Interview of the Honorable Dale W. Meyerrose
Chief Information Officer – Office of the Director of National Intelligence

With Ms. Dorothy Ramienski of Federal News Radio
“Ask the CIO”

April 12, 2007
Transcript – As Aired

ANNOUNCER: Good morning and welcome to “Ask the Chief Information Officer,” brought to you by SAIC on Federal News Radio on AM 1050. Every week Federal News Radio interviews CIOs of federal agencies about the latest directives, challenges, and successes. “Ask the CIO,” with your host Dorothy Ramiensky.

MS. RAMIENSKI: Today my guest is Dale Meyerrose, Associate Director of National Intelligence and Chief Information Officer of the Office of the Director of National Intelligence. Thank you for joining me. Let’s get started.

I think something that’s extremely topical concerns which agency should have control of what information. Maybe you could touch on how this debate affects your job as CIO.

MR. MEYERROSE: And it’s really at the crux at what I do. Ever since 1947 when the intelligence apparatus was set up in our country, the idea of information ownership was a central part of it, controlled by whoever collected the information. And as the events of 9/11 and the information age have shown us the business about ownership is not a good way to think about it.

So we try to think about it as stewardship. The nation owns the information, not any particular agency. And as stewards of that information, we have responsibilities and Director McConnell, the DNI – the Director of National Intelligence – has tried to inculcate in us the idea that we have a responsibility to provide, which goes beyond just the business of owning information, beyond just the business of sharing of information, all the way to the concept that says we have a responsibility of stewardship, that says that we need to ensure that bring along partners, stakeholders, and folks who are users and consumers to ensure that we provide all those responsibilities.

MS. RAMIENSKI: Let’s talk a little bit about the actual mission of the Office of Director National Intelligence. The mission as stated on your website of the Office of the Director National Intelligence is to integrate foreign, military, and domestic intelligence in defense of the homeland of the United States and of our interests abroad. How do you, as CIO, support this mission overall?

MR. MEYERROSE: I think if I re-characterize it some plain language, it kind of makes it a little easier to understand what I do. In essence, we were created as a result of 9/11 and the war on global terrorism. Our organization is the [Office of the] Director of National Intelligence. Our responsibility is to make intelligence better and we have 16 different intelligence agencies, organizations around the U.S. government who are individually excellent, centers of excellent in their own right – some would say without peer, I would say without peer. But together, they need to be – we need to become better. And so that cohesiveness, that collaboration, that synergy is really the responsibility of the Director of National Intelligence.

In that view, my principal responsibility centers around information sharing and all the concepts all the way from the technical side through the policy side of sharing information. And as you might imagine, information is really the essence of what intelligence is about and does that information get to all the people it needs to in a format that they can make use of it and does it get there in time in order for them to perform their job. And so, in a nutshell, that's what I do, again in the context of making the intelligence community collectively better.

MS. RAMIENSKI: Just to kind of put in perspective for our audience, perhaps, take us through a typical day. What happens as CIO for you?

MR. MEYERROSE: Well, the first thing is I enjoy the Washington traffic on the way to Bolling Air Force Base. (Laughter.) But beyond that, I have a series of interactions, both in the Office of the Director of National Intelligence and with other elements of the federal government on a broad range of topics.

And, you know, in the course of a typical week, I'll participate in one or two inter-agency forums, you know, usually in the Old Executive Office Building or the New Executive Office Building, or in somebody else's facilities. I'll spend a significant amount of time interfacing with other Chief Information Officers, not only within the intelligence business, but also across the federal government.

We spend a significant amount of our week in trying to make sure that we have the right processes in place for the purpose of making intelligence better. And then we try and set aside a significant portion of time to get feedback. When we talk about the field, we talk about intelligence organizations who are outside of Washington, D.C. supporting a myriad of military and civil missions on a global basis and getting that feedback from those users plus our allies in sharing – in how effective we are in sharing information is very important. Because the philosophy about what is measured is what you do well is something that we find very, very useful.

MS. RAMIENSKI: Maybe you could touch a little bit more on – since my third question has to do how closely you work with other CIOs – maybe you could just touch a little bit more on that.

MR. MEYERROSE: Sure, I'd be glad to. And if I could adjust again the sight picture here a little bit, I work with as many policy organizations as I do Chief Information Officer organizations. And that's because of the responsibilities and alignment of the Chief Information Officer within the intelligence community. We have a series of governance organizations. Some of them are internal to CIO type of functions; those tend to be more technical, tend to be more process-oriented, and tend to be elements of collaborating to make sure that we're both working on the same set of standards, the same set of processes, the same set of terms of reference, if you will.

Beyond that I've already mentioned working with policy elements and those tend to not be in chief information offices; they tend to be chief of policies of various agencies and organizations. And there we work very hard on policy, but not just the business of making policy. It's what are the second and third order effects that result from policy and does that policy make somebody's job easier to do.

There's sometimes a tendency to say if something's not expressly permitted, then you're not allowed to do it. And, of course, you know, that's sometimes the trap that you fall in when you work policy kinds of issues. And policy issues tend to have lots of resource impact and so chief financial officer organizations around the federal government are probably another part of the nucleus of what is important for us to work with.

MS. RAMIENSKI: Do you find as CIO that standardization is a problem? I've talked with other CIOs who say this is a real challenge for them, getting everyone on the same page when it comes to technology. What about you?

MR. MEYERROSE: It's interesting. Some things are very easy because they're pretty close to de facto to what everybody's doing, so agreement is fairly easy to reach. And once you've established that trust then you can, in fact, work together and establish some of those agreements, some of the tougher issues become less problematic.

But you're really talking about culture, and that "I like the computer set up this way" – well, my mission's different and so I want this adjustment to be made. So it's the business of does that adjustment – does this tailoring – affect the people that you interface with? If it does, then we need to curb the desire to have something a little different. If it is not critical, if it is not pivotal to how you interface with other organizations, then it becomes less of a problem.

There's a phrase that I've got which kind of captures this thought: every line of locally developed code represents a stovepipe to everybody else. And so working through that mindset that says that I could serve my particular internal mission this much better with this tweak, what kind of problems do I pose for my stakeholders, my partners, my users, and all those kinds of – oftentimes in the past, we have not had to make those outside considerations.

You know, in today's age, today's technology, those are the first considerations you need to make, not how do I personally do something more efficiently.

(Commercial break.)

MS. RAMIENSKI: Let's talk a little bit about IT security. What are some of your main concerns? What are you most worried about?

MR. MEYERROSE: Well, I'm always most worried about what I don't know. (Laughter.) But without getting too academic, something that we've been working on in the security area for the past year is, again, how we affect and interact with other folks and how we bring our risk and allow risk into our networks, our processes, and our systems.

In a vernacular – particularly within the intelligence business and the Department of Defense – we call it Certification and Accreditation. And these are the series of processes that we work that says we will – we understand the vulnerabilities and the capabilities and the inputs and outputs of whether it's a piece of hardware, a piece of software, an application, a system or whatever, and this is how we incorporate it into our network, into our enterprise. And so we've been working on that for over a year.

That was a policy that originally took three years to write, four years to coordinate, and we've not touched it in the last five. And I think that's because everybody thought it was so painful the first time, we don't want to go through it again. But if you add up all those numbers – and I don't do math in public very well – but what that says is a lot of our risk management criteria and our security policy is almost 10 years old, okay? And has technology changed in the last 10 years? Has how we use it changed in the last 10 years?

And you know, all those are very obvious questions. And so to me, it was just as obvious that we needed to become more dynamic, more inclusive and use some common sense in updating security standards, security policies and such. And so we went about a fairly lengthy process of inviting industry and academia plus all of our government partners in to help. And of course, the first thing they said, "but you're in the intelligence business, you know, we're not used to participating in this process." (Laughter.)

And so that openness, I think, has been a hallmark of the Director of National – of the Office of the Director of National Intelligence. And it became important to involve all of those folks in the process because they were affected by all of our determinations and, again, understanding second and third order effects in that equation was hugely important to us. And so we've worked through to where the National Institute of Standards and Technology and the Department of Defense and us have agreed to change seven major elements associated with what our security policy used to be and how we certify and accredit systems.

MS. RAMIENSKI: Do you think that as a, I guess, a newer agency – do you feel that because this is a newer agency, you've got a better perspective on IT and the problems associated with IT security?

MR. MEYERROSE: Well, you know, where you stand is where you sit, I suppose in many regards. The elements of a new agency are that all the other agencies aren't used to accommodating you and so while it's an easy thing to send you a copy of our normal correspondence, it takes a lot more effort to actually involve a new agency in the process of generating that correspondence or the process of doing business or the process of making decisions.

And so we've had those normal kinds of growing pains, if you will, in the first two years of the Director of National Intelligence. We've gotten by most of those early pains. Organizations know who we are; we've established elements of trust. We are effective in each others' processes about making the appropriate inputs, participating in a collaborative way of making appropriate decisions at the appropriate time. You know, I know people are counting days and months and years since 9/11 and there's nothing I can do about prior to the existence of our organization other than to realize that the war on global terrorism is a daily war and it is something that we don't have margin for error.

It's something that we have to take very seriously; we have to work very hard and recognize that in the intelligence business we need to allow the American people and all of our stakeholders and people who use our products to know that they have a right to understand what we do. Now, it may not be how we do it because that's the elements of the intelligence business, but we need to be more open. We need to be – have better outreach and those kinds of things. And again, that's the fundamental core of the Director of National Intelligence: being that facilitator which makes all the intelligence agencies more effective.

MS. RAMIENSKI: Let's step back from talking about the Office of the Director of National Intelligence and maybe talk about CIOs and the vision of CIOs as a whole. There was an article earlier this year in Government Computer News that quotes Karen Evans as saying, the Chief Information Officer is not a Chief Technology Officer, but they need to understand technology. And then the article goes on to say many CIOs, according to certain experts, have yet to force their way into the boardroom. What's your take on this?

MR. MEYERROSE: The concept of a Chief Information Officer is only about 10 or 12 years old: again, the growing pains of being a new force, a new element in process and business and those kinds of things. And I think a lot of the people that occupied the early offices of the Chief Information Officer, in fact, were information technology-based, so they were not raised, if you will, in their professional careers to be a part of boardroom decisions and things like that. They were raised to worry about red wire/green wire connections; they were raised to worry about whether or not the red light's on or the green light's on on the box. And so the business of information technology is a different set of skills than working information technology.

And the chief information office, as intended by Clinger-Cohen – which is obviously oriented towards the government sector, was to develop the business of information technology. And so in some regards, we've had to grow into that. We've had to grow a new generation of folks, just like corporate America did, of who maybe early in their careers had very technical, very finite jobs, and then as you move up through the ranks, you have to become more oriented towards what are the purposes of the business.

I recall reading a couple studies about two years back and they were studies on the global Fortune 500 companies and, in fact, less than 15 percent of the global Fortune 500 companies had anyone on their board of directors who had any information technology anywhere in their background. Why was that? I think that's again because the idea of having a Chief Information Officer who was about the business of technology and how it helped the business either improve revenue, have efficiencies, broaden its customer base or whatever, was just a foreign concept and it's taken us this long to grow into it.

There still remain, I think, two kinds of Chief Information Officers: there's the CIO who keeps email working and keeps track of IT services and assets and then there's the CIO which helps the corporation decide business direction, make corporate decisions. Both are still very essential. And the way we've tackled it is we've tried – in the Director of National Intelligence – we've tried to adhere to – as close as we could – to the letter and intent of Clinger-Cohen. And so my responsibilities are along the responsibilities of the business of intelligence and how information technology supports it.

I personally do not supervise anybody who provides IT services either within the Office of the Director of National Intelligence or to the intelligence community. Again, it's a recognition, I think, that this is an evolving role. It has not been around as long as, say maybe, the comptroller function or the marketing function or other kinds of functions in the commercial world, just like it's not been around in the government area as long as maybe logistics has or operations or whatever.

Plus, the impact of information technology in our business process, our mission process today, is fundamentally different than it was just a few years ago. If you think about it, 20 years ago, the prestige in the information business was whether or not you had a Selectric typewriter with an automatic reversible ribbon in which you could X out mistakes and still have a clean final product. We've gone from that to where I'm going to share my workspace as I create things with people that I don't see, not in my office, on a broader – and so, just what information technology does today. By necessity, the role of the CIO has to be a continually evolving one.

I see the role of the CIO – I would change the word I from Information maybe to Innovation. And so we in the CIO business, in my belief, is we largely represent the constant change of the nature of business process within all of our organizations. And so that's why I think you have a wide range of all the way from still a technical service provider to someone who is in the boardroom helping the corporation decide strategic direction.

MS. RAMIENSKI: I can only imagine the changing role of the CIO because it seems constant because technology is constantly changing, too. I mean, there are things around that are available now that weren't even on people's minds three years ago, let alone 10 years ago. What's your take on that?

MR. MEYERROSE: You see, it's about rate of change. For instance, I came in the United States Air Force over 30 years ago and I was in what one of the feeders of the information technology business was – in the Air Force we called it communications electronics. My largest work center in 1976 was a teletype maintenance work center. So there was nothing in 1976 – nothing more mainstream to communications and information sharing than the teletype. I don't think there are too many teletypes left.

And so where did all those people go? Where did the teletypes go? Well, we got replaced by technology. And, oh, by the way, the people didn't go away. We retrained the people; we re-educated the people. They took up functions such as small computer maintenance; they became database managers. The technical skills and the people skills that were needed by folks who worked on teletype maintenance – you know, a lot of that was directly transferable.

See, the technology is almost transitory if you think about it. You know, what makes an organization world class is what people does that attract, recruit, train, educate, and retain.

(Commercial break.)

MS. RAMIENSKI: You touched on your work with, maybe, chief financial officers a little bit earlier. And I think your agency is different than others because like you said before, you're fighting global terror everyday, every minute. How do you decide which projects get precedent? Because I feel like your agency is one where the newest technology is needed the most and – correct me if I'm wrong on that – but how do you decide which IT projects get what money?

MR. MEYERROSE: Well, first of all, we have some guidance. We have guidance from the Office of the President; we have guidance from Congress. A lot of that guidance has been distilled in executive orders from the president or in such things as our National Intelligence Strategy. And I think that's a pivotal document to make a point here.

Our first director of National Intelligence, John Negroponte, helped us create our first National Intelligence Strategy document and I think the thing that was transformational about it was that we made it unclassified. In fact, all the coordination process, as I observed it, was classified and the intent was – of the bureaucracy – that it needed to be classified. But I think he had the wisdom which said this is a paradigm we need to break; we need to have a sense of openness like I've talked about with our outreach and such.

And so by modifying a half a dozen paragraphs, the National Intelligence Strategy, which we publish is unclassified and available not only to our other partners within government but also the American people who care to read it.

One interesting thing, I think, about the National Intelligence Strategy is that the Chief Information Officer has at least a half a dozen specifically outlined tasks in the National Intelligence Strategy, which goes back to my previous statements about how important alignment is in working in the boardroom, if you will, and being at the decision table. So lining up those things, I think is – tells that story.

Now, as you know, and probably many of your listeners know, the details of the intelligence budget are classified. I personally don't think that we can be more open there, but what I personally think doesn't matter. The policy is that it's classified.

But we make it a point to be very inclusive for any decision that we make. And they're not votes; they're voices. You know, some people tend to think, well, you know, I can vote and non-concur and – voices. And voices of concern as we go through decision processes and so I don't make any recommendation on any expenditure or any decision on any program without first vetting with stakeholders, the users, program managers, and the components within the intelligence community because the components within the intelligence community are the organizations that actually carry out these projects. As I said before, very few of these projects you find in my office. You find them in the various agencies across the intelligence community.

And so we've established a governance process which works very, very hard to incorporate all those things. And if you want to know what we use as priorities, all you have to do is look at the National Intelligence Strategy. And remember that we're in the business of making intelligence better. We're not in the business of improving IT; we're not in the business of buying new IT; we're not in the business of upgrading IT unless it makes intelligence better. And so that's the guiding principle that we use for projects and making resource decisions. And we have guidelines out there. We have architectural guidelines; we have standards guidelines; we have a series of guidelines by which everybody knows the rules by which we engage in these discussions and so that's the basic approach we take.

MS. RAMIENSKI: Let's talk about – take a step back for a minute and look back for me and tell me a little about some of the projects of which you're most proud.

MR. MEYERROSE: Some of the initial things that we did, I think, were very, very important. A lot of them had to do with, again, this theme of sharing information because the reason the Director of National Intelligence was created – (audio break) – result of several commissions and actions by Capitol Hill, the administration, and a lot of other folks that said that we did not share information to the extent that we needed to, and that perhaps we could have interfered with the chain of events – either of 9/11 or other types of terrorist activity or extremist activity – around the world.

And so one of the early information sharing projects that I worked on was about opening up what was previously no-foreign networks to our allies. And we worked very hard. In fact, it had a euphemistic title of the Big Idea and that was because it was really seen as we are trying something that we've never tried before. And in a fairly short period of time, we managed to provide an avenue of information sharing on classified networks in operational environments that we had never done with allies which we think makes us more effective.

By the same token, we've had a couple other planning activities where we worked something on behalf of the federal government, not just the intelligence community. The middle of last year, we and the federal government were working on developing a planning mechanism to deal with pandemic issues. And so we in the intelligence business were asked to create a top secret, a secret, and an unclassified series of portals interfaces on which folks across the federal government and some state and local and other kinds of folks who were working with the federal government pandemic planning substances together. And in a fairly short period of time, we have a series of planning mechanisms of information sharing portals at the top secret, the secret, the unclassified levels by which about 45,000 people across the country and, in some instances, foreign governments use those mechanisms for planning activities associated with dealing with pandemic issues and problems.

So those are a couple, I think, of the – and, again, you notice the common theme of information sharing, the common theme of collaboration. And I would offer those as an example of one within the intelligence business with allies and the other is an example with other government partners in a less traditional role of the intelligence business as a couple of examples of how serious we are about figuring out how to share information in the right kind of way.

MS. RAMIENSKI: I guess maybe as a final question this morning if you could tell us a little about some of the projects or issues that you and the rest of the people who work at the Office of the Director of National Intelligence will be working on in the future.

MR. MEYERROSE: Well, there are a couple things I'd like to make about the future and that is to stay relevant we've got to continually challenge ourselves with regard to change. And we talk a lot about change; some people like to use the – I call it the T word – transformation. So staying relevant is very, very important.

And sometimes, you know, when we get into the business of fielding certain kinds of technology and becoming comfortable with that kind of technology, to move on to something else becomes a cultural mind shift change and we've got to continually work our organizations to do that.

And the other is to restate the point because I think it's so important. The most important function of any organization is to attract, recruit, train, educate, and retain the right kind of people because all problems are people problems. And there are no new problems in the world, just different ways in which we can address them. And at the heart of everything we do within our CIO organization is to work that people problem so that people become more effective in doing the jobs that they do.

MS. RAMIENSKI: That's all the time we have this week. I'd like to thank my guest, Dale Meyerrose, Associate Director of National Intelligence and Chief Information Officer at the Office of the Director of National Intelligence. I'm Dorothy Ramienski. Thank you for listening.