Program Transcript

Plenary Session #6:

A Conversation with Sue Gordon

Principal Deputy Director of National Intelligence

Walter E. Washington Convention Center, Washington, D.C.

Thursday, September 7, 2017

2:30-3:00 p.m.

This transcript has been edited slightly for brevity and clarity.

Participants

- **Sue Gordon**, Principal Deputy Director of National Intelligence, Office of the Director of National Intelligence
- **Letitia (Tish) Long**, Chairman, Intelligence and National Security Alliance (moderator)

Tish Long (TL): Thank you, Jill [Singer]. As Sue and I were listening to that introduction, we agreed, we saved the best for last and of course, representing – formerly, formerly –

Sue Gordon (SG): -- one of the great agencies --

TL: one of the great agencies [NGA], indeed. Sue, it is terrific to see you again and congratulations on your new position. I think it's been a little over a month?

SG: It has. I thought I'd be better by now, but I'm working on it.

TL: So confirmed on the fourth of August, a little over a month. But of course you've been in the Intelligence Community for a few more years than a little over a month. So let's just jump right into this: how would you characterize the state of the community? What's working well and what do we need to improve on?

SG: Great question, before I answer, let me offer the apologies for the Director [Dan Coats]. He really wanted to be here; unfortunately, maybe as a sign of the times of how this administration views intelligence, he had a principals meeting that he had to go to. Why was the principals meeting set today? It was because I wanted to be here. [audience laughter] I have 30 years of pretty slick tradecraft. [Audience laughter] So he thinks it was bad luck but it was actually purposeful design.

So here's what I'd say about the community. I'm old and I've seen a lot. We have never been better. The capabilities that we bring to bear are as stunning as any I've seen and I've seen a lot. The level of integration that we effect throughout the community is the best I've ever seen. I was thinking about the [IC agency directors] panel that was just here and if you ask me, one of the most exciting things that has happened in integration over the past five years was the inclusion of FBI and the growth that they've made as an intelligence partner and what that has allowed us to do against adversaries that have figured out coming to the United States makes it challenging for intelligence services. This partnership has allowed us to do great things.

We're awfully good, and we're not good enough. Intelligence is a business of advantage; that's really fundamentally what we do and for all the work that we are doing, boy, it's tough to stay ahead. I think what we're doing well is each organization is advancing its capabilities in a very tough environment. I think about the challenges that NSA faces and operating in a digital environment that is increasingly transparent to adversaries who might see you and people who have learned from what we do to understand that. I think about the CIA and the challenges of operating in a world where you must be who you are because of what's happened in terms of what (adversaries) know. I think about NGA and the challenges of harnessing a commercial revolution in GEOINT that has the potential to provide answers that you could only imagine in the past and yet you still have to figure out how to do it. And I could go on and on.

I think one of the challenges is just the continued growth in each of our discplines that make up the whole. We're not fast enough. We're not. The overhead we impose on ourselves is great in a world where speed matters, not casualness, but effective speed. When we have business processes that don't keep up, when we have barriers to effective sharing, we put ourselves at a disadvantage in a world where information and speed and analysis is at the premium.

TL: So along those lines, we had a panel earlier this morning about acquisition reform and we actually just heard the directors of the agencies talk a little about that, and in fact Kevin Meiners was a part of that panel and he coined – I believe Kevin coined this – CRTC, "cost realism, technically credible" as

opposed to LPTA [lowest price technically acceptable]. What can be done from the DNI's perspective on truly getting to agile acquisition or streamlining the acquisition system?

SG: Three things. Clarity of mission. What are we trying to accomplish? I know we like to beat on the mechanisms we have, but there are many mechanisms if you know what you want to do and you can articulate that clearly, so I think one of the things the DNI can do is to add and ensure that we are incredibly clear about where we must go to achieve the future. The second thing is, an environment where new capabilities can be added more quickly. I'm not going to talk a lot about IC ITE [Intelligence Community Information Technology Enterprise], but the imperatives of having a place where we can insert capabilities quickly, securely, and bring to commission quick is another thing I think the DNI can do because again it's that providing the foundation for collective effort that I think we can do.

And then the third thing is to really work on the issue of risk. It still feels that we acquire things as though those are going to be things that are going to last forever so we better make sure that we have it right. In my estimation we have to be right enough because things are moving so quickly that if software and hardware solutions change in six months to a year and it takes us two years to get something together. We simply have to be more thoughtful about the risks that we're introducing, and again, I think this is something the DNI can do to help level set what we're willing to accept by the processes that we by and large set the standard for.

TL: OK, good, three very specific things. You're not going to talk about IC ITE, fair –

SG: -- we can, but it's a topic we've talked about a lot.

TL: Exactly. But you also did mention integration, which of course was a focus for your predecessors, plural, both the DNI and the PDDNI. Is that still part of the DNI's and your vision continuing on the integration of the community?

SG: Heck, no. We think we should all go our way alone. [Audience laughter] Do not tweet that, it's a joke—humor. Lighten up, we're the Intelligence Community; we can be this way (chuckle).

Integration is our lifeblood. And let's talk about – the DNI has a pretty simple though difficult to achieve responsibility. The first is to make sure the best of the Intelligence Community is brought to bear at the moment of decision. Right? Not one voice, not one perspective, not people adding into something, but we each bring the best of what we each have to offer. That's the fundamentals of integration. And you do it for a purpose not because it's nice to have and so it's measurable. And that's a role specifically the DNI has. The second responsibility we have is to make sure we create an environment where each of our crafts can expand as they need to; in other words, clear the way. And that too is a different kind of integration. It adds a view of the polices and processes that govern what we do to make sure that we're establishing a way to work.

I see no diminution of integration. I do think where we can still grow is we are viewing integration as sometimes as additive – let's take all our capabilities and bring them all together to create the sum of what we have. I think the next step is to learn how to create together to do something new that each one couldn't do alone. So I still think there's growth we can do in how we think about integration, but that is our imperative from the DNI.

We just surveyed the community on the question of what the DNI does well and what it doesn't do well and I think we got as close as we're ever going to get to a mandate to exert leadership in the notion of bringing things together for new purpose so we'll push on that really hard.

TL: So that's good, getting that feedback. And you just touched on this a little bit and I've had a couple of folks ask if you could talk about – I think there's two reviews under way, there's an internal ODNI efficiencies review, and then there's also the future of the community. If you could talk about those, please.

SG: I think if we all went to our separate rooms and talked about what the Intelligence Community needed to be, we'd probably all come to the same conclusion, that the fundamental premise that we've always had of – and this is my paraphrasing – knowing the truth, seeing beyond the horizon, and allowing our policymakers to act before events dictate is pretty constant. I think one of the interesting things that has changed is that we've moved from a world of data scarcity to data abundance. Where we used to go looking for single pieces of information that no one else had and now what we have is a world that is so much information that we have to make sense of it. So if you think of the Intelligence Community going forward, how do you take advantage of the data that is now available and do something special with it so we know something a little more, a little sooner.

So IC 2025 is looking [at] what the community must be to continue to provide the advantage it always had. The DNI only exists to enable that. So you have to have that vision of where you want to go in order to be able to say, so now what is the DNI going to do. That's ODNI effectiveness study – I'm going to say effectiveness over efficiency because we've got into really bad trouble by saying we could do things a little bit faster and cheaper; we want to be more effective. And one of the ways we are looking at ourselves is to say what are the functions we must perform. Not the boxes we currently have, not the jobs we are currently doing, but what are the functions we must perform. If you take my earlier statement I would say there are probably four main functions – some of which we do well, some of which're not doing well. We have to help the community build more capacity, whether that's in artificial intelligence, or in cyber, capacity and capability. That is not a role that we have always played but I think you can see that there's some benefit, and I'll just choose what we're all doing in terms of being able to make use of all the data that exists, whether it's AI, or automation, or augmentation, all of us, Intelligence Community, DOD, we're all spending money—are we getting there? I think one of the functions we have is help that kind of leadership to make sure that when we do it, we actually are proceeding in a direction of outcome and we can then align the budget. So building capability and capacity; the second is adding context. That's what we do right now with our national intelligence managers and the job of integration is mostly to add that context. It isn't creating all that our own independent work, it's actually taking what's out there and producing something there. The third thing is, I'm going to say it negatively, but you can say it positively. I'm going to say we ought to reduce friction, or we could "accelerate the community" if you want to be positive about it, but we've got to get rid of the overhead. I am so worried about what we impose on ourselves.

TL: So are the agencies who are sitting here right before you.

SG: …right, and again, that's a function we have. Whether that's new business processes or legislation or looking at some of the policies or just the number of things we do or the way we task, all those things are just crushing us in terms of delivering the capability that I've just opined as there. And the last one is that we need to build some new bridges to partners outside the Intelligence Community. Whether that's the private sector, academia, or other governmental institutions. Even the big DOD that you would think that we have perfection with, I think that we still can do more. So if I think of those functions, then we'll use that to really align what we do, and align our resources, and neatly enough it will constantly change as the community changes and we drive the DNI. But it ought to be what you see reflected in our budgets, we ought to measure our accomplishment, and we ought to provide the room for the agencies to be really successful.

TL: And it gives you your priorities.

SG: It does, it's great, and it's pretty easy.

TL: So let's follow on from that, the building more capacity and capability. So this audience, and you just said also building bridges—we've got industry here, you've got academia here, you've got other government institutions, as well as DOD. Let's characterize: how are they doing in supporting you? How are you doing in partnering with them? And what more can and ought you to be doing together? That's a lot of questions there.

SG: Whoa. Out of time? [audience laughter]

SG: So I'll choose two areas that I think are really important and I'll trying to answer your questions. I'm going to take the data piece on AI and automation and augmentation. If you look at how much the U.S. Government is spending on that – we spend a fair amount. It is nothing compared to what is being spent in the private sector on the exact same things. How are we going to use the money we have to influence the money that's being spent? Because we know two things. One, if we just let the private sector go in that area, they will advance it but they will not necessarily advance on their own ways that solve our problems. Our problems are that we are simply going to be unable to make use of all the information that exists and that can help us provide more advantage if we continue to do so manually. Right? So all the money's out there, we have some money, we have to leverage it because we have needs that may or may not be met. And we on the government side I think are too disparate in our approaches, whether that's where we spend the money or how many times we go talk to the same partner about the same thing, not ever having that turn into a purposeful conversation. I think the DOD and IC need to have more conversation about this because increasingly we're part of the same continuum and they are just as interested in cloud and these technologies. We have to put our [inaudible] together.

I think we may have to come up with some sort of interlocutor. Whether we use some of the mechanisms we have in the past, whether it's IARPA or DIUx or In-Q-Tel or some other way for us to be able to have effective conversations between the government and people who may or may not—because of the whole privacy discussion—want to participate. So that's one.

Cyber is another one. Would we agree that as nation we need to get our act together on cyber a little bit more? Just a quick show of hands. Yeah, right? What's interesting about the cyber problem is that 90 percent of the issue is non-governmental. Right? It is, it's private sector, it's the vectors, or it's the target. And yet what we have is the ability to know things somewhat in advance of attacks but we can't see them in the same way. So how are we going to work together in a trusted way to be able to share what we both know in order to better protect the nation? It's a different kind of partnership that we need – but it does require both sides to find a way to trust and respect. Trust each other a bit to come to joint solution and respect the value proposition of both sides to not make it together. So just two areas I think that's what you have to do. And then one other thing, Tish, though you didn't ask for it, I think one of the things that we need to do – and I'll put this on the DNI's head – I think we need to engage a conversation with the American people because this whole security and privacy is too often set up as an oppositional thing –

TL: Either or --

SG: What I say to people all the time is we're on the same side. The people on the government swear to uphold and defend the Constitution of the United States, which is predicated on the notion of individual rights and privacy. This is one where we are going to have to reframe our conversation, because I think if we spoke about what we do whether it's from [FISA Section] 702 that I know you talked about earlier, to this kind of public-private partnership I think that we could – I think there is much more common ground than we presume.

TL: Good, we did talk about 702 earlier. I'd like to give you the opportunity to add anything to that conversation that you might like to add. Is it a priority for the DNI and for the rest?

SG: Yeah, I don't think there is anything more important over the net between now and the end of the year than to get it continued. It's simply a capability that we know has great effect, demonstrable effect that we can't replace any other way. We're confident that we have the guidelines, procedures, in place in order to protect the rights and privileges of the American populace, and we have to do this. We have to do it. I think we have to be able to describe it, not only the ways that we effect it and the ways that we govern it.

But I also think we need to talk more candidly about what it is and what it isn't. I think in the aftermath of Snowden, too many people think that this is just putting huge segments of the American population at risk for being sucked up into some great abyss that people can just go off and search. That is not the case at all, as I'm sure the previous panel says. It's a very simple program. It allows you to target

non-U.S. persons who are credibly believed to be outside the United States for the purpose of foreign intelligence. That's it. We have to have reason for targeting; it isn't a large number of targets, and what I would say if you are not talking to one of those people, you're not in existence in this world. I think we need to talk more openly because I think if the American people knew, they would support it as strongly as we did because of the benefit it provides.

TL: And I know Admiral Rogers has been out there really trying to tell that story as well as Director Wray, and so you adding your voice to that conversation I think is good. We did hear from two members of Congress this morning who felt that it would be reauthorized. Now that was only two of 535 -

SG: -- it's important, Tish, but it's also important that were able to talk about it. That's why this forum is so important. We learned our lesson with Snowden when we didn't have a voice, we have to be able to have a voice and tell our story.

TL: Well, we appreciate you appearing here Sue. Cyber, we have some questions from the audience I'll kind of integrate them in with the questions that I've already started with, but here's one on cyber and the role that the IC should have. What role should the IC play on cyber, given that the cyber domain tends to blur the lines between offense and defense and between espionage and military action? Should the Intelligence Community be conducting offensive cyber operations?

SG: The Intelligence Community - that's such a great question - the Intelligence Community is disproportionally in the business of collecting foreign intelligence. In this world most of the information exists in the digital domain and you have to go and be able to get it and it doesn't necessarily all just transit big pipes, it exists in lots of places where you need to go and get it. But the purpose of it is to do the historic purpose of the Intelligence Community; it's to know a little bit more and go where the data resides. So, in terms of authorities, those are pretty clearly delineated, again, by law. It is blurred because the domain is blurry; it intersects each other. But the authorities to conduct certain actions are either given to agencies—NSA's authorities, CyberCom's authorities, foreign intelligence collection authorities, and covert action authorities—and those are pretty clear and we know how to navigate those. So to those that think that yeah it's a blurry domain where we have to de-conflict our activities, but what governs the activities are pretty clear and distinct.

TL: Okay, Sue, in just about every panel, at least that I've sat in yesterday and today, the issue of security clearance reform has come up. I'm sure you're not surprised that I've just uttered those words --

SG: I know, it's weird. [audience laughter]

TL: The DNI - now there's been actually some suggestions, there's been a lot of complaining - but the DNI of course is the security executive agent. What everyone out there wants to know, inquiring minds, what are you doing to fix this and how long is it going to take?

SG: Okay –

TL: She said I could ask her anything –

SG: I did – it was real fun to talk about all of the national security threats we face and the capabilities we must effect in order to do that. I don't think there is anything more important for us to address that I'm going to call secrecy and security. We need to trust a reliable workforce but the workforce is one that - one, isn't going to be static, you aren't going to have a lot of people like me that are in this community for 37 years kind of straight through. We want them to be able to move in and out. I want to be able to attract the best talent, I don't want to lose them in the 15 months that it takes in order for them to get through. I want people to move in and out of our contractors, I want to be able to tap the expertise of the private sector to fill the gaps in our knowledge or the time gap between when I can hire staff people to do it in right now. Our system just isn't designed to be able to support that kind of mobility with the security that we wanted, the protections that we need to have. We will not succeed if we don't take this on. I can think of no higher priority.

SG: What makes me concerned is how many times have we tried this. How many panels, how many times have we looked at this? We will lead the effort to address this, both in terms of the vetting process and the other side, which is just security in general, and I can apply the exact same thing to our information systems, where our security systems aren't designed to allow us to quickly understand the risks of putting new capabilities in. I can't tell you how long it will take. I do know that the energy around it at the moment. I think this is an exciting time for us because I think that we have– we have great interest in the administration and the legislation in us getting on with this. Almost everyone is begging us to clean this up and produce something that will work. If we squander this moment where everyone is aligned to say we must do something, because each one of us is protecting how we've done things, more than what we must be able to do, then you'll have a sixth principal deputy pretty quickly. I wish I could promise you more, and a time frame and specifics on exactly how we do it—this is a partnership that we're going to have to effect. It's the topic of the conversation at my very next ExComm of how far the agencies [are] willing to lean in. The DOD is moving on this as well; I do not think this is one of "lacing up our shoes tighter and thinking we can put more people against it," we're going to have to reimagine how it's done.

TL: And there's a lot of folks in this room who have some ideas, some technologies, and – you know – are willing to help here. I'll just put a plug for INSA and the work that we have done with our security clearance process reform group led by Charlie Allen -

SG: Yeah, I'm looking at the faces in the room

TL: And there are some real concrete recommendations out there. You have some good pilots underway also. So you talked to the information systems, the whole continuous monitoring piece, and then of course continuous evaluation. So let us know, and that's a collective us, what we can do to help.

SG: I will, I will. The one thing I think we're going to have to do as a community is – I mentioned this earlier – it's this whole notion of risk. Zero loss is the way I grew up, right, for all the good reasons that we know. All the sources and methods that we have, all the things that we want to protect, the reality is that zero loss is not something that we're achieving today, and it's probably not the right thing and if you look at some of the security things that have been implemented in our world that you don't have to have zero loss but you do measuring and you do policy strategy, I think there will be ways forward. So I'll take you up on it.

TL: And it is all about risk, I mean there's a question here on leaks. There have been leaks --

SG: Yes.

TL: There will be more leaks –

SG: Yes.

TL: I mean, it is a question of risk.

SG: It is. I will say that unauthorized disclosure of classified information is always bad. It's always bad.

TL: Of course.

SG: But, I will also say that some of the burden is on us because we have classification systems that are pretty hard to understand when you classify information, so it's hard to know always where your line is. So, no leaking, it's bad, it gives us a disadvantage. No deciding what is "real secrets" and not. We build our capability with things that look innocuous to deliver great capability, but we as a collective have to look at this too because it's a crazy world in terms of the information that is available outside of our system that's putting us in conflict.

TL: Speaking of capabilities, here is a question from the audience. The Intelligence Community has focused on terrorism and on the wars in Iraq and Afghanistan for 15 years now, more than. Has the IC sacrificed the ability to understand strategic targets like China and Russia?

SG: Closed system. Finite set of resources, have to apply them to the pressing challenges of the day. Hard to argue with the choices that we made about counterterrorism following 9/11 and what that meant about very different target, very different set of capabilities you had to have, and a lot of energy in order to prosecute at the speed that it was evolving in a very different way than nation-states did. So I think that it's probably true that if you look at it that way you could say it sacrificed -- it had a cost, I guess, of resources. When I started, I was in office of scientific and weapons research, one of the great offices of all time at the CIA and there were about 750 people, 749 of whom did the former Soviet Union and one person did China and he also did the rest of the world. As the Wall came down, as proliferation became important, we took those capabilities and we applied them somewhere else without the foundation. Do we have those capabilities, that number of resources devoted, now? No. Do we cover the world's threats better than we did before? Yes. I do believe that strategic is one of the things that my national intelligence managers should be focusing on. Right? We have lots of people do the tactic work, how do we make sure we're prepared for the future, so when it comes we're winning. … We're out of questions?

TL: Oh, we are not out of questions. Oh, no. No, but we got the 5 minute warning.

SG: Oh awesome. Okay I'll answer everything in a tweet from now on.

TL: I haven't given you a chance to really take a step back and say so, what are the priorities of the office. Have you and the DNI had a chance—I mean you've been there a month, he's been there 8 months—you know, what are the top things that you're working on, where are you focused?

SG: So, one of the things that's really fun about having a DNI that disproportionately comes from a policy community is the effect I believe we'll be able to have when we deliver the intelligence that makes a difference. So, I'm going to choose the kinds of things - the priorities - some of which get chosen for us and some of which are enduring. We mentioned 702, we have to drive that across the finish line.

North Korea is vexing. They are on a path that seems inexorable with capability that is advancing every day with demonstrations that prove that their aspirations are not a pipe dream. And what is the U.S. and the world's response going to be. So how do we provide the intelligence that is necessary for the decisions that we're going to have to make as a nation? And that's not just against North Korea, but it's building a coalition because the pressure we're going to have to put is widespread.

Iran, another priority, is we look at not only its growing influence in the region because the conflicts in that area but also just continue looking at the [inaudible] to make sure that it puts us in a good place. Counterspace. An area of tremendous capability and dependence for us. How we make sure that we're both positioned to understand the threats we face, but also to support a growing industry that is also part of the great strength of this nation. Counterterrorism, it's a very different face than it was post 9/11, it's a very different face than even fighting the war in Syria against ISIS. It's like a half-full water balloon, when you squeeze on one end it comes out of the other end. Instead of just big-named targets this great mass of capability that seems to be able to effect terror, and what's the intelligence piece of that? How do we get intelligence to, I'm going to say non-national security partners, whether that is the private sector for cyber or whether it's intelligence that can support local law enforcement. And the last one is just this notion of foreign influence and geopolitics in general. How do we understand what that is because it effects everything from the order of the world but also our ability to understand what we're seeing in a world where things can be not what they are. But other than that, easy day.

TL: There are a ton more questions here, Sue, as you can imagine, and one was on the homeland front, and the working with state-local-tribal [law enforcement entities], and why is it still so hard. Another one on how are we doing integrating and working with our international partners. I mean you mentioned coalition forces, but we had a panel earlier today on counterterrorism with Nick Rasmussen and then representatives from the UK, Canada. What's your assessment on how we're doing on the international front, and on the homeland front?

SG: The homeland is interesting - we see it, we see the potential benefit that intelligence has to address some of those issues and we're finding ways to be able to use the organizations that have the

responsibility for interaction to give them better intelligence in a form that they can use to share it. That's a little clunky still but I think there's some places where you see it going really well. NGA, I'll shill for them a bit on this one, is one where they're really figuring out how to use it. What's interesting though even on the homeland is some of the capabilities that we grew in the Intelligence Community that makes us need to partner with them now, are actually capabilities that are increasingly available in the open. So it think there's almost a temporal effect of how much the Intelligence Community has to stay present or how much we need to see now for a capability that's going to come.

I'm really excited on the international partner front. One, I think we're better [on] 5 Eyes than we've been in a long time, including the integration of their officers with our officers in more places. On lots of different levels I think the next place were going to have to go is to be able to share information more quickly, digitally, and that's going to require us to really advance on the security front. Because these rules we have in terms of how you share, with whom you share, are not silly. So we have to find a way to affect them in a digital environment so we can get the sharing with the partners that we know we need in order to be able to get the information they increasingly have and we have and then we need to develop systems where that information can go right into each other's processes in order to do it and make sure that it's done in a way that you can trust the information that you have, because that's the other side right? I can put a lot of information in the system but what our lifeblood has been is trusted information and how did we affect that. So, pretty interesting world but on the partner front I think you see a lot of movement.

TL: Well we got the one minute warning about three minutes ago, Sue thank you very much we appreciate your time, we appreciate what you're doing. [audience applause]

SG: How fun was this?

TL: And I think I can speak on behalf of everyone here, we are certainly glad that you have taken on this next challenge and that you are our principal deputy director of national intelligence. So, thank you.

--END--