100,000 fine, which I don't believe has ever happened – but they were perfectly willing for a green-card holder at an ISP who may or may have not have been an illegal entrant to the United States to handle their data. It struck me as an anomalous situation.

So this is not something where groupthink works for an answer. I think all of us have to really take stock of what we already are willing to give up, in terms of anonymity, but what safeguards we want in place to be sure that giving that up doesn't empty our bank account or do something equally bad elsewhere.

GEN. LEE: Exactly. And the question was signed by anonymous, so – (laughter).

DR. KERR: A TFA arrest, somebody says from the front row. (Chuckles.)

GEN. LEE: Dr. Kerr, why doesn't the gang of four include CIA? Shouldn't this leadership team be the gang of five? CIA, HUMINT, and all source analysts must move along with the IC cultural reforms.

DR. KERR: I could have written that question. That's good.

Actually, General Hayden is planning to participate so it's already moving to the gang of five. And Bob Mueller, the director of the FBI, would like to find a way to come into this construct as well. The reason it started with the four of us was that we all had a common reporting line within the Defense Department. It was easy for us to hide; it didn't take a lot of policy judgments for us to get together to do it. But now that it's started, it's expanding, and it's going to have to serve the whole community at the end.

GEN. LEE: Next question. Would you comment on IARPA, its mission, and place within the intelligence community?

DR. KERR: I'll comment, but not answer your question I guess. IARPA is still a construct waiting for life to be breathed into it. One part of that has to do with the present effort to select someone who would be the leader of this activity. A second is to define what it is. Those who have studied DARPA and IARPA and DARPA as they've changed names over the years. There was a Dave Mann DARPA, a Steve Lucchesi DARPA, Craig Fields had a DARPA. Larry Lynn had one. And today, and rather tomorrow, you'll hear it from Tony Tether who's put his imprint on it since 2001. There isn't a single DARPA over time; it's evolved to meet the needs of the Defense Department as they've existed in different periods.

IARPA is a play on words, but it may turn out that the DARPA operating model won't work for the intelligence community at all. It may not be the case that all of the science and technology needed for our community can be attained by grants and contracts. We may have to find other means as well. So I would consider it work in progress, work that needs to be informed, in fact, by discussion with people who are here and some serious thinking about how it will add value to the community without becoming just a separated entity that's got a bit of a budget to support basic work, long-term work, but without any clear connection to the programs that might benefit from it.

GEN. LEE: Sir, and one final question. And we saved the congressional question for last. What challenges are there to ensure congressional and DNI resource support for multi-INT initiatives that are not accounted for using the traditional program's specific lineages?

DR. KERR: That, in fact, is something Mike McConnell and I are talking to the committees about now. There are things that fit. For example, in the NGP, the normal source of funds for NGA, similarly with the NRP for the NRO, the CIAP, but in fact, of a lot of the things that are needed by the community cut across. One approach is that we'll actually budget for them in something akin to the old community management account and then, apportion the funds to the different agencies as they collaborate in carrying the program out. If we do that, that forces us to think about having a, if you will, a program manager in the DNI level.

Another approach that we're weighing is to have a particular agency serve as the executive agent for the community for certain kinds of these activities. And we haven't resolved which is best. My guess is we're going to see a little of both for awhile until we understand what works and, in fact, where we can attract the right people to execute such programs. There have been a few small successes at the DNI level to push some things across the community. We need to get more experienced before we can say there's a single model that works.

GEN. LEE: Sir, thank you very much for those insightful remarks. Please join me in thanking Dr. Kerr.

(Applause.)

(END)