INCIDENTAL PAPER

Seminar on Intelligence, Command, and Control

NIMA and the Intelligence Community
Roberta E. Lenczowski

Guest Presentations, Spring 2003
A. Denis Clift, Dale W. Meyerrose, Roberta E. Lenczowski, John P. Stenbit, Patrick M. Hughes, James M. Simon, Jr., Richard Hale

July 2003

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

The Program on Information Resources Policy is jointly sponsored by Harvard University and the Center for Information Policy Research.

E-mail: pirp@deas.harvard.edu URL: http://www.pirp.harvard.edu
ISBN I-879716-86-0 **I-03-1**

July 2003

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University **Center for Information Policy Research**

Affiliates

AT&T Corp.
Australian Telecommunications Users Group
BellSouth Corp.
The Boeing Company
Booz Allen Hamilton
Center for Excellence in Education
Commission of the European Communities
Critical Path
CyraCom International
Ellacoya Networks, Inc.
Hanaro Telecom Corp. (Korea)
Hearst Newspapers
Hitachi Research Institute (Japan)
IBM Corp.
Korea Telecom
Lee Enterprises, Inc.
Lexis–Nexis
John and Mary R. Markle Foundation
Microsoft Corp.
MITRE Corp.
Motorola, Inc.
National Security Research, Inc.
NEC Corp. (Japan)
NEST–Boston
Nippon Telegraph & Telephone Corp (Japan)
PDS Consulting
PetaData Holdings, Ltd.
Samara Associates
Skadden, Arps, Slate, Meagher & Flom LLP
Strategy Assistance Services
TOR LLC
United States Government:
- Department of Commerce
  - National Telecommunications and Information Administration
- Department of Defense
  - National Defense University
- Department of Health and Human Services
  - National Library of Medicine
- Department of the Treasury
  - Office of the Comptroller of the Currency
- Federal Communications Commission
- National Security Agency
- United States Postal Service

Upoc
Verizon

NIMA and the Intelligence Community

Roberta E. Lenczowski

March 6, 2003

Roberta E. Lenczowski is technical executive, National Imagery and Mapping Agency (NIMA). She began her professional career with the Defense Mapping Agency (DMA) in 1977, and after serving in several technical positions was promoted to a supervisory position in 1984. In 1986 she was made a supervisor in the digital products department. In 1987, when the DMA realigned its technical support into a Systems Center, Ms. Lenczowski was named manager of a staff-level office for the Systems Development Group. In 1988 she was named chief of the Aerospace Center department that produced the DMA's standard digital products, and in February 1989 she became chief of the data services department. She was reassigned to the Systems Center in July 1991, reporting to the Washington headquarters facility as chief of the warrior support division. From August 1992 until July 1995, she served as technical advisor for geographic information systems for the DMA and was then selected as DMA's director of acquisition and technology. She was assigned to the NIMA implementation team in December 1995, and when NIMA was activated in 1996 assumed the position of associate deputy director of operations. A year later she became the deputy director for operations, until she was selected for her current position in September 2001. Ms. Lenczowski holds a classical B.A. degree in philosophy from Creighton University, an M.A. in philosophy from St. Louis University, and an M.S. in geodetic science from Washington University.

Oettinger: I need not take much time to introduce our speaker today, Bobbi Lenczowski. I sent you an e-mail with her biography. We are delighted to welcome her once again, and so saying, I turn it over to you.

Lenczowski: I came last year and talked to the class,[1] also as a last-minute replacement for General Clapper. General Clapper did plan to give this presentation. In fact, he's incredibly disappointed that he is not here. He made the commitment, and we got it onto his calendar, but unfortunately, as is typical with his calendar, there are always intrusions. Originally he was supposed to be down on the Hill today giving his budget testimony before the Senate Select

---

[1]See Roberta E. Lenczowski, "The National Imagery and Mapping Agency," in *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 2002* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-02-1, March 2003), [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/lenczow\lenczow-i02-1.pdf

Committee on Intelligence. That got moved, but by that time I was already committed to coming here and was moving in this direction. Instead, this afternoon, while we're doing this, he is being grilled back in his own conference room by a group of seniors who are doing a murder board with him. I can guarantee you that he would rather be here.

I'm going to use his theme and walk through a group of slides that was put together for him with the message that he wanted to communicate. I understand this is a seminar environment, and I really do encourage you to ask questions as we go along. If something occurs to you and you want some clarification, or you've been working on a particular topic and that might be the opportune time, please interrupt. The nature of being here is to be able to share some of this information.

This is what we're going to talk about (**Figure 1**). We'll talk about NIMA, just so we can give you some context as to where we belong in the intelligence community. Then we're going to talk a bit about an intelligence issue, namely: how do we assure the integrity of intelligence? We'll only talk about that at a very high level; we won't go into great depth. Then we'll talk a little bit about organization in the intelligence community and some of the steps that are underway today.

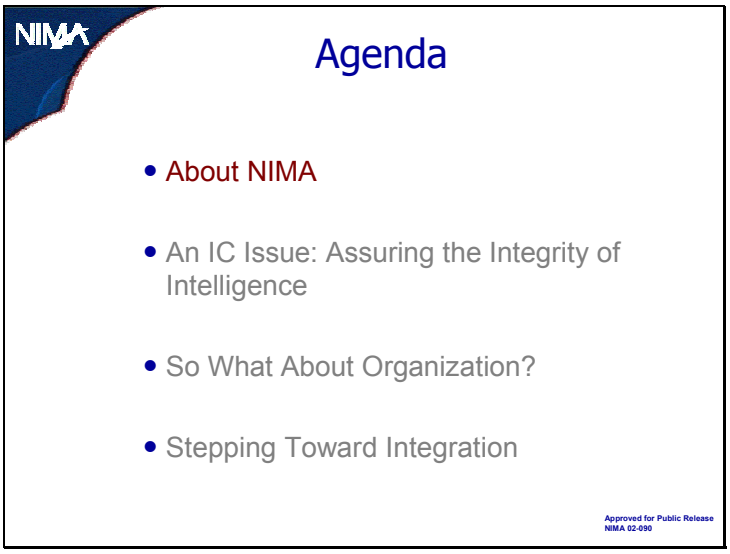


Figure 1

This is our standard NIMA slide that tries to capture visually and textually what we're about (**Figure 2**). If you were to have seen a comparable slide before General Clapper became the director, you would have seen a mission statement that looked very similar, saying that we were in the business of providing highly relevant and accurate geospatial information and imagery and imagery intelligence in support of national security. What General Clapper realized as he came on board as the director of the agency in September 2001 was that it was time that we as NIMA, the newest agency in the intelligence community, actually set about realizing what the proponents of this agency had in mind: the synergy of being able to incorporate imagery, imagery intelligence, and geospatial information into a product suite that we call geospatial intelligence. Geospatial intelligence is that exploitation, that analysis, of the imagery and our geospatial information so

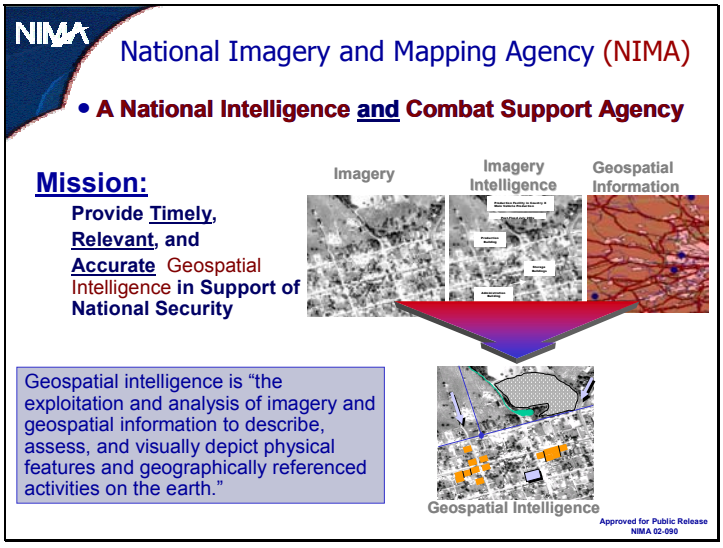


Figure 2

that we can describe, as well as assess and visually depict, things on the earth, or things that are happening on the earth.

Oettinger: Could you comment a bit on the title? What the class read for last week was Amy Zegart's *Flawed by Design*,[2] which makes the case that those two roles—being both a national intelligence agency and a combat support agency—have been historically incompatible, so that looks like a high ambition.

Lenczowski: We are not the only agency that is comparably described. The National Security Agency [NSA] is also both an intelligence agency and a combat support agency, which means, as the director of NIMA would be quick to point out, that he has two bosses. He reports both to the director of central intelligence [DCI], Mr. Tenet, and to the secretary of defense, Mr. Rumsfeld. As you pointed out, this is, and has been since the establishment of NIMA, something that is frequently seen as a stress area. There is always the concern that one or the other of those bosses will get dominant attention: so that somehow if we focus on the national need we will limit the support that is provided to the military, or if we focus on the military we will somehow disadvantage the national interest.

In the history of NIMA, particularly in its first four years, there were multiple studies done by a variety of committees that looked at the standup and the ongoing progress of NIMA against its objective state. This particular question, and this particular stress, were looked at multiple times to determine if NIMA was unduly influenced, giving support to the national at the sacrifice of the military, or vice versa. Not one of those studies or investigations was able to cite evidence of a time when one or the other aspect had been disadvantaged. Clearly, there is recognition that, under different sets of circumstances, one or the other may receive the priority focus and

[2]Amy B. Zegart, *Flawed by Design: The Evolution of the CIA, JCS, and NSC* (Stanford, Calif.: Stanford University Press, 1999).

consideration. We always remind folks that the old way—and it's old only as of a couple of weeks ago—of prioritizing intelligence issues, which is PDD [Presidential Decision Directive] 35, also identifies the priorities of the intelligence issues that one would address.[3] It starts with a Tier 0 (the most important) and works its way down the tiers. What would always move to Tier 0 as a national security priority would be giving support to military engagement in an on-going operation, which of course would also be the highest military requirement. So when we're in a crisis environment, the DCI's priorities and the secretary of defense's priorities would, in fact, be synthesized.

Under certain circumstances, this dual responsibility can be a stress. We find it very interesting that, from our perspective, our budget is also aligned that way. In terms of helping you to understand the funding of this part of the government, we are funded by both the National Foreign Intelligence Program and the Joint Military Intelligence Program. Our budget is divided and overseen by those two different entities that have oversight responsibilities.

This is a different way of describing geospatial intelligence (**Figure 3**). It's the "what," the "where," and it's also understanding the context. You want to know where you are, but you also want to know where the friendlies and the enemies are, and where the noncombatants are, so that you don't put them in harm's way or you avoid harm to the extent possible. How do you navigate? We blend a whole variety of data sources and data formats into this service that we call geospatial intelligence, and it gets identified as the foundation upon which other elements of the intelligence preparation of the battlefield can be incorporated. Once you have this base, you can add in military logistics if that is your issue, or you can add in weather if you're worried about navigation. There is a variety of things you can incorporate if you have built this base. It's about the past, the present, and being able to predict as you move to the future. But it is a basic foundation.

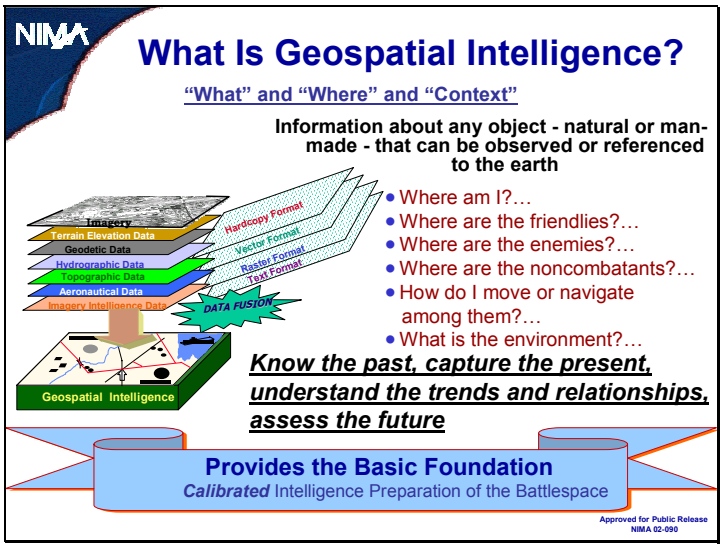


Figure 3

[3]Presidential Decision Directive 35, Intelligence Requirements (Washington, D.C.: The White House, 2 March 1995).

As we begin to do a better job of articulating what we mean by geospatial intelligence, we've just published something that we call the capstone concept (**Figure 4**).[4] The reason we care about that is that we have a responsibility to develop the doctrine that goes with this notion of geospatial intelligence. Many of you have heard about imagery intelligence—IMINT. That's our business. You've heard about HUMINT—human intelligence. That's not our business. It's incorporated into some of that information we create as a foundation, but it's not our business. You've heard about signals intelligence—SIGINT—but you've probably not heard about geospatial intelligence, and there are people out there who will create that comparable abbreviation and call this GEOINT. The reality is that we are trying to ensure that we have firmly established the understanding of what the doctrine is, because we are also responsible for training in geospatial intelligence: training internally to NIMA but also across the community on the intelligence and the military sides.

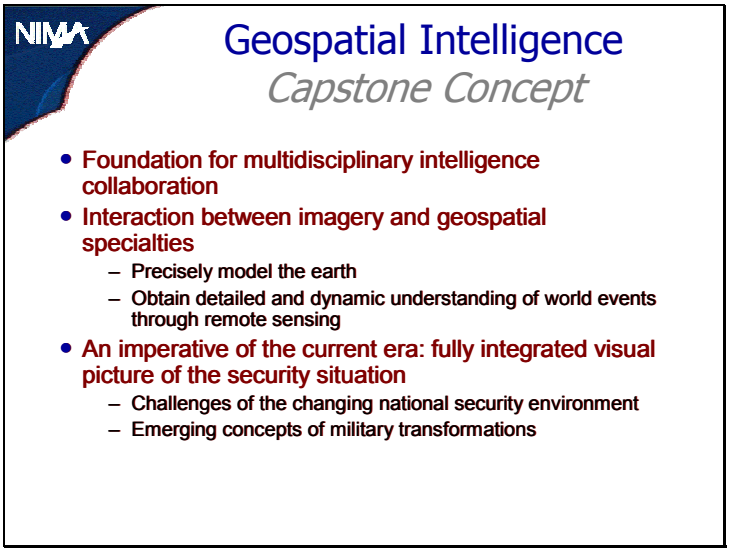


Figure 4

We look at geospatial intelligence as a foundation for our multidisciplinary intelligence collaboration. You're going to hear more about collaboration as I continue talking today, because, as we talk about intelligence organizations, their future has to rest on being able to accomplish this collaboration. It certainly has to do with us internally in terms of how we accomplish that interaction between the imagery and geospatial specialties.

I tell an anecdote about General Clapper before he actually took over his assignment as the director of NIMA. He spent several months in the latter part of the summer of 2001 learning about NIMA before he came over to take the job. In the first session that the officers who were working with me and I had with him, he commented that, just in terms of reading the various documents and his past experience with the DMA and the National Photographic Interpretation

[4]NIMA's *Capstone Concept for Geospatial Intelligence*, published in January 2003, is available on-line at URL http://www.nima.mil/ocrn/nima/panews.html or http://www.fas.org/irp/agency/nima/capstone.pdf

Center, he recognized a kind of tension that would naturally exist within the cultures that constituted NIMA: between the geospatial side of the house and the imagery intelligence side. The tension that he so astutely recognized was that on the geospatial side we have a group of people who by discipline, by work, are focused on being able to describe the earth precisely. Precise measurement and precise description are their business. Getting something accurately located and put into databases or placed on map sheets is their job. On the imagery intelligence side we have a group of people who have learned to deal with a world of ambiguity. They use imagery as a source, but frequently deal with information where, on the basis of what they acquire visually, they are giving probable or possible explanations of what they see. So you have this real contrast.

You also have a group of people on the geospatial side of the house who are very accustomed to spending disciplined hours, weeks, months, and perhaps years on creating earth-descriptive products, as opposed to being on the more time-dominant imagery intelligence side of the house. This is particularly true if you are in the business of indications and warning [I&W], which is very dynamic and deals in minutes and hours in terms of being prepared to provide good information to those who are waiting for it.

Then, of course, an imperative in the current era is to be able to provide fully integrated visual representations of a variety of security situations. Fusing sources of information is an intelligence challenge, certainly, created by the complex needs of the changing national security environment, and the visualization is clearly indicative of the concepts that are emerging with the various military service transformations.

This is among General Clapper's favorite slides (**Figure 5**). He acknowledges that he actually stole it from the DIA [Defense Intelligence Agency] when he was over there as director. He believes this does a wonderful job of explaining what has happened over the years in terms of

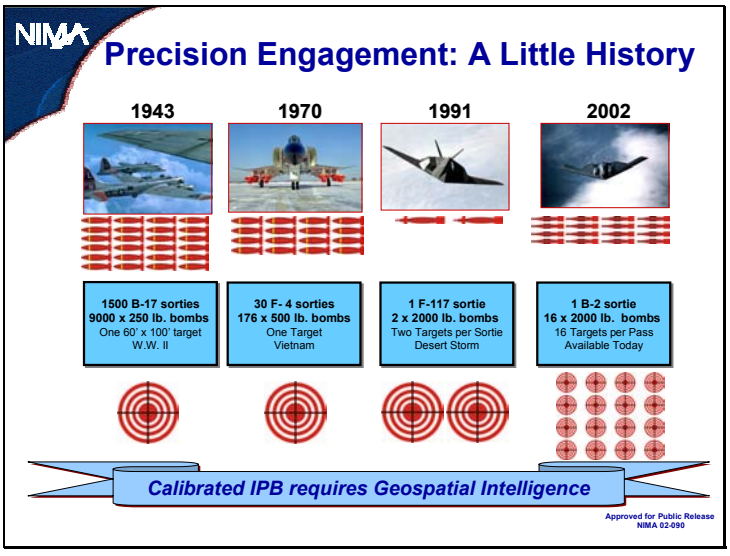


Figure 5

having a calibrated, integrated picture of the battlespace and the requirement for that calibrated, integrated picture. You move from an environment where you would deliver lots of not-particularly-accurate weaponry on a variety of targets, and collateral damage was expected and tolerated, to an environment where precision and accuracy are dominant. We deliver smaller bombs and we have environments where being lethal and maneuverable and stealthy are incredibly important characteristics. Over this period of time we have had responsibility, either as NIMA or as one of the legacy organizations, for providing the information that is used to support this kind of an environment, both from an intelligence standpoint (that is, identifying what the targets will be) and from a geopositioning standpoint (ensuring that you can deliver the weaponry on target very accurately.

We're going to come back to this slide a little later, because I did a little historic reading. One of the things that General Clapper likes to point out is that when you talk about NIMA and you examine the vision, which is "Know the earth and show the way," it's like in real estate: everything has to be somewhere (**Figure 6**). It's "location, location, and location." That's the business we are in. It's geospatial intelligence: it is talking about describable things and events, things happening, people who make those things happen, and *where* they are.

Figure 6

This is just a little bit of background (**Figure 7**). I told you that we were stood up fairly recently. We are now at the point where we have passed the five-plus year mark, but these are the elements that we incorporated to stand up NIMA in 1996. I look back at that time, its era of transition, and what we have gone through in terms of establishing this agency and refining its mission, and I recognize what a formidable challenge the new Department of Homeland Security [DHS] has.

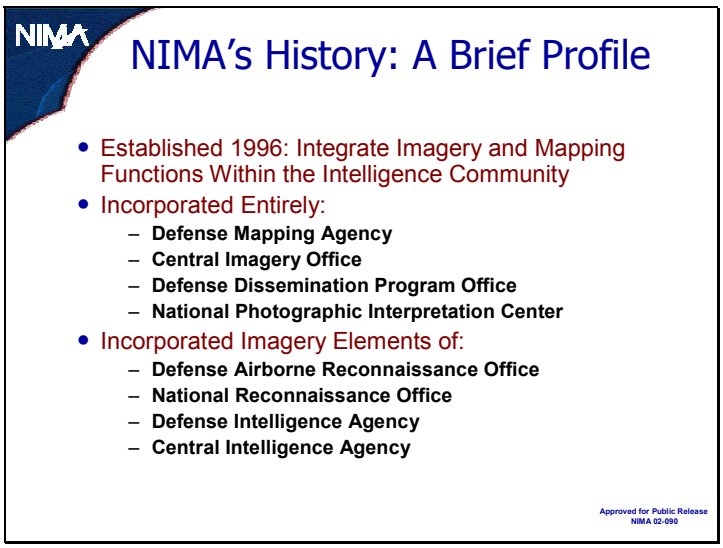


Figure 7

Oettinger: You've almost taken the question out of my mouth, which is: On the basis of your experience at NIMA, what would you advise the secretary of homeland security to make his top priority?

Lenczowski: The first thing to do is get your infrastructure well established. One of the things that created an incredible difficulty in standing up NIMA was the assumption by others that there was minimal need to worry about the fact that we communicated differently. When we pulled together all of these various elements, which were spread out not only in the Washington area but also globally, there were different infrastructures in place for each of the elements that came together. So there were pressing challenges for us just to communicate internally from one part of the organization to another.

There are significant and real challenges in how you deal with distinct legacy cultures, and how you answer the basic questions that those individuals who are now part of the new department have, like "Will I have to move? Is my boss going to change?" That anxiety happens throughout the organization, but if you haven't facilitated relieving it by having a solid infrastructure in place so that simple communication can take place, you're in trouble. We didn't even have a single telephone system to be able to communicate across or throughout the organization. Certainly you can pick up your Verizon telephone and call someone, but when you're dealing with elements of the intelligence community you are dealing with classified communications systems, and there are all kinds of firewalls and other protective environments that precluded a lot of basic discussions that needed to take place. So that's one of the very important things to understand: what the infrastructure is going to be.

About three months ago or so, I attended a conference at which one of the panel sessions included a group of individuals representing several of the component activities that have become the DHS. To focus the topical discussion, they were asked a similar question: "What do you think are the biggest challenges you're facing?" Repeatedly, I heard the response about the infrastructure. The first thing they wanted to do, for instance, was get everybody together on a

common e-mail system. Those things seem trivial, because you take them for granted in an environment where any one of us can get an e-mail account from an Internet provider and have open e-mail exchange. When you start to put together a large organization, it's erroneous to assume that e-mail connectivity is readily available. Some of those considerations can be critical factors in future success.

This is as close as you will find to any wiring diagram of NIMA (**Figure 8**). This is the way the director of NIMA wants to communicate the organizing principle that he saw was needed as he came to take over leadership of the overall organization. I told you that he had done his prep work by reading several of the reports of committees and commissions that had been tasked to take a look at this organization called NIMA. He realized that even the very best of them, even with the most sound of recommendations, missed recognizing the need for an organizing principle. His organizing principle is focused on what he calls his line organizations (shown in the center area of the graphic). This constitutes the bulk of the employee and resource distribution within NIMA, and these globes are also designed to represent their varying importance, as well as their relative size, within the organization.

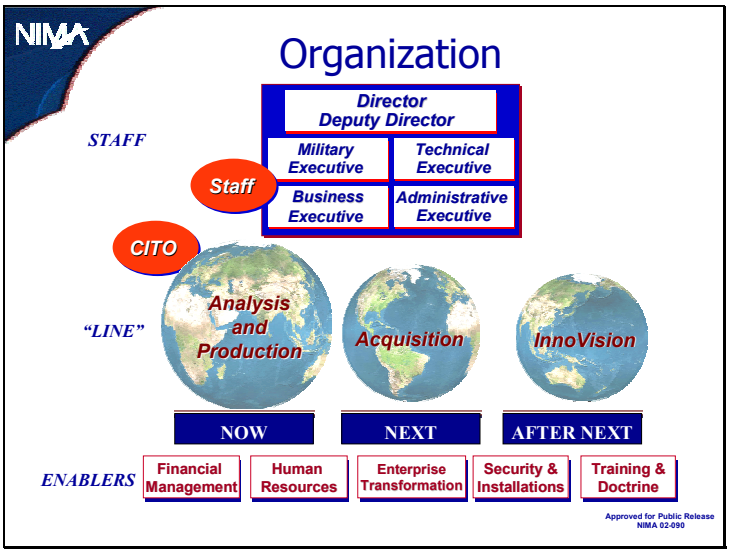


Figure 8

We exist because of our mission. Our mission is providing geospatial intelligence. Our "now" organization that does analysis and production is, in fact, the most important aspect of NIMA, and it has the majority of the agency's population. It is focused on what we do now. Our acquisition organization, the "next" part, if you will, is responsible for providing the systems, the tools, and the hardware that are used by the employees in the "now" part of the organization. They're busy buying things and creating concepts of operations for the systems that will be delivered. The third part of the organization, the "after next" or the "innovision," is discovering and examining the capabilities that we need to look toward, that will ensure our analysis and production activities can be accommodated by the tools and hardware to be purchased in the future.

This explains the temporal representation. I always like, however, to point out that "after next" can be as much about time in the future as it can be about the truly transformational "after next" ideas or ways of doing business. When you become intensely involved in forward-thinking discussions about transformation across the entire defense and intelligence communities, some of the things that will emerge from those penetrating discussions will be found or suggested by this "innovision" activity and can be incorporated directly into our "now" activities. Because they are the right thing to do and can be assimilated easily, time is not the characterizing distinction between the "now," the "next," and the "after next." There are other things that need to go through the acquisition cycle for purchase or building that distinguish the "next" from the "after next."

The boxes at the bottom of this organization chart are the essential wheels that keep the rest of the organization functioning. They are the enablers. The staff under the director is very lean. The other ellipse identified there, CITO, is our Central Imagery Tasking Office. That is the organization responsible for the ordering of national intelligence imagery that is used in our analysis and production, as well as by the community at large.

Oettinger: What distinction do you make between analysis and production? After all, the product is an analytical product, so you make a distinction that for some agencies wouldn't make sense.

Lenczowski: Perhaps in time, even in a NIMA organizational picture like this, one would worry less about production. "Production" is inherited terminology from the geospatial side of the house, where there is an actual line-production activity. We are still making maps and other standard products. Increasingly our traditional line production is done under contract. Source material is converted into information that is then built into something on some type of medium, and that is what you would typically call a product.

What a good lead-in! I actually brought examples of products for you. What we have here are three charts that we are making available for general distribution; I think they can actually now be ordered through the U.S. Geological Survey [USGS], which does public distribution for us.[5] There's a Middle East graphic here, there's an Iraq graphic, and there's a Baghdad graphic; additional graphics have also been added to our Web site and are available for purchase from USGS. These are products, something that is actually rendered on media and distributed. Each of these was extracted from a public-releasable subset of digitally "databased" but traditionally map-like information.

I would certainly also claim that an intelligence report is a product. In fact, we make and distribute multiple imagery intelligence products, all predominantly textual descriptions of what is extracted from imagery.

Analysis is the intellectual process exploiting the source material. Although we have not historically associated the term "analysis" with the exploitation process used to build the geospatial products, we have begun to describe our employees as either geospatial or imagery analysts. The outcome of their analytical service will populate databases, create annotations on a film base, and expand understanding about regions, issues, events, and people. Packaging for

[5]See URL: http://mac.usgs.gov/nimamaps/index.html

presentation renders the product. Even these map product examples, however, are not the result of a standard "production" process. Once a database is established, as a consequence of analytical exploitation of the source material, the elements of information can be assembled in multiple ways to build a wide array of products.

This next slide simply walks back through the definition of our "now," our "next," and our "after next" in terms of what the real focus is (**Figure 9**). The "now" has to do with what we do, how we satisfy our mission requirements; the "next" with how we look to investments for the future; and the "after next" with new methods and technologies.

Figure 9

Let's talk about the integrity of intelligence (**Figure 10**) and digress a bit on the resemblance of this chart to the "location" chart. Remember that I told you I was going to bring you back to this. I did this because I knew that, as General Clapper was preparing to come here today, he might get the opportunity to read the transcript of what he had said the last time he was here: back in 1996, when he was in the private sector.[6] At that time he had already retired from the military and had left his position at the DIA. In the middle of his earlier comments, he said, "If you don't have integrity, you've lost everything, because it's like real estate: location, location, location." The earlier chart about the business of geospatial intelligence [Fig. 6] is vintage General Clapper. Yesterday I asked him as we were talking about my visit here, "Sir, do you know that back in 1996 you said that 'in intelligence it's integrity, integrity, integrity'"?

[6]See James R. Clapper, Jr., "A Proposed Restructuring of the Intelligence Community," in Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 1996 (Cambridge, Mass.: Harvard University Program on Information Resources Policy, I-97-1, January 1997), [On-line]. URL: http://www.pirp.harvard.edu/pubs_pdf/clapper\clapper-i97-1.pdf

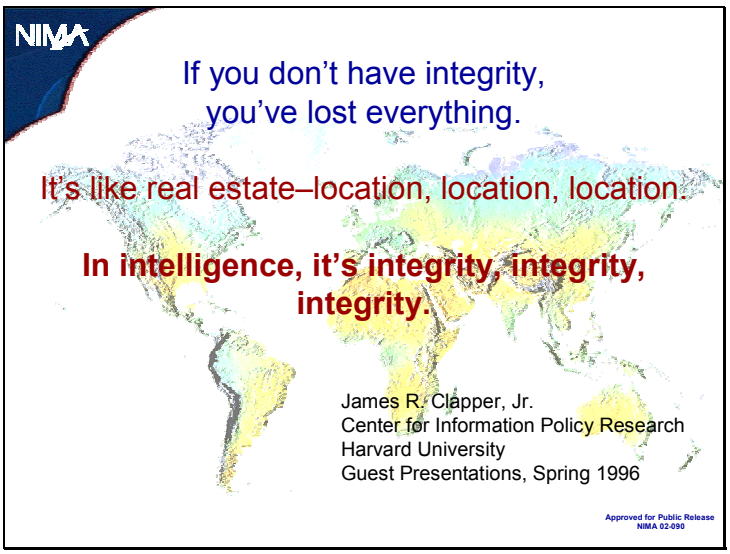


Figure 10

This anecdote gives me a nice lead in to where I wanted to take our discussion today as we talk about roles and responsibilities in the intelligence community at large. I've given you some background about how we contribute to that larger collaborative environment, but it's important that we see some of the other aspects, and that you have the opportunity to ask more questions about that fit.

I hope that the discussions you've had in the course have made most of you familiar with the concept of information assurance and what that means in terms of protecting data (**Figure 11**). The focus there tends to be on all of the security services that are associated with how you assure information. One of the things that General Clapper has been very interested in is taking that notion, which he clearly sees as one where the vested responsibility in the intelligence community resides in the roles of the NSA, and seeing how, then, our responsibility for geospatial intelligence links into that issue. If what fits in each of these environments are lots of bits of information (those zeros and ones, if you will, that populate databases) there is definitely an overlap with the way we carry the activity of the security services into our environment of geospatial assurance. Like any of the other agencies in the intelligence and the defense communities, we are in fact responsible for complying with the information assurance directives and guidance that are provided by the NSA: confidentiality, integrity, availability, and authentication. As I pointed out, when we stood up as an agency and brought together a variety of other entities and our connectivity systems, we all came with our own stovepiped ways of protecting information. That is the obvious reason that we didn't all suddenly come together, pick up the same classified phone environment, and talk to everyone across our agency. There were these kinds of protections to assure information at each level.

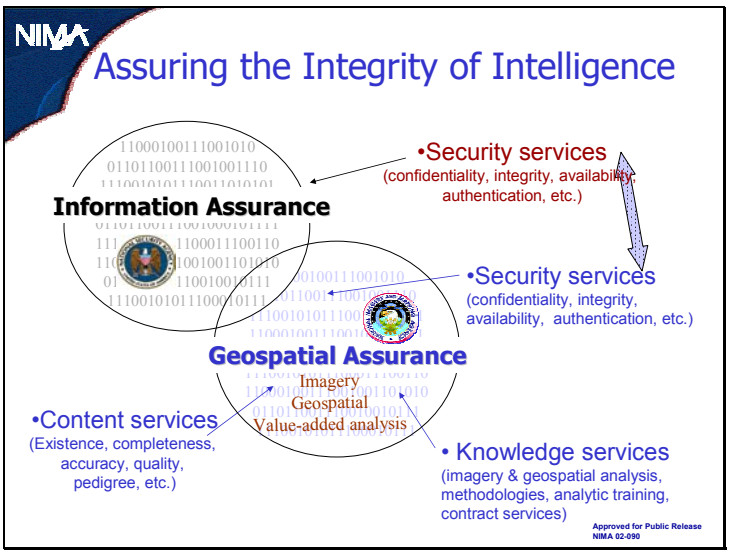


Figure 11

We have further responsibility when assuring geospatial intelligence. We are additionally responsible in the areas of content services and knowledge services. So from a geospatial intelligence perspective, we have to guarantee that the necessary information does exist (**Figure 12**). Our entire program on an annual basis is designed to look at what is needed. What are the priorities determined by the PDD 35 counterpart on the intelligence side in terms of the DCI's priorities to the operations plans from the DOD that describe what the military requires for geospatial intelligence? Not only must the information exist, but we must also ensure that we have put in place all the appropriate procedures and processes for accuracy, completeness, and currency.

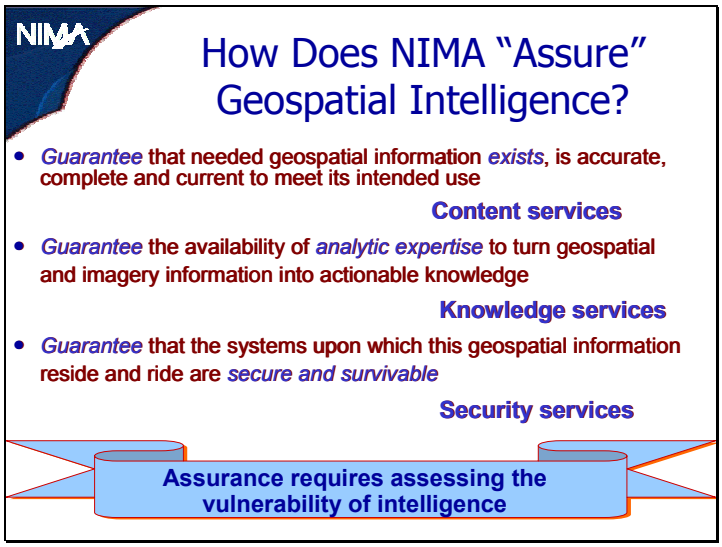


Figure 12

We also have to ensure that there are knowledge services that go along with these data or this information, and that we offer and provide the trusted analytical expertise. Certainly one of the things that we have learned over the years is that on the geospatial side, as we do our production, there is a great deal of information that we can acquire from the private sector. We have several contracts with the private sector for geospatial information production, specifically for data that are provided into our databases. We are increasingly dependent on "off-the-shelf" products that we call "commodity buys." We buy information that already exists in the public domain and incorporate it, as appropriate, into our databases. So, we can find information, just as we can build information, but when we find information we must also provide the knowledge services. It is absolutely critical to use our expertise to ensure that information that is defined as being accurate, that is reputedly complete, and that seems to be current can in fact be turned into information that can be used for planning, decision, and action. It takes a formidable amount of expertise and acquired skill, in terms of developing the tradecraft and the analytical capabilities, to provide this. Then, of course, the assurance that this information is secure and is survivable is crucial.

Student: How do you assure the accuracy of private sector information? Can you give some specific examples of private sector information?

Lenczowski: This turns out to be one of the great challenges of the information management age. Each of us has the ability to surf the Net and find information on nearly any particular topic we might be interested in. We are effectively held hostage, if you will, to the credibility of the source that provided that information. That's a challenge, regardless of the particular information domain you're working in: relying on someone else, not necessarily personally known, for the information.

Let me speak specifically to NIMA's information assurance issue, related to your question. On the geospatial side of the house, which is where we have been doing more and more of our commodity buys as well as our contracted geospatial production, if it's a commodity buy we look for what are called the metadata elements. They tell us what the source was, what the age—vintage or currency—is, and what the skills or expertise of that particular source are. That's not easy. In the area of geospatial information, there is not yet a cooperative domain that is completely populating the metadata. This reluctance or negligence in populating the geospatial metadata, however, does not simply apply to geospatial information. "Tagging" of all elements and aspects of intelligence information is also a growing expectation. There is a lot of work going on in the standards community on what will be considered the acceptable elements that must be populated in metadata to characterize information. But back to your question: there is still some uncertainty regarding the known quality of information that you may get from commodity buys.

Let's move, however, to the situation where we actually go out and contract for production. In that case, we have worked very closely with those contractors, and our internal experts have cooperated in developing techniques for their work processes and also for doing the quality assurance and the quality control. In that case, we have some bona fide processes that we can endorse and, because of the contractual relationships, we insist upon the quality control to verify whether or not the data are acceptable.

There is generally a higher risk when you're dealing with commodity data. Unless a conscientious producer has characterized the metadata during the commercial processes, you

work after the fact on validating the claims that are made about the information. If you use it, because it happens to be all that is available at times, you have to be able to state the appropriate reservations. You need to be able to tell where it can—and cannot—be used with any degree of reliability.

Student: Is a subset of this commodity data a result of shutter controls, where basically the U.S. government bought out imagery from SPOT Image and IKONOS during some military actions just to ensure that it wasn't also sold to anybody else?

Lenczowski: Although the sense of your question implies that buying commercial imagery describes the way we use the term "commodity data," it's an entirely different situation. The distinction is between a finished product and a source for building products. When we use the term "commodity data," we may be buying "value-added" output that has commercial imagery as its exploited source.

But let me talk about Operation Enduring Freedom and buying imagery to answer the implications of "shutter control." Space Imaging was the only U.S. company with commercial imagery on orbit at the time. Never has shutter control been invoked. Never. However, shutter control is part of U.S. government licensing conditions, applied through the Department of Commerce, with the U.S. commercial remote sensing industry. When the commercial imagery providers are licensed, they acknowledge that, as condition of license approval, the U.S. government may request that they restrict their commercial operations. That further gets incorporated into any contracts they might sign with international partners, because their international partners need to know that their contracts are constrained by that particular condition.

So, what's the story that you've read about Operation Enduring Freedom and Afghanistan and Pakistan? NIMA has contracts with all of the U.S. companies that provide high-resolution commercial imagery. One of the options in our contract was an option to buy all of the time on orbit over any place. Incidentally, that same provision is an option offered to others. During Operation Enduring Freedom, we entered into a contractual agreement with Space Imaging to buy all of the orbit time over Afghanistan and Pakistan for two months. The reason we did this was to ensure that we had full and complete access to all of that imagery collection so that we could acquire all of the imagery that would be needed during the operational period, without competition for that asset, as well as have it available should it be needed subsequently for reconstruction activities. What Space Imaging would be more than happy to point out is that if somebody else had come to them with a contract to buy all the time, they would have sat in negotiation with them.

For example, in the Middle East, over this particular geographic area we're talking about, Space Imaging has five international regional partners, all of whom have what is called a "cone of collection" area. That means they have a ground station in their area that has the ability to downlink directly imagery that is collected within that particular footprint. These are, incidentally, intersecting cones of interest. The way that's managed by Space Imaging is that the various international partners have bought time on orbit. For instance, the United Arab Emirates have bought X number of minutes, Turkey has bought Y number of minutes, and Saudi Arabia has bought Z number of minutes. Those are the contractual agreements in terms of selling time on orbit. What we—the U.S. government through NIMA—did during the Operation Enduring

Freedom period was buy all the time on orbit over those two particular countries (Afghanistan and Pakistan) for those couple of months. We ensured that we had all that un-competed access and the tasked imagery, which was subsequently put into the public archives for sale by Space Imaging.

Student: Does that mean that while you were getting it you had exclusive rights and none of those partners on the ground got it?

Lenczowski: At that particular time, only one other partner was operational, and except in one instance that partner was not interested in collecting in that same specific geographic area. There were different areas they were far more interested in that did not compete with our interests. That's what they collected, which was not a business conflict for Space Imaging. Nobody had to invoke any kind of shutter control to restrict the company.

Student: Will it become necessary to exercise shutter control when it gets too expensive? I understand that with the arrival of new companies, it may become too difficult to buy out all of their imagery. Is that an issue?

Lenczowski: The reality is that even that approach, during that period of time, could have been difficult had there been other regional partners. There were not at the time, and so we bought the access time and the imagery. In the future—and it's always difficult to predict what might happen—there is always that opportunity for the U.S. government to decide that it wants to invoke shutter control, but one would have to ask why we would want to. What would be the net benefit of doing shutter control? What would be the rationale?

I'm going to talk a bit more about this. This is pertinent both to the question and to my theme of information assurance. I brought a paper for each of you that was put together by RAND that talks about "The Age of Transparency."[7] The authors' assessment is that while overhead satellite imagery is certainly of great value and great interest, if you were using shutter control because you want to deny information to others, there are a variety of other information sources that are comparably revealing. There are various other, readily available ways to acquire information.

An example that's used in the paper has to do with actions in Kosovo. If you wanted to know the status of the various military support activities, it was easy to walk up to the fence of a military installation with your GPS receiver and your cell telephone, and you would have been able to communicate immediately what was leaving or coming in. It would be timely and positionally reliable! You'd be able to do that much faster than one of the commercial companies could collect an image. You need to understand that these companies typically revisit a particular spot every three days (and if we're talking about the U.S. companies they each only have one satellite). So they have to be there at the right time when you want the image taken. Second, they have a very poor distribution environment. On average, based upon historical data for each company, if you order an image from any one of these companies it can take you twenty-five days to get it.

---

[7]Kevin M. O'Connell et al., "American Security in an Age of Transparency" (Santa Monica, Calif.: The RAND Corporation, 17 April 2002).

So you have to ask yourself why you would exert shutter control, and what the conditions would have to be when you would invoke that. The spirit of shutter control is that you would do it for the shortest period of time over the smallest footprint possible. So you have to define very carefully where you want to focus, what you want to do, and whether you want to do shutter control or just want to restrict distribution. You may not want to turn the collectors off. We certainly didn't want to cease operation during Operation Enduring Freedom.

I told you that there were five different partners within the Middle East area of interest. Most of those are not commercial organizations. Most of them are either government or military partners, so they also have some vested interests in terms of not randomly selling imagery and of not losing collection access.

Student: It sounds to me as though commercial satellite imagery falling into enemy hands is not an issue.

Lenczowski: I don't think one ever says it's not an issue. It's as much an issue as recognizing that there are all kinds of methods for exchanging very important information. You need to understand what your operational security plan is for each of those elements.

Student: It sounds as though what you're saying is that the speculation at that time was that this was shutter control by checkbook; that there wasn't operational security thinking behind this. You're saying that's flat wrong. That's interesting.

Lenczowski: I'm saying that we had the opportunity to buy. We did buy. We needed the imagery. Certainly one of the consequences was that it restricted the flow of that imagery elsewhere. I can't even speculate whether anyone else would have wanted to buy it. I don't know. I know that we bought it.

Student: Denis Clift in his book[8] said that it was for shutter control that total purchase was made so that nobody else would get it, especially so that news organizations wouldn't get it.

Lenczowski: Again, you have to see that as certainly being an effect. I don't think you can dissociate the effect from what was done. The rationale was to buy it for exclusive use so that it could be used by the ongoing military operation without competition for the valued asset. And to restrict access of collection to our military and the coalition ensured the U.S. government had imagery when needed so it could be used across the full breadth of the military activity.

Student: From talking to a few people in the industry a few months ago, my understanding was that far from people being worried about shutter control, they were actually very grateful for the huge infusion of cash at the time. The industry was very much in its infancy. Everybody had lost a satellite, and suddenly they had this huge exclusive contract, with guaranteed income for a certain period of time. So, from the industry point of view, rather than people getting very upset about the First Amendment, shutter control, and that this was going to restrict information, people were saying thank you.

Lenczowski: Again, when you're talking about the effects, from an industry perspective—and, again, there was only one company at the time; DigitalGlobe was not yet on orbit—it certainly

---

[8]A. Denis Clift, *Clift Notes—Intelligence and the Nation's Security* (Washington D.C.: Joint Military Intelligence College, 2nd edition, August 2002).

improved Space Imaging's business. There were more purchases than they would have expected had there not been that particular crisis.

Student: Were any restrictions put on SPOT Image?

Lenczowski: There were no restrictions put on SPOT by us. Remember that the SPOT model is not the DigitalGlobe or Space Imaging model. SPOT certainly has a commercial activity, but it is a government-subsidized activity. The government of France did impose some limitations on the sales of the SPOT imaging.

Student: That was not done at the request of the government of the United States?

Lenczowski: The United States did not request that be done. It was done voluntarily by SPOT.

Student: It also makes me wonder, as I think about the maturity of the commercial imagery industry. Had they had the option to provide archived images of Afghanistan, whether they were a week old or a year old, for whatever purpose, it might have served a lot of other people's requests. Then our limitation on distribution would have been more focused on operational security issues, because while the image probably hadn't changed in the last week, where U.S. forces are located does change. So there's probably some compromise that we would figure out in the future.

Lenczowski: Again, we get back to the spirit behind shutter control as an option that the government can exercise: the shortest period of time, and the smallest possible footprint, so that you're not inhibiting the rest of the commercial activity.

Student: Doesn't that create a perverse incentive for companies that own these satellites to hang out over places of which the U.S. government might not want images distributed and get these big, fat contracts?

Lenczowski: They don't have dwell capability. They're in orbits that are controlled by the laws of physics, so every three days they come back over the same place. These companies in fact do what is called speculative collection. For example, if they have available time that they have not already sold (as in Space Imaging's case, where they have regional partners) they are free to do speculative collection and put that into their archives and have it available. You can go to Space Imaging or DigitalGlobe's homepages on the Web,[9] and if you know the geographics of the region of interest, you can find out what imagery exists in their archives and what its age is. You can even take a look at thumbnails of the images in the archives.

Student: This discussion revolves around the use of overhead imagery for strategic intelligence versus tactical intelligence. The last time I had to deal with overhead imagery was in 1996, and at that time it was strictly for strategic purposes. It was good for buildings and things that didn't move, but pretty much useless for tactical intelligence. Nowadays we have these Tom Clancy movies where they show infrared guys doing attacks in real time. I don't think that stuff exists. You said it takes twenty-five days for the commercial stuff to get to you?

Lenczowski: On average, the reports about Space Imaging are that it takes twenty to twenty-five days to get an order satisfied.

---

[9]See http://www.spaceimaging.com and http://www.digitalglobe.com

Student: So we're still at a point where overhead imagery is more for strategic intelligence.

Lenczowski: In terms of the current commercial capabilities, yes. I do want to qualify that in terms of "current," because the commercial companies are certainly thinking about their next generation or iteration of satellites, and whether or not there's a business case to add more satellites to their constellations.

Student: I don't think we'll ever get to the point where we have real-time overhead imagery downloaded, as the Predator seems to do.

Lenczowski: Actually, that's a really good point. The reality is that even with the commercial capabilities, you could do what I would call "theater downlink." The Air Force has a system called Eagle Vision, which has the capability to downlink in real time. At present they are still working with DigitalGlobe and Space Imaging to put that capability on their systems, but today they can downlink Landsat, SPOT, and Radarsat. You can do theater downlink, so it's real time from that perspective, but again the real time still means that the satellite has to be in orbit at the place and time you need it.

Student: Do you have computers that can do the processing fast enough?

Lenczowski: Yes, the processing to convert the signal into an image does exist, absolutely. In each of these ground stations that are located around the world there are increasing environments where, if the collector is going overhead at that point and you can downlink it, you've got it in real time. I only talked about the five ground stations in the Middle East, but Space Imaging has several other regional partners. They just opened a ground station in Thailand, and they have two in the Japan and Korea area. So technically that's not a limitation.

Student: Can we shift the conversation a bit? We've been talking a lot about spaceborne platforms. Does NIMA exploit imagery taken from air-breathing platforms as well, or is that only done in theater?

Lenczowski: No. I want to define terms here. You say "air-breathing." For instance, we give support to some of the homeland security organizations in the United States, and much of the imagery that is used over the United States for geospatial purposes is in fact airborne. It has higher resolution, it's faster to collect, and it doesn't have licensing restrictions. There are a lot of reasons to prefer airborne imagery to satellite imagery in the United States.

Student: Is that electro-optical only, or is it multispectral and hyperspectral as well?

Lenczowski: For the most part, it is electro-optical, as opposed to multispectral, because most of what is being used for the mapping activities or for creating the ortho photos over the various cities and states is done in the panchromatic range. We have also acquired some LIDAR [laser detection and ranging] imaging to build elevation models or vertical profiles, particularly of urban areas. But we also do some of our imagery intelligence using some of the other tactical airborne assets.

Student: I assume that would be supporting I&W.

Lenczowski: Typically not I&W, because again you have a time dependency there in terms of how valuable it would be. Much of that tactical intelligence gathering is done in the tactical arena and is exploited in theater to be timely.

Now, back to the relevance of the question that was asked earlier about the potential for shutter control or what we referred to as "assured access" during Operation Enduring Freedom. You get deeper into this discussion when you're talking about the vulnerability of the information that you have in a variety of arenas—not exclusively commercial imagery—and what you do about restricting the access (**Figure 13**). Do you restrict the content? Is it all available, is some of it available, or is none of it available? Do you restrict the accuracy? Do you release accuracy information that tells the user how the producer generally complies with specified values (in other words, what's the minimum acceptable?), or do you take it to the level of insight where you release the actual accuracies? There are ranges of accuracy.

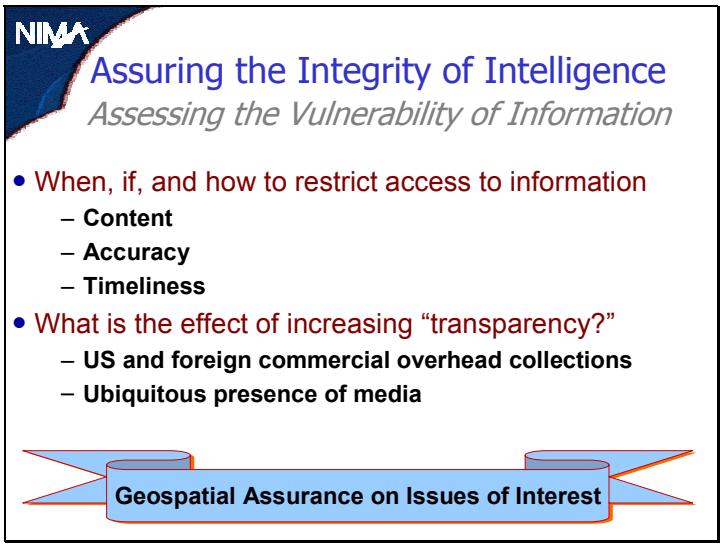


Figure 13

For instance, a map sheet traditionally has an accuracy associated with it, based upon its scale, to which national standards of accuracy are applied. The reality is that the information in the database that sits behind what's put on the map sheet may have accuracy and completeness components for particular elements of information that far exceed the information that's actually printed or needed on the map sheet. If you are in a digital environment you can determine how much of that information is essential for the particular use and release only certain elements to a specific group of users. As an example, the map sheets I have here represent only a fraction of all the information about these locations, but this information and the scale of presentation are publicly releasable so that everyone using the sheets has a common frame of reference, which reduces a certain level of ambiguity. More detail, however, is distribution limited, but it provides higher fidelity to military operations to further reduce the ambiguity when creating the common picture of the battlefield.

Timeliness of delivery is another factor that makes information more or less vulnerable. Sometimes the way you restrict access to information is that you simply delay making it available.

For instance, going back to the commercial imagery story, DigitalGlobe's resolution on its imagery is six-tenths of a meter. That's very high resolution. Under the way the Department of Commerce licenses the industry, anything that has a better resolution than approximately eight-tenths of a meter or more, because that's the capability of Space Imaging, has a twenty-four-hour delay in distribution. Part of that licensing constraint was to address this sensitivity to the potential that you would be able to provide information about a tactical operation in real time at a very high resolution, so that is incorporated into the overall licensing. As we move into the new policy for remote sensing that will be issued shortly, we see that there is an opportunity to consider how licensing might be tiered: a certain resolution is commercially available and better resolutions have some kinds of restrictions, whether they're time-delay restrictions or restrictions on the community of customers.

Student: This doesn't relate as much to the commercial aspect, but to the accuracy. You're talking about digital mapping, and I was wondering how accurate that really was. If it is very accurate, could you discuss some of the operational military aspects? Could it be used for targeting, GPS, or other such interfaces, and could you maybe discuss the road you're going down with that?

Lenczowski: Let me distinguish between the concepts of digital mapping meaning geographic information resident in a database and digital mapping meaning the processes by which that database content is rendered into a paper map. When you put information on a map sheet—a piece of paper—you have to displace some of the information because of the nature of the medium. (One seldom works with a one-for-one full-scale representation.) There's only so much resolution—only so many features—that you can convey on particular scales of maps. Even with a down-select of the features used, not every feature may be equally accurately positioned, although their relative relationship may be truly representative. As an example, if you had a road and a railroad and a stream or river that were all adjacent—and that happens frequently (as you travel across the country, just look to see how frequently those modes of transportation are very close together)—there is a hierarchy of determining what is positioned most accurately and, then, what is displaced accordingly. That convention has matured in the history of map accuracy specifications in terms of how to proceed, because you are limited by the medium of presentation.

When you move into the realm of databases, and use good, solid, stereoscopic, photogrammetric methods to exploit imagery with all its inherent geometric information, you can derive very accurate geospatial information that you populate into the database, and you can populate it as what we call "center line." Whatever the center line of the road actually is in terms of its latitude, longitude, and vertical height can be put into the database, and the exploiter of the stereoscopic imagery can do that for multiple points along that road. If the railroad tracks and the river are immediately adjacent, you can do the same thing for each line of transportation or communication.

In the database, you are not constrained by portrayal, so if you're pulling and using information from the database it can carry a high degree of accuracy. That is an additional reason the metadata are so important as we look to the standards for geospatial data and databases. Those metadata tags are important down to the feature and the attribute levels. That's accuracy information to a level of fidelity that's not important to the map sheet. The map sheet typically has an accuracy designation that applies to the entire sheet. Generally the accuracy definition reads: "90 percent of the well-identified features on this sheet are within X feet of their actual location."

In a database, every element and even the attributes of elements will need descriptive information about them in terms of accuracy, timeliness, and completeness.

Oettinger: I may be anticipating your next bullet, but what you describe as accuracy strikes me as precision, which may or may not be accurate. You made no mention of denial or deception. It may be very accurately portraying something that is meant as a spoof, so that would seem to be an important distinction.

Lenczowski: That's an important point. There is certainly a difference between precise information and accurate information. Take a bull's-eye. If my targeting shows that I consistently hit the same spot in the outer ring I'm being very precise but not very accurate. Being both accurate and precise would mean consistently hitting the center of the bull's-eye. So, when I use "accuracy," I am talking about the center of the bull's-eye and the envelope of confidence or range of error that the geographic coordinates provided, or even perhaps the descriptive information, fall within. I am talking about ensuring that I can support your using information for accurate targeting.

The issue that Dr. Oettinger was raising has to do with ways that intelligence information can be presented so that it seems to have all the right consistency—so it's got a lot of precision associated with it—but it isn't really accurate. There's a certain amount of intentional deception associated with it. That disinformation or misinformation is a different part of the spectrum of discussion as we look at the problem set. Here, we've been primarily focusing on our accountability and responsibility to ensure that what we put in our databases and what we distribute is accurate and reliable. As guardians of a public trust, we certainly worry that information gathered is consistent with other available information in which we have identified levels of confidence. We must also worry that it might have a certain amount of deniability or duplicity associated with it. That's always a threat, particularly when you get information from other sources, as in the commodity buys that we referenced earlier. How do you know that you are not being duped by information that seems very good but is not, because someone has intentionally set out to deceive you? Intentionally altered data either to deceive a user or to deny access to correct or complete information can be a pernicious attack on our databases. Such data might also be used for special operations. Those are two different aspects of the problem set associated with robust information assurance or information management.

So we again return to the earlier question about what's in the database. By supporting the intended use of the geospatial intelligence by a particular user, we, the producers, can also introduce error into the delivered product that does not endanger decisions or operations.

Let's return to an earlier comment. The database can be very accurate, but the problem is that once you decide you're going to visualize and portray something, whether it's on paper or on a screen, you must make some judgments about intentional displacement unless you happen to be building a one-to-one scale product. On the other hand, today's digital technology allows you the advantage of visualization and hot-linking to the database. If you can build the view on your computer screen, and then use the tools that are available to you in the computer electronic environment, you can link your visual presentation directly back to the underlying database and its descriptive and accuracy components. For instance, if a particular graphic of the Middle East had a very rigorous database sitting behind it and you decided you wanted to know what the coordinates were of a particular airfield, you wouldn't scale them off the charts or even the

physical screen to do the targeting. (Despite the inherent danger in such a practice, I'm not going to tell you that's not done by some inadequately trained users.) You would load the graphic to your computer screen, position your cursor on the object of interest, and use the information that links the screen position back into the database. That database holds the content that describes the object of apparent interest and can also identify to you what the actual coordinates are and provide the estimate of error associated with those coordinates.

Student: So then, basically, you could do that with computers and the other mechanisms. For example, if there were a building in Baghdad and you said "I want that out," rather than going through everything else you could use those mechanisms, get the GPS coordinates (because I'm sure the databases are all by lat-longs and very precise), and plug that into a GPS-guided bomb. Theoretically, you wouldn't even have to do the visual piece of the map.

Lenczowski: Yes, except insofar as you use the visual to allow you to pick the building, for instance, or to visualize it in its environmental context. If you're only dealing with bits and bytes that happen to be sitting in a database, you have no way to create that interface. The human interface in this case is your image or your map sheet. What you want to be able to do is have the strength of the very robust database of information that sits behind it, which gives you the information you need in terms of those absolute coordinates.

Now, do not assume that data always and everywhere exists. Populating the databases with those degrees of reliability is very difficult, very costly work. That is why we talk about building and providing the metadata. When you do go into the database and you pull out the information, you know the error envelope that surrounds it. You know what uncertainty also gets incorporated into the database.

Student: Could the human interface in fact be a nonpictorial representation, such as raw coordinates that were picked up from a human source? It would not then be necessary to print or display it on a map.

Lenczowski: The information that you have initially may in fact come from HUMINT. It could be an intelligence report that doesn't have anything visual associated with it, but was derived from a reliable source. Now you get back to the previous point about how you authenticate the sources, so you're back to the problem that Dr. Oettinger pointed to in terms of the reliability of the information you're being provided.

Student: This question is interesting, because he's assuming there's a universal coordinate system. Traditionally there are lots of local coordinate systems, and when you move to a GPS realm you need to know about the offsets. How is the GPS moving us from local coordinate systems to a unified coordinate system, and how does that affect your work? The earth is moving, too.

Lenczowski: The GPS provides coordinates that are referenced to something called the World Geodetic System [WGS] 84. In everything that NIMA produces, in all the information in our databases, we use WGS 84 as our reference environment. However, we receive sources that are registered to local data, so there are those offsets that you talked about. There are mathematical parameters used to transform from one of the local data systems to WGS 84, which is designed to be as globally compatible as possible—a "best fit" global model.

You talked about the earth moving, and actually there are various aspects of that beyond simple diurnal or annual rotations, so WGS 84 is looked at periodically to determine if there is an improved geodetic model of the earth that should be used to ensure the highest possible accuracy. The difficulty is that data are a very complex subject, and most people haven't a clue what "datum" means. They could pick up a chart, and it may say something about what the reference ellipsoid is or what datum was used, and yet the only things that many people notice is that the chart or map has coordinates and those coordinates look like something that's reasonable. In general coordinates of latitude and longitude establish a familiarity with the kind of information that map users always associate with a map sheet. There is no reason to assume that casual or infrequent users would understand that there are different reference systems for geographic coordinates.

So there are occasions when people will use a map sheet that comes from a source other than NIMA—as an example, the Russian sources that we used to help populate our database over Afghanistan. Those users could take one of those map sheets and not realize they were not in the WGS 84 reference environment. They could then derive coordinates that are accurate in that context, but not within the reference system that is used by other coalition partners. Apparently identical coordinates from two map sheets over the same area might identify two different objects. Consider the potential danger of friendly fire. For instance, in the particular situation using the Afghanistan maps, as in other cases where we did distribute the Russian base charts, we overprinted a WGS 84 grid on that chart source so that it could be used quickly but consistently with other WGS 84 sources, such as GPS receiver readings.

Student: Going back to the question, it's still much more accurate to have a person on the ground shooting a laser at a target that's being fed into a GPS bomb than it is to go into any database that might exist. Would you agree with that?

Lenczowski: Yes. Given a particular set of circumstances where you have that kind of overall capability, where you are able to create the full environment of all those necessary elements, you will be able to get very accurate positioning. You must still know where you are, where the target is, and where the weapon is within a time-sensitive three-dimensional coordinate system. All that information must be within a defined system. The reality is that you're frequently not in that kind of environment, and so what you're doing is looking for the best information you have to be able to put ordnance on the target.

Student: That would be useful for blowing up buildings, for instance, as opposed to keeping troops in contact with other troops. There's too much margin of error in your content that you don't want to live with.

Lenczowski: It's useful for sending a B-2 from Whiteman Air Force Base to Belgrade or its destination around the world.

Student: When the Northern Alliance is in contact with the Taliban, and you're sending a B-2 to blow up the Taliban, that's a tactical military audience.

Student: Or you're blowing up the Chinese embassy!

Student: That's a whole other story. That building was identified wrong.

Lenczowski: That was a B-2, and it did a very accurate targeting job, but the information in the database was not reliable. Now we're back to the reliability and the integrity of the information that happened to be in the database.

Oettinger: You might want to ask that question of General Hughes.[10]

Student: Maybe you can, sir. I'm not sure I want to.

Student: I read a quotation that said that smart bombs are not smart, they're just very, very obedient.

Student: Those are Air Force folks. If you talk to somebody else they'd have a different take on it.

Lenczowski: Now we get to transparency (**Figure 14**). We talked about many of these things as the questions have flowed, which are very good. This is a very interesting topic that has a lot of controversy surrounding it. The paper from RAND is an easy read,[11] so those of you who are interested in the issues of information assurance, information denial, and information protection, as well as denial and deception, will find some of the comments in that paper very provocative. In effect, this particular discussion says that it's the nature of the free market system and of advancing technology that gives us this transparency. There's ubiquitous communication, so it doesn't make any difference if it's a satellite going overhead taking a picture or if it's a person standing outside the Air Force base with a cell telephone and a GPS receiver. We can turn off that satellite, because we have mechanisms to control that industry. Are we going to turn off all cell phones? That's the kind of question that the paper asks.

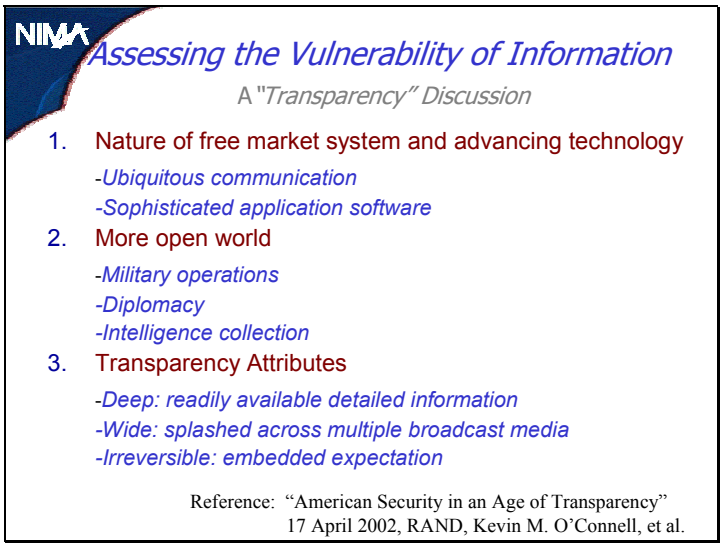


Figure 14

[10]Lt. Gen. Patrick M. Hughes, USA (ret.), who headed the Defense Intelligence Agency from 1996 to 1999, spoke at the seminar on March 20, 2003.

[11]See note 4.

There's lots of sophisticated software out there that doesn't require you to visualize what may be going on. You can take information from databases and let computers and their applications work to help you with the analytical job of determining the consequences of the information. It's a very open world with respect to our military operations, our diplomatic activities, and the intelligence collection that takes place. CNN [Cable News Network] is there before we are, so information about who's operating what and why is rapidly disseminated across the media.

The third item is the focus of the paper. It says, first of all, that we must look at transparency. We've got to pay attention to the fact that transparency is deep, because of the technology that individuals have available to them. It's wide, because it goes everywhere. It's irreversible, because there is an expectation that we have a right to have access to the technology and to the information.

Let's talk a little bit about organization (**Figure 15**). If you look at the organization of the intelligence community, you have to recognize that much of its structure is a legacy of the cold war paradigm. We're looking at major nation-states as being a threat; lots of firewalls, particularly between foreign and domestic intelligence; and all the restrictions on the national intelligence community with regard to things that happen in the United States and things that happen involving U.S. citizens. There are restrictions on how the assets that belong to the intelligence community for use against foreign threats can be employed as we look at domestic threats. As a result, stovepipe restrictions have grown up in this community in terms of agencies' lanes in the road and what one intelligence discipline does versus what another does versus what a third or fourth or even fifth discipline might do. That legacy has discouraged much collaboration and coalition building.

Figure 15

When NIMA was being discussed as an organization to be established, one of the first steps was to break down some of the stovepipes. From his vantage point as DCI, John Deutch looked at

what was happening on the imagery intelligence side and realized that what they used as a source was the same source that was being used on the geospatial side to build maps and charts and to populate digital databases. From his perspective, we had two stovepipes that could create a great deal of synergy if they were brought together, because they were using the same source. They were using it from different vantage points, and to create different suites of products, and what he saw was the opportunity to put the analysts on the intelligence side together with the analysts on the geospatial side and to improve the analytical capability of the community.

At the same time as that discussion was taking place, there was also work going on in the House Permanent Select Committee on Intelligence, which was looking at an organizing concept named IC21.[12] It was a concept for creating more collaboration and more coalition activity within the intelligence effort. It tried to look at a different model than the stovepipes that existed with IMINT and HUMINT and SIGINT, and to build a construct that would allow integrated work across those particular entities with an entirely different structure in the community. Since that time there have been other commissions that have also taken a look at this and have made recommendations, including the Scowcroft Commission in 2001, which also issued its observations, findings, and recommendations for better ways of organizing the intelligence community.

The reality is that 9/11 forced us to look at some of the issues very differently (**Figure 16**). The enemy was not outside our boundaries; the enemy had taken serious and dramatic action within the boundaries of the United States. If you look at what has evolved, you still have to ask the question "What is an effective organizing principle?" We now have the DHS, which has a responsibility for addressing the domestic threat of terrorism. In the new department there is an under secretary who is going to be responsible for information and infrastructure, and that role and its attendant responsibilities are not clearly defined. We have just been through the confirmation hearings for Dr. Steve Cambone as the under secretary for intelligence on the Defense side. So now, as opposed to an individual sitting in the DOD who is responsible for command, control, communications, and intelligence—currently Mr. Stenbit[13]—we have separated the command, control, and communications from the intelligence activity. Then, of course, we have the traditional roles of the DCI, who is dual-hatted as the director of the Central Intelligence Agency [CIA] and the leader of the intelligence community. We also have NIMA and NSA situated prominently here in the middle to represent this broad intelligence activity from the perspective of what the component parts are, what the responsibilities of the existing agencies are for certain activities, and how the intelligence activity gets organized.

As I said, there are various provocative discussions underway. There are very important and very fertile areas for resolving how the work gets coordinated and who is responsible for the full coordination across this activity. One of the recommendations—and only one among several—that has come out has been to create, in effect, an individual responsible for all of the intelligence activities without a specific agency role, so that the community wouldn't be sitting here with a DCI who is both the director of the CIA and responsible for all of intelligence. In the meantime,

---

[12] *IC21: The Intelligence Community in the 21st Century*, Staff Study by the Permanent Select Committee on Intelligence, U.S. House of Representatives, 104th Congress (Washington, D.C.: U.S. Government Printing Office, June 1996), [On-line]. URL: http://www.access.gpo.gov/congress/house/intel/ic21/ic21_toc.html

[13] John P. Stenbit spoke at the seminar on March 13, 2003.

we now have two new key players at the department level at DHS and DOD. So this chart characterizes the very real challenge of how we can work cooperatively and collaboratively.

Figure 16

Oettinger: Would you agree that it's a fair statement that this chart, busy as it is, understates the problem? There's no mention of state and local entities.

Lenczowski: That's right, and the people around this room know that there are any number of intelligence activities that I didn't capture on this particular chart. These are the big players. This is what General Clapper likes to refer to as "looking at the elephants in our living room." He even has a graphic where you've got the elephants of DOD and the new DHS sitting in the living room with these three agencies in the middle that have the responsibility for providing good intelligence support. As Dr. Oettinger pointed out, this chart doesn't cover the entire spectrum of the intelligence activities that are actually involved in the entire picture. How you establish an effective organization and enable the collaboration is a formidable issue.

It is to General Clapper's great credit that he had been thinking about this problem for a very long time. When he came to NIMA, one of his focus topics was on building stronger collaborative relationships with our sister agencies. So, for instance, we have formed a cell of NIMA individuals who sit in the NSA footprint to ensure that collaborative work goes on between the SIGINT and the IMINT, and there is appropriate cueing of information. What one may see or hear may be important to the other discipline in terms of being able to leverage that information in the most productive way. We are providing a similar activity in the Defense HUMINT effort that belongs to DIA, so we continue to look for opportunities where we, under General Clapper's leadership, start to work out venues of collaboration and cooperation.

Let's talk a little about some of the small steps (**Figure 17**). Those of you who listened to the president's address know that he chartered a Terrorist Threat Integration Center [TTIC]. He announced it and instructed that it be assigned to the DCI, but the director of the FBI, the attorney general, the secretary of the new DHS, and the secretary of defense would all be assigned to work

this particular activity. Winston Wylie, who is in charge of the effort focused on homeland security over at CIA, has taken the lead in forming a working group that has laid out some of the fundamental initial mission statements for this activity. The group reports to the DCI. It is intended to optimize the use of information and expertise across the community of intelligence activities, to give appropriate guiding information to the various collection strategies of the various INTs, and to maintain an up-to-date database. The database theme continues. The information management and information assurance themes continue to permeate the solution to the challenges that we have.

Figure 17

We will continue to see this TTIC activity grow. There have been statements in the past week from the DHS to the effect that the department does not intend to have a separate intelligence effort. DHS intends to depend on what will come out of this TTIC as a source of intelligence information.

Now let me go back to an earlier point I made about the roles, responsibilities, and restrictions on the national intelligence community regarding domestic issues. There are some real internal issues and challenges in connection with authorities and legal rights that must be confronted and examined, and these issues have not been resolved. These are issues that are in open and intense discussion.

Student: I'm curious about the database that TTIC is developing. It seems that it would be a huge asset for them. Who will own that database and how will access to it be allocated? How will that work?

Lenczowski: That again turns out to be one of the great current challenges under way in terms of who populates the databases, what the restrictions are on access to the information that is put into the databases, and who will have the appropriate clearances to be able to access the databases. There is a whole history of the culture of restrictions. What I'm telling you is that this effort is in

its formative stages right now. Winston Wylie has a very formidable responsibility here in terms of trying to pull this activity together.

In the next slide, I address one piece of the databases (**Figure 18**). There is an effort under way that's called ICSIS [Intelligence Community System for Information Sharing]. It is one of the attempts being made (it actually predates the establishment of the TTIC) to grapple with some of the issues. It is intended to be Web based and to use JWICS [Joint Worldwide Intelligence Communications System], which is at the TOP SECRET level, and SIPRNET [Secure Internet Protocol Router Network], which is at the SECRET level. It also addresses the difficulty with the earlier effort that was intended to give us that kind of environment, namely Intelink. As users know, it's incredibly hard to find out what you have or don't have there. It was a wonderful initiative to put in place an Internet-like capability on the intelligence side, but it has no real discipline. So the ICSIS is a mechanism to ensure that the capability is Web based, put in browser front ends and create the trusted interfaces, make sure we have the metadata markup for data discovery (so a lot of work is going on with XML [eXtensible Markup Language] and the standards for XML and databases), and then look at virtual collaboration spaces with controlled interfaces and some automated sharing of intelligence.

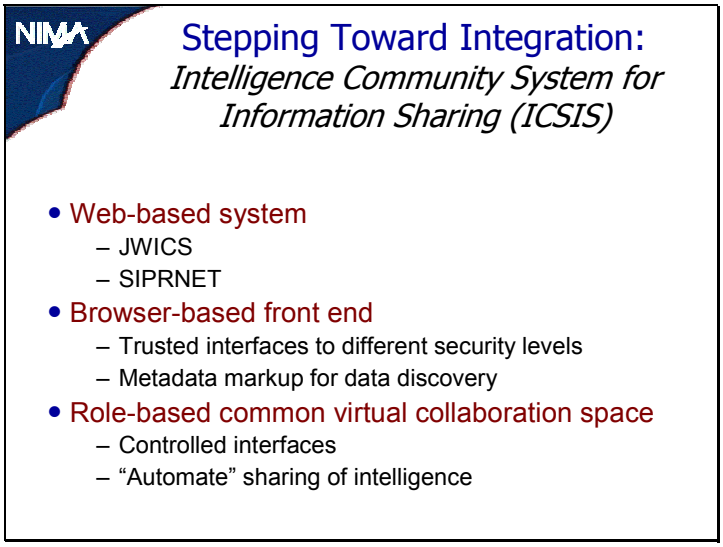


Figure 18

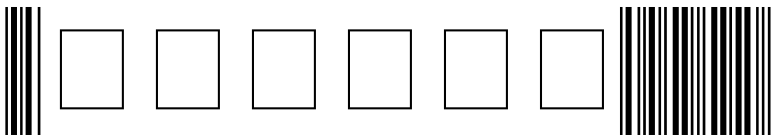
Again, that initiative is under development, and there are pilot and prototype activities. We, for instance, are participating with a pilot database effort and we are going to put our country databases within this environment. We decided to offer access to the country database that we had developed since Operation Enduring Freedom challenges, and we're one of the first agencies to come forward with a database for community-wide information sharing.

Oettinger: I hate to break into this splendid conversation, but I have made a commitment to get our guests to the airport in the face of our meteorological disasters. It's actually not a bad time to break in. What Bobbi has done is point out that there are a lot of open questions out there. It is far from a cut-and-dried subject. Even if we had another half hour, or two hours, we would only

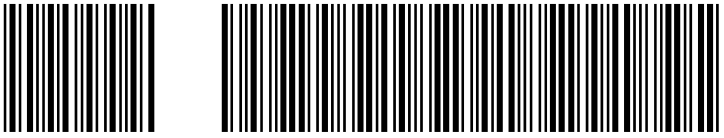
begin to scratch the surface, so I don't feel too bad. I do want to end this by giving you a small expression of our large gratitude for coming out in this lousy weather to talk with us.

Acronyms

CIA	Central Intelligence Agency
DCI	director of central intelligence
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DMA	Defense Mapping Agency
DOD	Department of Defense
GPS	Global Positioning System
HUMINT	human intelligence
I&W	indications and warning
ICSIS	Intelligence Community System for Information Sharing
IMINT	imagery intelligence
NIMA	National Imagery and Mapping Agency
NSA	National Security Agency
PDD	Presidential Decision Directive
SIGINT	signals intelligence
TTIC	Terrorist Threat Integration Center
USGS	U.S. Geological Survey
WGS	World Geodetic System



Seminar2003



ISBN 1-879716-86-0