Intelligence Community Chief Information Officer Panel

Moderated by Intelligence Community Chief Information Officer, ODNI
Ms. Priscilla Guthrie

2009 GEOINT Symposium
San Antonio, Texas

October 20, 2009

Video of this event is available online at www.dni.gov/video.

Moderator:

- **Ms. Priscilla Guthrie**, Intelligence Community Chief Information Officer, Office of the Director of National Intelligence

Panel Participants:

- **Mr. Robert L. Arbetter**, USD(I) Representative to the IC CIO Council, Office of the Under Secretary of Defense for Intelligence
- **Mr. Charles R. Barlow Jr.**, Chief Information Officer, National Reconnaissance Office
- **Mr. Chad L. Fulgham**, Executive Assistant Director and Chief Information Officer, Federal Bureau of Investigation
- **Ms. Catherine Henson**, Chief Technology Officer, Defense Intelligence Agency
- **Dr. Robert H. Laurine Jr.**, Chief Information Officer, National Geospatial-Intelligence Agency
- **Mr. Kelly Miller**, Deputy Chief Information Officer, National Security Agency
- **Mr. Al Tarasiuk**, Chief Information Officer, Central Intelligence Agency

---

JOAN DEMPSEY: As we bring the panel out this morning we are going to hear from CIOs and deputy CIOs from across the intelligence community who will talk about there collaborative approach to information sharing. We have with us this morning the Honorable Priscilla Guthrie who is the IC Chief Information Officer, Office of the Director of National Intelligence; Mr. Robert Arbetter, Director, Collection Concepts and Strategies, Deputy Under Secretary of Defense for Collection and Analysis, Office of the Under Secretary of Defense for Intelligence; Mr. Charles Barlow, Chief Information Officer, National Reconnaissance Office; Mr. Chad Fulgham, Executive Assistant Director and Chief Information Officer, Federal Bureau of Investigation; Ms. Catherine Henson, Chief Technology Officer, Defense Intelligence Agency; Dr. Robert Laurine, Chief Information Officer, National Geospatial-Intelligence Agency; Mr. Kelly Miller, Deputy Chief

Information Officer, National Security Agency; and Mr. Al Tarasiuk, Chief Information Officer, Central Intelligence Agency. Priscilla, take it away.

PRISCILLA GUTHRIE: Thanks Joan, more CIOs than you've ever seen on stage before. That ought to scare everybody, I guess. (Chuckles.) Let's see, in my four months in this community, I have come up with this marvelous vision that I'd like to share for just a minute.

You know, this community has the information that could provide the basis for ongoing persistent situational awareness that is shared among decision-makers. Think about the fact that this persistent situational awareness could be used, it could be always available and at some point if someone feels something is happening, they could bring – as Dr. Dugan said this morning, anticipated and unanticipated because we really don't know what is going to happen – stakeholders to the table to share the information, to view it, to collaborate, to bring their shared experiences to the discussion.

We could then develop courses of action using some of the tools that have been developed on the DOD side, the adaptive planning tools. We could affect a course of action, track it and then contribute to the ongoing situational awareness. I actually believe that the community has most of the pieces to make that vision a reality. So let me start by talking about the four priorities this team, the ICCIO team, is tackling in support of the director's national intelligence strategies.

The first one is information integration. We affectionately refer to it as I-2. And it is something that must – it is the infrastructure that must allow users, anticipated and unanticipated, to access the information they want, when they want it, anyplace and anytime. And the goal is to make that technically possible and prohibited (ph) through policy. It has to be adaptable; it is the infrastructure that allows the intelligence and business missions to adapt. Creating this environment is a community-wide activity. Doug McGovern, who is here, is in my office and he heads it up for us.

It is obviously one that is going to evolve over time. Our job in the DNI is to set the expectations and standards and to work with both ongoing programs and new programs in concert with Dawn Meyerriecks, who is our new acquisition and technology DDNI. One of the things that Dawn and I have been talking about, and I think you will hear a little bit more about later, is consumption metrics. This I-2 environment is the place where we would measure use of the data that this community provides and figure out how we fund it adequately.

Second thing – okay, so I said four things the first one was I-2, the second thing is the IC business transformation. And perhaps you would say, well, how does business fit? Why is it part of this? Well, it has to ride on that same environment. Unless you think that is not important, think back to the tsunami and one of the combatant commands tried to figure out how they use their command-and-control environment to get access to logistics data; the logistics data was for tsunami support. So obviously we want to make business data a part of the overall environment; it is imperative.

The third thing – so third of the four goals, cyber. Glenn Gaffney has the lead within the DNI within the IC for cyber. On the CIO side we are responsible for defense and I'd like to say and operations. That means making sure that the environment can operate. It will require us to develop operating constructs and build to performance constraints that are above and beyond what we have

traditionally had to do. So I think it sets the bar for us and it sets the bar a little higher. It is also going to require us to do risk management sometimes in near real time. And that is something, again, that is a little different from what we've had to do as a – deal with as a community.

And then the fourth thing I'd like to highlight – and you'll hear more about this from the rest of the panelists – is the support to Afghanistan and Pakistan. There we're focused on delivering capabilities within shorter timelines – I know that is not something you always think of when you think of the CIOs – but enabling the capabilities that are needed for operations, doing a better job about selecting those things that we field. Wherever possible we want to both support ongoing operations but also pick something that is strategically aligned with where we are going with the IT environment. Otherwise we wind up with one-offs.

And then the last thing on Afghanistan-Pakistan is to bring the edge innovation in, the wonderful things that happen in the field because people have to make things work. They come up with innovative ways of doing things, I like to call it edge innovation. And somehow we need to bring that back into the broader environment. With that I'm going to be quiet and I'm going to pass it to Kelly Miller. Kelly is from NSA and he is going to talk to us about how we balance the priorities as we move through our day-to-day business.

KELLY MILLER: Thank you, Priscilla, I'm going to just talk a little bit about the defense of our networks and information sharing and the various aspects of that problem that we are really trying to conquer as we support the mission Af-Pak and the COCOMs. And that is really about bringing the IC and DOD and in many cases our international partners together with our information systems. And it is, as you expect, a very much a multidimensional problem and it is about balance, similar to what has already been talked this morning in the prior panels.

There is obviously a technology aspect to this in keeping pace with the latest technologies, merging our disparate technologies and dealing with the large legacy systems that we already have out there.

Every one of us has a network enterprise out there that is robust and moving and it is not something that we – we do not have a green field solution here. So basically we have a balance of balancing our missions versus the modernization vector that we would like to achieve. There is a huge culture dimension to this as well. And that was highlighted this morning I think in the analyst roundtable. We are moving to a culture within DOD and the IC of sharing, the need to share versus the need to know. We are starting to accept risk. Priscilla has already mentioned that and we are trying to overcome what I would call the protectionism of our data. That was mentioned this morning in this morning's roundtable, and understanding that there is a dimension of knowing your data, knowing what you have but allowing it to access to others.

So we have to balance the access to the data versus the security of the data and balance the consequences of allowing people to see imperfect data. In the analyst roundtable this morning they talked about how a Twitter solution converged over time to more accurate data. But where is the line that allows us to say it is accurate enough for what we want to do?

All of us are battling a cost-value dimension to our modernization vectors. There is a huge appetite amongst the analysts and everyone else to have more. The COCOMs want more: The more we

give them, the more they need, the more they want. What can we really afford in that since we are all dealing in largely declining budgets, or mostly in the IT world, at least a zero-sum vector?

Another dimension that we have to balance is policy and legal. There are very, very strict laws on information management access and storage. There is obviously the issue of privacy versus U.S. data and access and so on and so forth.

But, for example, in my environment, I have very strict laws on what I can do with SIGINT data versus COMSEC data, for example. And when you add that to all the other INTs in trying to connect all the networks and have common repositories, the laws and policies that we have to obey challenges us to balance what we want to do, what we'd like to do, what the analysts would like access to with what the laws and policy actually allow us to do.

There are several what I'll call locational issues: Where do we go first with this? Obviously we can't modernize; we can't connect the entire globe one time overnight. So there is a logic, a strategic set of vectors as to how we can modernize. But we still have to make sure that we are paying attention to the mission, the tactical side of the mission, the mobility and the flexibility and adaptability that they talked about this morning from a tactical and theater support.

And then, last, we also have hostile and friendly environments. So balancing the mission needs which are largely tactical against our CIO strategic vision of where we want to go and interconnecting our network enterprise is another balancing vector.

Several other things that are just dynamics – we need to – where this is an evolution forever. You know that as well as we do. This is not something we are ever going to see the end of.

We obviously can't be intrusive to mission. You heard the analyst panel this morning talk about the single sign-on design desires that they would like to have and the environment the analyst works in down to the 10 degrees versus 20 degrees of swivel and certainly not wanting to add new sign-ons or new dimensions or new databases that they have to connect to – so enabling the collaboration and use and balancing the missions along the things like prevent, detect, respond, all of these kinds of vectors are things that we are dealing with on our modernization.

And we are doing this while we are trying to maintain our networks and operating at a high reliability rate, robustly and a connected enterprise across the entire IC and DOD. Now, I'm not telling you this because these are excuses. I don't want to sound like they are excuses. This is a challenge that we on the stage and the IC CIO Council have accepted. It is something that, as Dr. Dugan said this morning, we're in so we're here; this is what we're trying to do.

A couple of the things you are going to hear from the rest of the panel this morning on what we have done and what we are doing. For example, in architecture we have a layered common model. We are populating that model now so that we understand what each of us has in our environments and our enterprise and know what we have so we know what can – where we can reach commonality. More work on strategic vision and vectors and how we operate than has ever been done before – again, another major vector of the CIO council.

On network integration, we are proceeding against common standards, common definitions of our networks. Just talking about our networks in a common lingo and a common context allows us to understand the edge nodes where we connect and better understand how we can make more progress in passing and moving data and information across them. Common enterprise licenses, obviously licensing is another policy issue; that is one that you folks have a lot of control over but moving data across our boundaries and software licensing are something that we have to deal with.

We are doing a lot of work in IDAM, identity management, as was mentioned in this morning's panel, about common registries, common directories, common authentication so that we can again, balance the risk of who has access to the common data that we are looking for and the common repositories and still maintain a security posture that is acceptable to us across all of our security domains. We are doing – and you should hear about some common cross-domain solutions pilots that we are working on today as well as cloud computing pilots.

Going to talk a little bit about the common data centers: We are making progress and building common data centers and we have a vision on that that is pretty complete and we're in the implementation stage on that. And then last, but not least, we have chosen amongst ourselves some executive agents on transport services, common messaging services and so on. And all of this, when I've used the term "common" it doesn't necessarily mean one; it means a minimum set of those services that allow us to accomplish all the missions.

So those are some of the dimensions and the vectors that are the challenge to us and that we've accepted as trying to move forward with information sharing and securing all our networks. With that I'll pass the mike to Bobby Laurine from NGA.

ROBERT LAURINE: Thanks, Kelly. So let me take you to the role of the functional manager for geospatial intelligence and from an IT perspective. The challenge that we see as we move forward is to ensure that we have a very and we're leveraging across the community from a governance perspective the capabilities that we bring to bear to meet these challenges. Next we want to make sure that we have a very active standards and architecture strategy, one that lays out the ability to be able to foster interoperability across the community and making sure that we understand the investments from a portfolio management perspective and ensuring that we provide the best capabilities to the analysts – and then, finally, leveraging community solutions as Kelly has highlighted to ensure that we are providing the best capabilities across the board, across the IC.

And so, as we step back, one of the challenges that we have is really taking the time to lay out an integrated strategy for IT. We've done that from an NSG perspective. We've laid out an IT strategic plan. It allows us to make sure that we are leveraging the investment as we move forward and provides the opportunities to entertain new capabilities as time goes on.

Next in the area of geospatial standards and architectures, this really is the framework by which we will be doing business and are doing business today. We have the GEOINT reference architecture and that allows us to really focus on what are the services and applications that we can leverage across the community. What is the infrastructure that needs to be brought to bear to support the common solutions that are out there. Kelly highlighted some of those for us. And also what are the

standards, what are the glue-ware, what are the policies that allow us to be able to bring a tightly coupled environment to support the analyst?

The way I see it is that the investment we make in standards provides huge dividends from a cost-savings perspective as well as a capabilities perspective. We have adopted more than 60 standards across the board and continue to do and work very hard with that. Some of the new emerging challenges that we have of course were highlighted by the huge volumetrics and sensors that are coming on board and what does that entail. That entails ensuring that we have the policies to be able to store that data and actively retrieve that data and disseminate that information to support our customer base.

We've defined currently six policies out there that provide the framework from hyperspectral all the way to full-motion video to allow us to optimize the storage of those types of phenomenologies that are coming in. And, I'm telling you, that is a huge transformational activity across the community. We need to continue to build upon that and make sure that we are leveraging community solutions as we deliver infrastructure capabilities to support the war fighter. And so the data center's capabilities that were highlighted by Kelly, the network capabilities that were highlighted by Kelly as well as the ability to provide a common framework that we can access applications is something that is key and we need to move forward on.

In addition, as we look forward, NGA is continuing and NSG community really needs a mechanism by which we control and really evaluate the capabilities that are coming from the community and we are doing that through the ability to be able to assess standards compliance as we move forward. And we have a seal-of-approval capability from an NSG level that we are going to be actively working on across the community.

This will foster interoperability and ensuring that we are providing the best capabilities. Next, as we look at portfolio management, as we look at the series of applications that are out there across the community, which ones are the best of breed, that provide the best capabilities to the analyst?

We've been designated as the GVS capabilities manager, providing 70 services across the board and we will continue to do that but there are other opportunities across the community to leverage those types of services, those types of capabilities and making sure they are promulgated across both DOD and the IC. And that is actually a big change in the way we do business.

Finally, as we move forward, I think that the information sharing across the board as it relates to new capabilities, whether it is A-Space being delivered by DIA or whether it is network connectivity being delivered by NRO, or NGA and NSA working together on providing support to the AOR, these are the basic mechanisms by which we can leverage very fast, very rapid solutions to target the adversary as we move forward. And we are doing that today; we are doing that through the NSG expeditionary architecture.

We are deploying capabilities supporting the war-fighter day in and day out with the services, not only from NGA but across the NSG, and that is a big and fundamental sea change in the way we do business. And that sets the stage for what we need to do in the future and ensuring that we support

the next active adversary that is out there. And these are the investments as we look back that really provide us the opportunities to be able to move forward.

So I think we are at really a unique juncture here, a unique juncture in the sense that ensuring that we are providing both the infrastructure, ensuring we are providing the applications that are out there, making sure that we move forward on standards compliance, leveraging the capabilities across the community to provide and support the war-fighter, the national customer and the civil customer. And I think that is something to be very, very proud of, all of us as we sit here today. So Casey.

CATHERINE HENSON: Thank you, Bobby. This morning I am going to talk to you about a few initiatives on information sharing that DIA has been involved in the past 18 to 24 months. As we all know – specifically in the Af-Pak area. In late 2008, I'm sure everybody that there was a lot of things were heating up in that AOR. Maj. Gen. Flynn, JCS-J-2 and Brig. Gen. Fogarty from CENTCOM J-2 was trying to develop the plans for that AOR.

There was many different layers of the IT infrastructure and they were both trying to understand that laid down a little bit better. And so what DIA did with CENTCOM J-2 was we started a series of summits. And those summits are the – was a co-chair DIA and CENTCOM J-2 on the Af-Pak, IT synchronization summits.

And it had – the first one was in April and it had elements, multiple elements from everyone up here. It also had DISA, various J-6 representatives, the military services, Department of State, the taskforce that we're in, the AOR, and of course we BTCed in the AOR. The first summit was basically who is doing what and where are they doing it within that region. One of the big initiatives at that time was the facilities. People were building facilities; everyone was trying to build the facilities, trying to get communications, trying to get those different layers of the architecture into the AOR as quick as possible. I'm sure it doesn't surprise you that maybe there was some duplication of efforts; maybe we weren't really synchronized in what we were doing.

So the very first summit got a very large group together to understand what they had been doing the last few months and where they were going in the next four to five months. A lot of this was on facilities floor space, HVAC, wax space, what is coming in. And with that, it was also very quickly shown that – requirements: Was there a good a handle on the requirements going into the AOR, especially from the intelligence piece? There were so many different requirements and what is the priority of those requirements?

So coming out of the first summit was discovery of who was doing what. And the second was, the development of the CENTCOM J-2 intelligence requirements matrix. That is a very valuable asset that the senior leadership uses today. It's both on the SIPR and JWICS side off the J-2 homepage.

The second summit that we had was in July, and that one focused more on what type of infrastructure had been laid out. The buildings were built but a lot of the components were all bringing in different sets of infrastructure at different times. Depending on what needed to be built, there was a lot more infrastructure coming in from the IC than the J-6 was building. Could some of the J-6 elements use that bandwidth that was available in the disparate regions? A lot of these

coordinations were being done for the second one. So the second one was mostly on the infrastructure coming in and the bandwidth and how we could leverage each other for that.

The third summit was done just last week, and this one focused more, as Kelly was saying, some of the cross-domain issues. It's not a four I's out there; it's not a five I's. It's not a nine I's; it's not an 11 I's. It's more than that. And we need to ensure that we're providing on the different domains – CSI, SIPR and NIPR – what they need; and to get it to our coalition and international partners that needed that information. So for the last week, that was for the first two days; the session was mostly how do we move those things across?

A couple of things that DIA has done in that realm is NATO is now on JWICS; we are working with the J-2 to put CIDNE and replicate that data across to the RELs (ph) so all the RELs that are in the AOR can see the data that's on CIDNE. It's a very good intelligence and operational database that they're using.

And then the third part, even more for DIA, on the unclassed environment, working with the DNI analysis group in support of the State Department to give the provincial relocation teams, reconstruction teams, a database in order to enable them to start communicating better. The PRTs are located throughout the country in very disparate places, and so building a database on the unclass so that they can help is something that we're also doing.

So what I've done is I've discussed a lot of things that we're doing within the AOR, and this is all of us plus the DOD. The other thing that DIA's doing is working very closely with DISA on the enterprise services. The services – as Bobby has stated, we need to put services on SIPR and in the SEI platform, but we also need to ensure that DISA is our partner with us and the services. And so we're working very closely with DISA to ensure that the SIPRNet and JWICS enterprise services are the same. We don't need to develop different services; we need to leverage those services – and working with Becky Harris very closely to make sure that happens.

That also works in with the JIOCs in what we're doing with the JIOCs. They're fighting the war – they're fighting their battles in each region on that SIPRNet piece. So as they're taking the intelligence from JWICS, those enterprise services also need to be down on the SIPRNet in the same.

And last I'd like to leave you with is from the analyst round table. As you noticed, everyone said we're moving forward with information sharing. We are all dedicated to do that but we have a long way to go, and we're dedicated to moving forward and bringing those innovations from the field to do that information sharing globally.

MS. GUTHRIE: Thank you, Casey. Al?

AL TARASIUK: So when you think about the strengths of the intelligence community, you think about the unique strengths and capabilities that every agency in the community brings to bear on a problem. And we are most effective when we bring those technologies and capabilities together, and that's what this panel, the group of CIOs, here is doing.

You've heard a lot already – what I want to share with you this morning is on the Problem set of information sharing and some real practical things that are happening today that this is where rubber meets the road.

I want to talk to you about three unique capabilities that – and there are more, but three specific capabilities that are disseminating intelligence today more than we've ever done in the past. I think we're breaking new ground on customer service as a result of this, and we're dealing with the challenges that we faced in the past with information sharing.

The first one I want to just mention is the OpenSource.gov Web site. It is the flagship dissemination engine for the OpenSourceCenter, which is part of the intelligence community and sits in CIA. It also sits on SIPRNet and disseminate there. There are 20,000 active users representing all IC agents – uniform, civilian, DOD, and NT-50 agencies, senior policymakers, war fighters both in the field and on ships in the seas.

Besides the current OpenSource featured articles, you can get access there to 16 commercial providers such as Jane's, Oxford Analytica, ProQuest, and others. And within those, there are 128 distinct databases that are available if you log into this Web site.

The latest in the Web site is a groundbreaking contract just last month with Thomson Reuters that now provides Web of Science data available to the entire IC. The OpenSource.gov Web site also rehosts OpenSource materials from 115 other U.S. government entities.

But one of their real key features besides the featured articles and the other postings that they do is the video that they capture. They call it video FedCasting. And this is video from 50-plus live foreign TV stations that are all brought to your desktop.

They also push information out so it's not just a pull mechanism. They push information out to about 170 subscriptions. And these go to host agencies and get disseminated into the internal messaging systems.

Looking forward in OpenSource.gov, they are continuing – or beginning to work collaboratively – across the community to develop an integrated community OpenSource architecture where the vision is that anyone working on OpenSource anywhere in the DOD and intell community would have access to a common set of tools and a common set of data to help them do their job. It would be network agnostic and platform agnostic.

The second platform that's advanced a lot in the last few years is called CIA Wire. It's available both on JWICS and on SIPRNet. It's CIA's flagship information-sharing Web capability. It contains intelligence reporting but also managed online content using a lot of Web 2.0 capabilities.

Since 2007 to date, 5.5 million documents have been posted; 3.3 million available on JWICS; 1.9 million available on SIPRNet. If you remove the big chunk of OpenSource reporting that also gets reported on this Web site, the preponderance of the reporting that's in the Web site is clandestine reporting by a factor of five over analytical products. And these are up to TDX level. The total readership is now about 100,000 and we're adding about 1200 new readers every week.

The heart of this dissemination engine and what makes it work and has made it successful is the security architecture. It's an architecture that balances the need to share with the need to protect, as well. And it's a model that has been replicated for NCTC Current and the DNI's new Intelligence Today, and also the Library of National Intelligence as we look forward with CIA Wire and some of the things to come; moving into the mobility space and providing more capability there, and also tailor content for every user.

I mentioned the Library of National Intelligence – this is the third of the vehicles that I wanted to mention this morning. It is being used to implement ICD-501, which is the community's information-sharing policy. We have implemented phases A and B, and this is the – if you know anything about 501, it's the policy that says that information needs to be discoverable and accessible by anyone that needs it to do their job and is authorized to have it.

So today we have about 2.2 million documents that are in the site – and this is since June of this year, when Phase A started. There are about 4800 unique users since June and most IC elements are contributing. So there are 17 IC elements and most of them are contributing to the LNI.

These are examples of how technologies that we have invested in within our own agencies are being brought to bear on the problem of information sharing. I'd like to pass it now to Charlie Barlow from NRO.

CHARLIE BARLOW: Thank you, Al. Well, as most of you are probably aware, the NRO has been going through a redefinition process over the last 2 years – not only from a standpoint of placing emphasis on the ground but also forging more robust and cooperative relationships both within the DOD and the IC.

Within these partnerships, we are developing and building together the integrated information environment that Priscilla talked about. This is greatly increasing the information-sharing capabilities across the community and is providing additional support in a number of different areas.

The NRO, NGA and NSA have also renewed and created greater partnerships in moving forward with placing the emphasis on the ground systems to improve processing and dissemination of collected data. Among the three agencies, we have worked to provide greater cross-tipping and queuing of signals and imagery data; cross-infusion for enhancement of intelligence products; and search and discovery capabilities to make more accessible to those that need the information.

Priscilla just spoke about initiatives that we as a community are pushing. The NRO is fully participating in supporting these activities in all areas; in fact we are leading the cross-community network integration activities through the network integration steering group. The goal of this group is to develop plans for greater federation of both IC and DOD transport networks. An integrated network environment is key to the information-sharing activities that we need to undertake.

However, just looking at these from a strategic perspective is not an option. We must address the tactical near-term needs, as well. In this endeavor, the cross-community partnership and

cooperation are paying huge dividends. It is allowing us to identify needs and bring technology solutions to bear much more quickly than in the past. Community efforts in Iraq and in Afghanistan are clear examples of how this has paid off.

However, as we move forward towards greater emphasis in Afghanistan, we must continue to draw upon the cooperative partnerships to solve problems and increase the need for intelligence support.

To help with this, the NRO is providing embedded support to assess in theater information-sharing needs. This activity is looking at what information is needed; where it is needed; what forms does it need to be in; who does it need to be shared with and at what classification levels; and how do we ensure CNA of rapidly-deployed systems to properly protect the information that it processes?

We are also actively participating back here with the USDI on their information sharing and collaboration IPT, which is bringing together all the sources of information pertaining to what the needs are in theater. Together, we expect these activities to provide us with a solid roadmap for how we at the NRO can best support the Afghan theater.

Areas where we have provided continued support include increased bandwidth capabilities to more quickly disseminate large, bulk data files. We have improved data search and discovery capabilities, allowing individuals to be able to find information. We are providing data at its earliest point of consumption.

We are working with NGA for expanded development and use of a central repository of chip imagery, reducing the need to reach back for full-frame high data-content imagery. NRO, NGA and NSA via the Real-Time Regional Gateway concept, have dramatically enhanced the rapid transfer in information to theater and able the fusion and virtualization of multi-end data.

NRO is actively supporting a strategic intent effort by participating in a quad team among NRO, NSA, NGA and DIA to identify actionable items to support dissemination of information to the war fighter.

We are also working on the development of an integrated desktop for analysts. This desktop will allow the input for multiple sources at multiple classifications level, and the dissemination of information to individuals where it is needed at the different classification levels.

Talked a little bit earlier about the need for the identity and access management access processes we're working on. We're working on that for both U.S. networks and to foster greater agreements with our allies.

We are establishing reciprocity of certification and accreditation clearances across the U.S. agencies, enabling rapid fielding of IT capabilities. We are also working on establishing common standards to enable the passing of classified data via other sources – Internet is an example – and other sources.

I believe our combined community efforts have shown the value information sharing and integration provides to national security. It is essential to the decision-making and timely responses that we need to provide.

However, our successes to-date are only the start. We need to continue to be flexible and agile to be able to meet the needs of the future. What we have learned from Iraq and Afghanistan have demonstrated this. The best way for us to achieve this is through continued cross-community activities and support. And with that, I'll turn it over to Bob Arbetter.

BOB ARBETTER: Thanks, Charlie. Yeah, just in effort to get to questions here, I'll just pick up a little bit on what he said about the information-sharing IPT that we stood up. It's just getting its feet on the ground but we have stood up an effort to help information sharing in Afpak. It is established as an IPT under Gen. Koziol in the ISR taskforce, and it is off and running. So we expect to, with this effort, gain a better understanding of how information is moved around the AOR and to improve information sharing within the U.S. and amongst the many nations that are helping out in that area.

I also just want to touch a little bit about where we are on DCGS and JIOC integration. As y'all may know, we have had a governance board for quite a while on creating a common framework through a centralized governance but decentralized execution of the various DCGS capabilities out there today.

We have also recently included under a common governance system now called the Defense Intelligence Information Enterprise as kind of the senior governance mechanism – a piece or a board that will manage JIOC integration, as well. So now it's a single governance structure for DCGS on one side and for JIOC integration on the other side. And that's, I think, going to prove very advantageous for us as we actually try and take those two efforts and coordinate them as we move forward. So that's all I've got.

MS. DEMPSEY: Great. Thank you all very much. We have a huge number of questions, so I will try to combine as many of them as I can topically and see if we can get through them.

We've seen tremendous gains in the last few years since the IC went to badge reciprocity. On the digital front, will we ever see the day when we can use a single IC log-in and credentials as the true passport to access all the IC systems to which an individual is authorized, and if so, when?

Related to that, can you provide a specific example of a common or shared data center across agencies?

And then, finally, your issues can be broken up into technology, policy and culture. Several of you have addressed the first two, but what are we doing to address culture? I.e. how are we rewarding information sharing?

Those are all related topics. So maybe, Priscilla, if you would like to start?

MS. GUTHRIE: (Chuckles.) Sure. I'm trying to figure out how we would break this up to make it useful. And I'm thinking since Kelly started talking about identity and access management, he ought to talk to that. And, Al, maybe you want to talk to data centers? Is that a good idea? And then I'll talk just a little bit about culture, since I'm probably the person who knows the least – maybe the newest observer. So Kelly, do you want to start with identity?

MR. MILLER: Okay. The question was, will there ever be a time? Hopefully, yes. We are making a lot of strides on some of the enabling services below the identity and access management. IDAM is the highest priority on the CIO council list of to-dos. But as I've said, there's enabling services that are necessary to get that moving. I mean, you have to have common directories and common access lists and so on – working – that's both a security issue and a CIO issue. That connectivity has been made, so yes, there is significant progress on that. whether we will get to one access – that's always a goal – not likely in the next year or so, but we are certainly starting to minimize the number of access hoops that you have to go through in order to get there. so great goal; it's high on our radar screen; it's heavily pushed by the analytic community; but this is one of those – you need to get the enabling services in place first and there are several of those that we're working on at this point in time.

MS. GUTHRIE: Okay, Al?

MR. TARASIUK: So on data centers, the answer of the question is I don't think that there is any single data center where we all have capabilities today; that doesn't mean that we don't have data centers where a few of us are together – and that includes some of the data centers at CIA.

Let me be careful here and not get into any classified terminology and things, but let me tell you where we are with our IC data center program. It's funded; it's a high priority for us; we just established CIA as the executive agent, and we established a program office within CIA to manage this.

We expect the first capability to be available somewhere around 2011; there are still some things to work out as far as locations – are we going to outsource this, are we going to build buildings? Our strategy at this point is to look for services. And we're all playing in this because we all have requirements in about that time frame for additional floor space.

So that's kind of where we are. Now, tied to that is the entire information integration effort, and how do we deal with data? Do we collocate physically? Is it logically separated? And those are all the issues that we're working through right now; someone mentioned the culture piece; you know, we might be able to overcome the technical policy issues and the security issues, but we still have huge cultural barriers as far as, you know, comingling data. And we're continuing to work all that; it's not as easy as the technical problems that we've been able to solve.

MS. GUTHRIE: Okay. So I'm going to say something about culture, and i'm wandering in here – I am an engineer talking about culture; so with that as a backdrop.

First of all, we are indeed taking the collaborative services that were to be part of the enterprise environment and putting them in I-2. The point is that information sharing without collaboration isn't what we want; we want the collaborative aspects as well.

Second thing, though – I mentioned early on that Dawn Meyerriecks has been thinking for a while about the idea of consumption metrics. And before you say, Oo, this is an engineer's answer to collaboration, let me point out that the idea here is to look at what data is used and who uses it, and then to go figure out why we're not using things; why we're not accessing services; why we're not doing collaboration; why we're not looking for data sources, I'm going to say, edges.

And then the third thing I'm going to throw out is this concept that I mentioned of edge innovation. Part of the reason for wanting to work in such a focused way one the support to Afghanistan-Pakistan, innovation, new ways of collaborating actually really move rapidly on the edge, where people have to do things that are different; they have to think differently and they have to work, as Casey said, cross N (ph) I's our coalition partners and across multiple departments and agencies.

And so those are three things that we're looking at. I'm not sure – I've heard people say, well, gee, you've missed the boat on culture. I'm not sure what else we do. We're not going to write a policy about culture. But, looking at how people use it, monitoring progress, looking at what is happening on the edge and then making sure that the collaborative services are front and center primary parts of the information-sharing offering, I think are all focused on helping change the culture.

I'm going to mention one more thing before Jen cuts me off. I was talking with Hill staff. And, you know, I'm old and they are definitely young – (laughter) – younger and younger every year. And they were talking about culture and use of collaborative services.

And it was interesting to me that they weren't that young. So they thought they were, perhaps, but they weren't that young. And they were talking about e-mail as a collaborative tool. And I thought, oh, my goodness, that's not the right answer. And it struck me: Here is a group that's kind of outside the norm of our community and they're talking about e-mail as one of their collaborative services. It obviously helps, but it's not the basis of where we need to go.

So it just tells me we have a huge amount of work to do when we look at collaboration and we look at how the different layers of the organization use collaborative services and then we look across the disparate cultures and see how we use collaborative services. So a lot of work there.

MS. DEMPSEY: Great, thank you. A lot of questions about security. To sum them up, I would say that a number of the questioners made the comment that we were in a security environment that actually aided collaboration over the last few years, but we seem to be entering a more restrictive security environment today, whether because of real or perceived threats. Has that security pendulum shifted and how do we deal with the higher costs and the other implications of a more restrictive security environment? First of all, is it true? And, secondly, how do we deal with it? Want to try that?

MR. BARLOW: I'll give that one a shot. I don't think we've really entered an environment that is moving back from a standpoint of the pendulum. We have always had a responsibility to provide, but with that responsibility to provide is also the responsibility to protect.

And if you look at, from a standpoint of what has been worked under the ICD 501 that was talked about, is there are authorized IC individuals who are provided with the information, who have access to that information. If you are not an individual who is so authorized then you do not have access to that information. If you are not an individual who is so authorized then you don't have access to the information.

We cannot forget that as well as providing we also have to protect. That is an extreme position that we have to take because of the fact that the information is important to us and we have to ensure that that information isn't shared with individuals who are not cleared or allowed to have access to that individual. So as trying to find the middle ground of where we need to be in that arena, it is not moving – the pendulum is not moving back. I think what it is we're trying to find – still moving to try to find where that resides within the middle ground of providing and protecting.

MR. FULGHAM: Let me add to that. Let me tell you what's changed. Am I on?

MR. : Yeah.

MR. FULGHAM: We're not walking back from information sharing. The pendulum is not swinging. What has happened is that as a result of the visibility of the cyber issues, the operational side of cyber and the defensive side of cyber are closer together than ever. So, in our organization we use the term "inform the defender." We are smarter now about how to defend our networks and how to protect our data than ever before because we now understand what our offensive folks are doing and telling us.

They are much smarter than we are about what is really going on as far as situational awareness. And so I think, because of that, the pendulum is probably going to remain where it is. And while we do – you know, I agree with Charlie and I mentioned it before, we do have to provide that balance. I think we now have a better appreciation of how to defend than we ever did before. And that is the result of the visibility and the transparency into the whole cyber program.

MS. DEMPSEY: Thanks, Priscilla.

MS. GUTHRIE: Yes, one last thought on that. We do have something that is very interesting to me. We have policies on information sharing and information protection and then we also have what I fondly call the "court system." And it is not really literal a court system but it is an opportunity to listen to concerns about information that is perceived not to be sharable.

And I think that it is an interesting checks and balance. You know, policy moves admittedly slowly, faster in the field but slowly at headquarters. But having a court system where people can come in under ICD 501 and talk about what works and what doesn't and prompt review of policy, I think, is an important part of the balance that Al talked about.

MS. DEMPSEY: Okay, great. Thank you. Lots of questions about uGov and I'm going to impose the moderator's tyranny and ask the one I want to ask, which is, with the announcement that uGov will be shutting down, will the agencies be moving toward providing their own classified, remote access, like NGA's current sensitive, Web-accessible, network-secure remote access, or what replaces uGov?

MS. GUTHRIE: Okay, let me take that one because – and that's why I took culture, too – somebody actually said that I had destroyed the IC culture because of the uGov thing. Golly, I hope that's not true. So the uGov timeline is – let's see, first of all, there were three parts of it: networks, collaborative tools, which as I said, we're moving into the main part of I-2, and then e-mail services.

The e-mail services support both the headquarters for ODNI and some users in the field. There is quite a long timeline that was being developed to look at how we move the mail services to existing offerings. The intent is to work with all the CIOs, and that includes not just the CIOs within the intelligence community, but also State and DOD. I guess State and DOD actually sit in the IC CIO council, so they've been part of it.

So yes, the answer is not to take away Web service e-mail; that was never the intent. The intent was that when we look at ODNI and scarce resources and the idea that we're not operators, it didn't seem that operating a separate e-mail system was an important part of our offering.

MS. DEMPSEY: Thank you. This is a very specific question, but I think it's an interesting one, and either Kelly or Bobby, maybe you can answer: Why isn't there an NGA server – Web, Google Maps, WMS – directly on NSANet and do you not see value in having that capability?

MR. MILLER: Go for it.

MR. LAURINE: Well, I think, you know, Kelly would tell you, sure, there's a value to that capability and as we move forward with NSA, I think that's something that we could entertain.

MR. LAURINE: Clearly, as we step back and highlighted supporting the RTRG initiative as well as other collaborative issues with NSA, the capabilities to provide Google Earth and mapping capabilities are clearly a capability that needs to be there. And I think that it's already there, as I understand it.

MS. DEMPSEY: Okay, thank you. For all of you, is the ICCIO council collaborating on desktop operating system migration? A shared roadmap for desktop operating system deployments would be very beneficial; for example, Windows N and N+1.

MS. GUTHRIE: Does anyone want to help me with that?

MR. MILLER: Charlie, why don't you talk a little bit about the cross-domain pilot?

MR. BARLOW: As I mentioned, we have a pilot program underway that is looking at creating a desktop optimization activity that allows us to have cross domain multi-system inputs where an analyst can take that information, can massage that information and then can take it and post it out at on SIPRNET or on JWICS through utilization of a single desktop. But what I think this question is really addressing is will we ever get to the point where we have a single operating system on all of our desktops, am I right Joan?

MS. DEMPSEY: I think so.

MR. BARLOW: So if you're looking at some of us, some of us are operating on XP; some of us are moving to Vista; some are waiting for System 7. But I think at some point in time, as we start moving with creating a more collaborative environment on the desktop, you will see that coming as a natural result of the things that we have moving forward.

At this point, it has not been considered to be one of the primary items that we needed to focus on. There were a lot of things – network integration, identity access management, are all things that we felt were of higher priority.

Moving into that type of environment is something that is probably on the agenda but, at this point in time, I would say is probably a little a lower on the priority list of the things that we need to address.

As long as we have an ability to be able to interface with each other, to be able to share information with each other regardless of what operating system we are on, we are getting the job done.

We have a common e-mail system now; we are building a common service directory where information on individuals within the community is listed so you can get e-mails to anyone that you need to.

We're all using certain products, the same, and so we can collaborate and we can move information between each other. So getting to the common operating system is not high on the priority list at this point in time.

MS. DEMPSEY: I think, based on the number of questions touching some aspect of a single intelligence enterprise, what I'm getting from now about 70 questions is that while it's true that there is the ability to communicate across agency or organizational boundaries, sometimes it is really, really hard and it requires different types of communication, different interfaces and a lot of work on the part of the people who are trying to communicate. So at least this group I think would like to see that priority raised a little bit higher in the future.

MS. GUTHRIE: So the whole – the first thing we talked about, the information integration – the first priority – that is a heavy-duty priority, and there are five subordinate pieces to that, but it's information, discovery and access; it's the audit capability; it's the identity management that Kelly talked about.

And the focus – not to take anything from what Charlie said – the focus is on providing the enterprisability, as I said, to technically discover and access information anywhere, anytime, prohibited by policy. So admittedly, that is the Holy Grail; we are not there yet, but that's why I put that first. That is the number one priority. I view that as somewhat different from working on a common desktop solution, but that is the Holy Grail; that's the top thing on the list and that is what we're focused on doing.

MS. DEMPSEY: Okay, great, thank you. This has been a terrific panel. I want to thank our panelists for being here today and providing such good information to the group, and thank you for your efforts.

(Applause.)

(END)

Ms. Priscilla Guthrie, Intelligence Community Chief Information Officer at the ODNI, moderates a panel at the 2009 GEOINT Symposium in San Antonio, Texas.