SPEAKER:

AMBASSADOR TED McNAMARA

PROGRAM MANAGER, INFORMATION SHARING ENVIRONMENT

AUGUST 22, 2006

AMBASSADOR MCNAMARA: Thank you very much, Rich, for that very kind introduction. Good morning. It's a pleasure for me to be here with you today. It's a big conference and it's an important conference, and I'm going to talk to you today about the theme of today's conference, and I think probably the theme of much of the work that we're going to be doing in the future weeks, months, and even years, and that is expanding that intelligence environment that Rich just referred to.

But before I start, I'd like to introduce myself and also the position that I hold and the office that I head because I've found out over the last few months that I've been on the job that there's a good deal of confusion and misinformation about what the program manager is, does, and what the office of the program manager is designed to do.

By way of background, the position of program manager was established in the Intel Reform and Terrorism Prevention Act of 2004. Specific provisions of that act provide for the position of the program manager and give it government-wide authority to plan, to oversee, and to manage the information-sharing environment. My mandate is to assist the president and government agencies in developing and operating the information-sharing environment and then to monitor and assess the progress of that ISE, as it's called, while it's being set up and has got underway.

I'll briefly note what the program manager's office is, what the program manager's position is, and what it is not. First of all, what it is. It's a small office of about two dozen people located in the Office of the Director of National Intelligence and therefore part of the intelligence community. What I'm not is I'm not a CIO, nor do I pretend to be one because that wouldn't work at all. I'd be found out in about five minutes. Instead, what I do is I try to help develop policies, procedures, guidelines, rules and standards that are implemented by the federal agencies that handle terrorism information. What I am is a facilitator, a facilitator among all the ISE's participants, especially among federal agencies. And in

particular I'm assisted by an information sharing council, an advisory body that was also established by the IRTPA.

Next, we're not an intelligence agency; that is, we're not just concerned with intelligence. We're responsible for all terrorism information, whether or not it's intelligence. And there is a lot of information out there; in fact most of it, which is not intelligence. There's law enforcement information, there's defense information, there's diplomatic information, and there's homeland security information. Of course there's also intelligence information.

Let me pause for just a minute in the what we are and what we are not to say that those five communities that I've just listed are very important in understanding the information sharing environment and in understanding what our task is in setting it up. And I'll repeat the five of them and will refer to them frequently throughout my remarks today. Law enforcement, defense, diplomatic, homeland security and intelligence. We are responsible in the program manager's office for working also with state, local, tribal governments and the private sector, and additionally with out foreign allies and partners regarding their participation in the ISE. They are not onlookers; they are participants.

What we're not is we're not a substitute for federal departments and agencies. The agencies are responsible for establishing and implementing the ISE, not the PM. We manage, we oversee, we coordinate the implementation that takes place throughout the agencies and the governmental entities that we deal with.

Finally, we're a temporary office. We'll cease to exist when the ISE is up and running. And let me give you my working definition of what it is the information sharing environment. The ISE is a structure and a mechanism designed to facilitate sharing terrorist information by using agreed policies, practices and technologies to ensure that information is shared rapidly, effectively and securely among federal, state, local and tribal authorities, the private sector and our allies and partners.

Now let me get to today's theme, and I particularly appreciate the opportunity to join you today on a day when the conference will focus on extending the intelligence enterprise. The intelligence community is operating today in a world where the business of the IC – of the intelligence community – must be deeply intertwined with nontraditional partners. This is a dramatic change from the years of the Cold War when only three of those five communities that I've just mentioned were focused on national security. And indeed one of those five did not even exist: homeland security.

In this new world, therefore, I interpret extending as meaning reaching out; reaching out beyond the IC to new consumers of the intelligence that we produce, reaching out beyond the IC also to gather in the information that the IC needs, but does not have in this new environment.

It is in a sense holding out a helping hand and getting a helping hand in return. It is, in short, not a one-way street. The lanes in the road – that famous or infamous phrase that we've been dealing with in the federal government these many months – the lanes in the road carry traffic in both directions. In fact, what we're really talking about is interlinking the intel enterprise with other information management enterprises which are not intelligence orientated, but which have much valuable terrorism information to offer the IC and which need valuable information that the IC has gathered if they are to do their jobs.

Today, around the globe our nation's interests, our infrastructure and our people are at risk of being targeted for attack by extremists who desire to destroy the economy of the country, to cripple our society and to kill as many Americans as they can. Since the mid nineteen nineties we have been facing a new phenomenon that has been characterized quite accurately as catastrophic terror. The protection of our national security is a top priority for our intelligence community, our law enforcement personnel, our diplomats, our military and our newest defenders: the homeland security people.

While these instruments of our national power are mighty, I believe that we will defeat catastrophic terror only when those instruments of power are strategically integrated with those local and state-based strategies used by state, local, tribal authorities to prevent crime, reduce fear and improve the quality of life in our towns and cities across the country. Furthermore, given that we live in a nation where most of the infrastructure that's attractive to terrorists is run by the private sector, we need to include that sector in our strategic integration also.

We live at a time when local police officers walking the beat or a detective investigating a gas station robbery or a cigarette smuggling ring, or narcotics trafficker can uncover a terrorist cell and all three of those have happened already. I'll mention it later. And even when the attack is not prevented these same agencies perform essential roles in response and recovery. Therefore, our state and local and tribal partners are now a critical component of our national security capabilities as first preventers and as first responders.

But we also live in a time when terrorism in London, Madrid, Bali, Moscow, Toronto and elsewhere can result in major changes in the way we live and work in the U.S. Those faraway events change our calculations of the risk and potential dangers inside the U.S. and anybody who came to this conference by air knows that the events of London changed dramatically the way we come here on aircraft today as opposed to just a few short weeks ago.

Because these effects affect the planning and deployment or first preventers and first responders inside the U.S., those local and state organizations need that information available at various levels of control including sensitive but unclassified and classified so they can make the right decisions at their level about what they need to do.

In brief, the enemy is not going to strike through the Fulda Gap; it's going to strike in our cities and our towns, it's going to strike our people and our infrastructure. This means that our ability to use the information that lies outside the U.S. is essential to our security inside the U.S.

Let's recall that every one of the many al Qaeda leaders that have been killed, captured or arrested since 9/11 has been killed, captured and arrested outside the United States. And that's happened because we cooperated with other nations, many of them Muslim nations. These are our partners in this effort and these partners are all nations that feel themselves in danger from al Qaeda. Additionally, of the many thousands of terrorists put out of action since 9/11 – and there indeed have been many thousands around the world – less that 10 percent were put out of action inside the United States. That makes international cooperation, including sharing of terrorism information, a major part of our effort in this new protracted struggle with international terrorists.

Does this not tell us loudly and clearly what we must do to be successful against these fanatical extremists? I think it does. Protecting this nation from terrorist attacks begins far from our borders and continues all the way to the cop on the beat in our cities and towns. This is the new post-Cold War reality we must face. As we did during the Cold War, we need to understand what motivates our adversaries, what they intend to attack, how they intend to attack, what their modus operandi is. Our ability to understand the enemy comes from acquiring information about the enemy and ensuring that this information is used as the driving force behind prevention, response and recovery efforts.

Unlike during the Cold War, this information will oftentimes be gathered and held by those who operate outside the intelligence community. At the same time, information and intelligence held by the information community is needed by these non-IC organizations so they can protect us from attack or be prepared should an attack occur.

The information sharing will be achieved through the information sharing environment: the processes and technologies that facilitate the sharing of information to those who need it, for those who need it and for those who should have it and those that need it but don't have it. This is what I understand by extending the intelligence enterprise. Success will come by extending the intelligence enterprise so that it becomes more interlinked with the information outside the intelligence community with partners at home and abroad.

What does this extension of the intelligence enterprise mean from the perspective of how the IC will operate? Well, essentially the IC will not change the mission, but it will change how we carry out the mission. Clearly, the IC will continue to carry out its traditional missions to collect, process and analyze intelligence and to get that intelligence to the decision-makers. What I'm saying is that the national security decision-makers are different and it's a different mix from the decision-makers of the Cold War period. They are not all in the federal government. In supporting efforts to protect the homeland, the intelligence community must now look at how to better gather and utilize information from a larger set of partners and how to securely share information with a larger set of consumers and end users.

In sum, these non traditional partners and end users fall in to three categories: they're the non-intelligence community of the federal government; secondly, they're the state local and tribal governments and the private sector; and thirdly, foreign law enforcement and homeland security organizations of our partners and allies.

This information sharing as I said is a two-way street. Improved information sharing with such groups will produce better intelligence. This morning and today and tomorrow you'll hear a number of presentations designed to enhance your appreciation and understanding of this central fact of the new world we're facing. Let me talk about where we are now in developing the framework for the information-sharing environment – today's information-sharing environment.

Today, information sharing is extensive within each of those five communities that I mentioned originally. Compared to the pre-9/11 period we're doing much better sharing inside the law enforcement community and inside the federal intelligence community, but we're still deficient in sharing between and among federal communities. The system is even more deficient at sharing out to the state and local

levels and between and among states and localities. Additionally, state and local and tribal levels seldom share their terrorist information in an effective manner with either the federal level or with each other.

We've come a long way in information sharing since 9/11, but we – and by "we" I mean all of us in this room – we have a long way to go before that sharing will be satisfactory. It's not easy or fast to construct an information sharing system where none existed before. It means changing policies, business processes and institutions. In short, it means changing cultures. But we'll get there. We've been working in concert with federal state and local officials on a framework that once it is implemented will enhance the sharing of terrorism information at all levels of control. There's now a general acknowledgement of the main principles of such a framework.

Five essential elements of the framework are: first, there needs to be a coordinated federal inter agency group responsible for vetting, packaging and disseminating terrorist information to state local and tribal authorities and to the private sector. Secondly, that this federally coordinated information should be identified as such and should move to the state and local levels clearly distinguished from the mission-specific and agency-specific information that will continue to move as before in agency channels.

Thirdly, a new IC should organize itself in a federal manner. We do things better when we do them federally. And to do that, state and major urban area fusion centers, must assume a much larger and more important role in the information sharing environment through a national integrated network of these fusion centers.

There are about 40-plus fusion centers that have been set up by the states, largely at their own initiative. These fusion centers at the state level can and will have to play a valuable role in processing and disseminating information collected at state and local levels to other states and to the federal government. And they will be particular important in the passage of information down and out from the federal government to state and local authorities.

Finally, fifth, the effort needs to be made at the state and local levels to encourage the collocation of statewide major urban area fusion centers either physically or virtually with the JTTFs, the field intelligence groups, National Guard intelligence units, and other organizations that deal in terrorism information at the state level.

So what are some of our biggest challenges as we stand here today? Where do we need to focus and put our resources to surmount the difficulties that we face? Let me mention just three very high priority areas that in my opinion will impact the ISE of the future in very fundamental ways. I don't have the answer to all these issues, but I am convinced that if we work together to resolve them as partners in a cooperative venture we will indeed be able to solve them.

The first and in many ways the most complex is that there needs to be a major reform of the way we deal with sensitive but unclassified information collectively known as SBU. The federal government must make a huge effort to rationalize the way we handle SBU among ourselves. But in addition, state and local authorities need to work with us and with each other to agree on putting a rational system of control in place for sensitive information as it moves to and from state and federal governments and as it moves from state governments to state governments.

The federal system for SBU is a tangled mess – a result of 40 years of lack of attention when a period, essentially the Cold War period, when unclassified information was left to its own resources, classified information was rationally processed and had a control mechanism that functions fairly well and has functioned fairly well for over 40 years.

The states and the localities, but particularly the states, need to start now I think to examine conflicting and incompatible state laws and regulations that limit the sharing of state controlled information among the states and with the federal government. There are many cases where law enforcement officers and homeland security officials are unable to pass information from one state to another because of differing laws at the state level as to what privacy safeguards are needed or how law enforcement information can be handled and can be communicated.

A second area of major importance: in our eagerness to share information we cannot ignore the need to maintain undiminished security of classified and controlled information. Let's not think that this is intended to cut people out who ought to get the information. It's not. I'm convinced – and the experts tell me – that current technology applied to the information-sharing environment will both permit the greater spread of information and provide for a significant increase in the security of that information even as it is shared more widely, but it will require the dedication of resources at all levels of government to accomplish this goal.

Thirdly, all of us in the federal, state and local governments are going to have to be sure that we have in place the safeguards that will protect the privacy and other civil rights of our citizens. This by the way is linked to that SBU problem that I mentioned in the first instance. The future information-sharing environment cannot function if it is at odds with our traditions of privacy and civil rights. Again, these protections vary greatly among the states as well as between state and the federal governments and cooperation is going to be needed to settle that issue.

So let me now look towards the future: the building of the ISE. And I'll address two issues: first, the technology and, lastly, the changing of cultures. In building the technology, the ISE is all about bringing terrorist information sharing to a wide variety of information consumers and producers. The ISE will be developed and it will grow by bringing together and aligning existing information sharing policies, business processes and technologies. The mandate is to build on what now exists. Let's not reinvent the wheel. The charge given to the PMISE is to ensure that this occurs across all five of those communities at multiple levels of security and with multiple governments, the private sector, and our foreign partners.

Two key levers that will combine technology, policy and business processes to shape and influence the ISE are, first, the development of an ISE enterprise architecture and, secondly, the establishment of common terrorism information sharing standards. Once the developed, the ISE enterprise architecture will guide the design if an environment that supports the performance goals and business needs for information sharing by all of the ISE participants. Because we do not intend to reinvent the wheel, as I said, we will map the ISE enterprise architecture to the federal enterprise architecture and the department and agency enterprise architectures. We will also integrate the ISE architecture into the national security enterprise architectures such as the IC enterprise architecture being developed and implemented by, Dale Meyerrose in the DNI CIO's office.

We'll also integrate it with the DOD enterprise architecture and the national communications system. We intend to use existing oversight and compliance processes within those structures to monitor department and agency implementation of the ISE architecture. This is how we'll ensure that the ISE is developing in accord with the vision outlines in the Intelligence Reform and Terrorism Prevention Act. The ISE enterprise architecture will also support state local, tribal and the private sector, and foreign partners that are involved in the ISE so that we understand how to connect to the federal government and how the federal government connects to them.

We're also working closely with federal, state, local and private sector partners in developing common terrorism information sharing standards. These provide critical functional and technical bridges between the wide variety of available terrorism information, resources and those responsible for carrying out the counterterrorism missions. First and foremost, these are functional standards that articulate the rules, conditions, guidelines and characteristics for identified ISE business processes, production methods, and products supporting terrorism information sharing. These standards will apply government-wide to all ISE participants and will have an important role in ensuring consistency of ISE business processes and infrastructure development. They will be an important decision-making factor when considering investments supporting the implementation of the ISE architecture.

Finally, a comment about changing the cultures. The threat facing our nation continues to evolve. As international measures succeed in debilitating centralized terrorist organizations, we face growing threats from independent regional and national groups with weak links – especially in operational terms – with a distant leadership. This is the pattern that seems to be evolving inside al Qaeda. Al Qaeda today is becoming more of an ideological movement than a centrally directed, hierarchical organization than it was in the past. The logical outcome of this evolution is the phenomenon that we are now witnessing: homegrown terrorism.

The first indicators of this new homegrown terror are very likely to come from what I referred to earlier as the non-traditional sources. Let us not forget that over the past several years, a federal narcotics investigation resulted in multiple arrests, revealed a Canadian-based organization supplying precursor chemicals to a Mexican methamphetamine producer, in fact, was a Hezbollah support cell. A local police detective investigating a gas station robbery in California uncovered a homegrown jihadist cell planning a series of terrorist attacks, and a state police investigation into cigarette-smuggling uncovered hundreds of thousands of dollars in wire transfers to individuals living in the Kashmir region of Pakistan.

What these examples illustrate is that given the developments of recent years, the changing threat environment, the old way of doing things is inadequate. As I said earlier, the traditional way worked well during the Cold War, but we have a different challenge today and a different enemy today. Therefore, we need a different method of operating. This highlights the most difficult problem we have to face: We need to change the culture of information handling and information sharing. That's hard to do because the old ways, the old culture served us so well for the last 50 years. We have to integrate. We have to default to sharing information, not withholding it. Failure to do so was correctly cited as the biggest defect that led to 9/11. This was the – the citation there is the 9/11 Commission Report.

We need to make information-sharing integrated, interconnected, effective and as automatic as possible in order to ensure our national security. Successful counterterrorism efforts require federal, state, local, tribal authorities and the private sectors to have effective information, sharing that

information in a collaborative fashion and ensuring the capability that can lead to success in this effort. We need to cooperatively collect, blend, analyze, disseminate and use the information regarding the threats and vulnerabilities regarding prevention, response and consequence management.

Prevention, response and consequence management were not common terms in the last 50 years. They've grown out of the post-9/11 realization that the world has changed. All levels have to devote resources to gathering, processing and sharing the information. That means that first we must understand what each of us brings to the table. We need to clearly articulate what we want, but we also need to know what is reasonable to achieve. I've spent a good portion of my career working with the military, with law enforcement and with the intelligence communities to disrupt violent transnational criminals and terrorists.

I've observed both from Washington and in the field that invariably our efforts to deal with crime, disorder, terrorism and quality of life problems depends upon our ability to effectively gather information and share it with those who need to address the problems we're seeking to resolve. Intelligence is not intelligence until it's used. Until then, it's just interesting data. And the use of the intelligence is ever more important at all levels of government, not just the national level. Regardless of whether we're dealing with international traffickers, transnational terrorists, domestic jihadists or local bank robbers, the goal is the same: prevent a crime or an act of violence from occurring, reduce the fear and improve the quality of life of the nation.

The challenge, therefore, is to transform the current information-sharing culture into one that better facilitates and expedites access to terrorism information and enables the sharing of that information at appropriate levels among state, local, tribal governments and the federal government and – oh, excuse me, private sector and with our foreign allies.

In conclusion, let me say that while I'm gratified that we're on the verge of making significant improvements in the way that terrorism information is shared, yet I'm distressed that it's taken almost five years to reach this point. Our enemies will not rest until they succeed in their attacks. Any, indeed many, may be in our cities today preparing to carry out the next attack even as we meet here to discuss the problem. We should be mindful that time is not on our side. It is time to get to work.

Thanks for allowing me to join you today and I'll be happy to answer any questions if there are any. (Applause.) And I gather the procedure is – since I can't see, please just stand up and someone with a microphone will hand it to you so you can ask the question. Can we dim the lights just a bit? Thank you.

Q: Ambassador?

AMB. MCNAMARA: Yes.

Q: You mentioned that one of your main principles was that the fusion centers would work with the JTTFs and the FIGs. I think this group may not be aware of what the FIGs are – the Field Intelligence Groups in the FBI and the importance of the JTTFs. I wonder if you could comment on that.

AMB. MCNAMARA: I didn't get – I didn't hear the middle of the question.

Q: Sorry. The –

AMB. MCNAMARA: Comment on?

Q: You comment regarding the Field Intelligence Groups – the FIGs of the FBI – and the JTTFs.

AMB. MCNAMARA: Right.

Q: I wonder if you would comment on the importance of the JTTFs in information sharing.

AMB. MCNAMARA: Oh, yes. Well, the importance of the JTTFs, the FIGs are – they're absolutely essential. When it comes to homegrown terrorism and when it comes to terrorism at the state and local level, law enforcement is really the most important tool that we have at our disposal to stop, as opposed to recover from, potential terrorist attacks, and the JTTF is the best national level integration mechanism that we have among law enforcement.

What I think needs to be done with the JTTFs and the FIGs is that there needs to be a better – and this not only applies to them; it applies to all of our efforts and all of our integrating mechanisms at the state and local level – to disseminate the information more widely to non-law enforcement in the case of law enforcement and from homeland security and other elements at the state and local level to disseminate their information to the law enforcement community.

They each have something to offer, and in many cases what we do is we share the information fairly well up and down the pipeline whether it's law enforcement, Homeland Security, Defense or the intelligence community, but we tend to do, as I said in my remarks, do less well, is to share that information across those channels, across those pipelines, and that I think is what's essential. But I have no doubt that we will not be successful unless we fully utilize the enormous capabilities of the JTTFs and the FIGs, as well as of the newly developed and increasingly important fusion centers that state governors are setting up around the country.

Q: Hello. You mentioned one of the key levers is immediate development of common information-sharing standards. These are going to be functional standards. I was wondering if you've considered how to make those – I guess, how to communicate those standards to the communities through (reference and limitations ?) or how you thought about how to make those real.

AMB. MCNAMARA: Well, we're making them real by, first of all, putting them on paper and getting them adopted by the interagency mechanisms that exist at the federal level and they'll certainly be published for use throughout the intelligence community and the law enforcement, homeland security, defense and diplomatic communities. Those standards are already being drafted, in some cases being promulgated. The mechanisms for doing that already exist, chiefly through the intelligence community, the defense department and Office of Management and Budget – OMB.

Q: Thank you.

Q: Looking at the implementation plan, I think there's some confusion in the community as to what exactly the ISE is going to be. Can you address the issue? Because some people are saying it's just an environment; some are saying it's a whole new network; some are saying it's more access to current networks. Can you address to help explain what the ISE is really meant to be?

AMB. MCNAMARA: Well, if you read the plan, it makes I think clear that the ISE is going to be an – will not substitute for any of the agency architectures that exist. Instead, what it will be an integrative mechanism, an integrative function to bring those architectures together so that they can communicate with each other. So the information in one area – let's say in the law enforcement area – and information in the intelligence area can be communicated across what are currently the barriers between the architectures of the different communities.

I think the ISE is not going to, as I said, reinvent any wheels. We're not going to try and create a whole new set of programs, pipelines, et cetera. We're going to use what now exists and try and bring it together in an integrated fashion. It is a relatively modest proposal actually when one looks at it carefully and I think if you read particularly the middle chapters of our implementation plan, it lays it out quite clearly, but I think possibly because many people think the ISE is some kind of a new monster that we're creating, that it should be all-encompassing or that it threatens to be all-encompassing, that the rather modest integrated mechanisms that we put forward in the implementation plan seemed to be just a partial explanation of what we think the ISE is going to be. Indeed, it's a full explanation. Much of the architecture, much of the information processing that goes on in the various agency and community architectures that exist are going to be utilized in the ISE. We're not going to substitute; we're not going to replace them.

Yes, over here.

Q: You have quite a mission – incredible. In regard to terrorism as you spoke that it's not just terrorist per se, but it's any elements, gray activities that may not be terrorism. The things that come into my mind is the National Counterterrorism Center as well as DHS have distinct roles. I find it hard to differentiate whether or not something is really terror or not terror and plus there's time elements that are involved in those issues – critical time elements. But I would say, how do you then pass it to the right areas? Obviously, we have to get the staff to the state, the local, the tribal elements, which is the most critical. I attended a Homeland Security conference not too long ago and I was quite impressed by various commanders from Los Angeles, Louisiana, Michigan, and so forth and their presentations and what they have done in their fusion centers.

I'm quite aware of the JTTFs' work in their relationship with the NCTC online. So there's a bunch of different things going on but I think the issue is how do you stay focused? How do you get to the right people at the right time?

AMB. MCNAMARA: Well, it's not a question that I can answer fully right now because we are, in fact, constructing those mechanisms, those organizations, but we've already begun. I think it's very clear that the National Counterterrorism Center, which was set up under the IRTPA, the same act that created the DNI and the program manager.

The National Counterterrorism Center is, according to the law, the main repository, collector, analyzer and producer of terrorism information – terrorism intelligence. That, however – that law, however, requires that the NCTC distribute that product through existing agency channels, most frequently Department of Justice and Homeland Security, and indeed that's what it's doing. But what we need to do and what I'd mentioned here in my remarks to create an interagency mechanism that ensures that when that information arrives at the state and local levels, that they understand that that is a coordinated product of the federal government, and that's what the new framework is designed to do, is to produce a federal government product that is useful for the state and local authorities, tribal authorities and also for the private sector.

Right now the complaints that I hear from the state and local authorities are not that they are not getting, if you will, a sufficient flow of information. In many ways, they are complaining that they're trying to – they're being asked to drink from a fire hose – to use that old military expression, that there are so many channels of so much information – each of it slightly different from the other channels carrying other information – that they find difficult to understand what is it that the federal government thinks about a particular issue or a problem or a crisis – a incident.

And that what we need to do at the federal level – and I fully with them in this regard – is to provide a combined coordinated federal channel, not a new one, but one that will use the existing pipelines so that what arrives at the state and local levels is one that says this is what the federal government considers the situation to be.

It won't substitute for, for example, the information going out on the JTTF channels or the information going out on National Guard channels. Those, however, are specific to that agency and to that mission – one case law enforcement and in other case, defense. There're also messages and information that's being passed to state and local governments by the Department of Homeland Security having to do with, for example, infrastructure protection. Infrastructure protection is not something that the JTTF spent a lot of time sending out information on. Their information is focused on law enforcement investigation law enforcement issues to law enforcement authorities, not to the infrastructure – infrastructure protection authorities at the state and local level.

What we need to do is to have those agency-specific and mission-specific channels of information continue to flow. Let's take an example. At the state level, if there is information having to do with, for example, a possible threat to nuclear facilities, clearly the law enforcement people at the state and the local levels in various areas that they operate are going to need to know what it is that the threat is to those nuclear facilities in their state. They're also going to want to have much more specific information about infrastructure protection of those facilities and to try and understand what they ought to do to ramp up that protection. That is most likely going to be coming down in homeland security channels.

They may also want to examine what possible facilities or what possible capabilities the National Guard could bring to bear if indeed nuclear facilities are under particular threat at a particular moment. To do that, they're likely to get that mission-specific information from National Guard channels.

And to bring this together at the state level, one hopes these fusion centers will be able to give the governors, the homeland security advisers, the adjutant general of the National Guard, the state police authorities, the kind of integrated information that they need in order to take action at the state level.

Right now, we don't have a mechanism that provides that and that's indeed what the frameworks that we're now working on are designed to produce: bringing it together. Information that is not user-friendly is probably not going to be used.

I've been told by a number of police chiefs of major cities that they get so much – so many messages on their inbox that at the end of the day, they can't possibly read them, they just zap them all. They try and pick out as best they can, based on the title line, which of those many, many messages coming in from the federal government they need to look at. Sometimes they guess right; sometimes they guess wrong. I think what we need among – in the major cities and the major urban areas and at the state level for the use for the governor and other state officials is some kind of a filter, namely, these fusion centers that can decide, yes, the governor ought to read this; he doesn't need to read this; chief of police of the state ought to be sure and read this and, obviously, that kind of a mechanism is precisely what we do at the federal level.

Nobody sends to the secretary of homeland security every bit of information that comes into the Homeland Security Department. Somebody has to sort through this stuff. Somebody has to make it useful to the user and the user in many of these cases are at the state and local level are hard-pressed officials who have many other jobs to do besides counterterrorism. They are providing security. They are providing all sorts of services to the local communities at the state and local levels that take up time and they need to have a mechanism that will enable them to get the information that they need, not the information that's so useful at the national level, but information that has been packaged and that's been sent to them for their use and that is precisely what the new framework is designed to provide.

Q: Thank you very much. I appreciate it.

AMB. MCNAMARA: Over here?

Q: Sir, my question revolves around SBU and you mentioned about needing to try to standardize that, which I think I concur with, but my question has to do with the policy side of that and the Executive Order 12333 to which – and I might be – (unintelligible) – from a future panel on U.S. persons, but there seems to be a disparity in the interpretation of 12333 as it pertains to U.S. persons and from my area of expertise of open source that U.S. persons' information collected via open sources and how SBU will handle that. So in other words, given that you may standardize SBU, there's this misinterpretation or different interpretations of 12333 and as it pertains to being able to share that information. Could you speak on that, please?

AMB. MCNAMARA: Well, what you're mentioning there is a particular subset of issues – very important subset of issues that are part of rationalizing the SBU environment. Right now, we have literally hundreds of different ways in which agencies deal with SBU information. As I alluded to in my remarks, over the course of the last 50 years, we'd created what we now generically call SBU, but there is no rational governing set of principles, no set of regulations; indeed, no single set of legislative mandates that are a single set of legislative mandates that control how SBU information is generated and/or protected.

One of the discrepancies in the SBU environment is the use of the term, U.S. person. That's something that's very important for the intelligence community. U.S. person and U.S. persons is a

category or a term which in many ways defines what can and cannot be processed and used and how it can be processed and used by the intelligence community. U.S. person and U.S. persons is a much less important term when it's used by, say, law enforcement or diplomatic communities. It's less important, but also used differently in some respects and we need to standardize and rationalize the way in which we deal U.S. persons, but that's not the only problem we need to deal with in SBU.

We have problems in simple markings. "For official use only" sounds like a very easy marking, one that is used throughout the federal government, but when we examined it, we found out that it was used in about – I don't know – maybe a dozen, two dozen different ways to control the access to the information. Almost all agencies have access control mechanisms that are peculiar and particular to that agency even though it says "For official use only."

Once that problem is solved, there's another problem and that is, how do you store and transmit that information that's labeled "For official use only"? We found out that each agency stores it and transmits it in its – according to its own regulation, its own agency regulations and agency procedures and they are not all the same. There are literally dozens of different ways in which "For official use only" is first of all marked, secondly, access to its control, and thirdly, the way it's transmitted and stored, and that's also true of "U.S. persons." There are all – there are just innumerable ways in which the mechanisms of the SBU environment are chaotic. We can't have SBU effectively utilized in the information-sharing environment until we rationalize what is now a chaotic system.

We have a fairly rational system for classified information. We have confidential secret, top secret, and code word. And when we deal with those, we have a set of nationally; that is to say, government-wide rules and regulations, indeed, legislation and those rules and regulations define how classified information is to be – is to be marked, how – who has access to it, how is it going to be transmitted and how is it to be stored. We don't have any of those four items when it comes to SBU. Instead, we have over a hundred different markings and we have within each of those markings dozens of ways in which agencies handle, store and allow access, and that's simply – and one of those is the question of "U.S. persons."

So I think we're going to have to sit down and, as I've said when I made my remarks, I don't have the answers to all of those questions, but I do know that there are answers out there. If there weren't, we wouldn't have a rational system with respect to classified information.

Finally on this point, much of the SBU information that we deal with – I don't know exactly, I wouldn't put percentage numbers against it – but a good deal of it should be simply unclassified, but it's put down as SBU. That is to say some control mechanism is put in place in many cases at very relatively low levels and for reasons that are not very specific and indeed subsequently when people are asked why has this control marking being put on this document, nobody can some up with a good reason, and that means that we're not marking at a high enough level so that there can be standardization.

So all of these issues, we're just now looking into them. We've done the basic research that has defined the problem and we now have to sit down and fix the problem. I'm not sure if that has answered your specific question, but that's the problem – those are the series of problems that we face in the SBU environment. Maybe one more so I don't run over or – nope. No time for one more.

So I thank you very much and I wish you all the best in the next couple of days. (Applause.)

(END)