[H.A.S.C. No. 108–46]

DEPARTMENT OF DEFENSE INFORMATION SYSTEMS ARCHITECTURE: ARE WE ON THE RIGHT PATH TO ACHIEVING NET-CENTRICITY AND ENSURING INTEROPERABILITY

HEARING

BEFORE THE

TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

HEARING HELD
FEBRUARY 11, 2004

U.S. GOVERNMENT PRINTING OFFICE
98–623 WASHINGTON : 2005

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

DEPARTMENT OF DEFENSE INFORMATION SYSTEMS ARCHITECTURE: ARE WE ON THE RIGHT PATH TO ACHIEVING NET-CENTRICITY AND ENSURING INTEROPERABILITY

HEARING

BEFORE THE

TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

HEARING HELD
FEBRUARY 11, 2004

U.S. GOVERNMENT PRINTING OFFICE
98–623 WASHINGTON : 2005

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE

JIM SAXTON, New Jersey, *Chairman*

JOE WILSON, South Carolina
FRANK A. LoBIONDO, New Jersey
JOHN KLINE, Minnesota
JEFF MILLER, Florida
ROSCOE G. BARTLETT, Maryland
MAC THORNBERRY, Texas
JIM GIBBONS, Nevada
ROBIN HAYES, North Carolina
JO ANN DAVIS, Virginia
W. TODD AKIN, Missouri
JOEL HEFLEY, Colorado

MARTY MEEHAN, Massachusetts
JIM TURNER, Texas
ADAM SMITH, Washington
MIKE McINTYRE, North Carolina
CIRO D. RODRIGUEZ, Texas
BARON P. HILL, Indiana
SUSAN A. DAVIS, California
JAMES R. LANGEVIN, Rhode Island
RICK LARSEN, Washington
JIM COOPER, Tennessee

THOMAS HAWLEY, *Professional Staff Member*
JEAN REED, *Professional Staff Member*
UYEN DINH, *Professional Staff Member*
WILLIAM NATTER, *Professional Staff Member*
CURTIS FLOOD, *Staff Assistant*

CONTENTS

CHRONOLOGICAL LIST OF HEARINGS

2004

WEDNESDAY, FEBRUARY 11, 2004

DEPARTMENT OF DEFENSE INFORMATION SYSTEMS ARCHITECTURE: ARE WE ON THE RIGHT PATH TO ACHIEVING NET-CENTRICITY AND ENSURING INTEROPERABILITY

STATEMENTS PRESENTED BY MEMBERS OF CONGRESS

WITNESSES

APPENDIX

DEPARTMENT OF DEFENSE INFORMATION SYSTEMS ARCHITECTURE: ARE WE ON THE RIGHT PATH TO ACHIEVING NET-CENTRICITY AND ENSURING INTEROPERABILITY

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES
SUBCOMMITTEE,
Washington, DC, Wednesday, February 11, 2004.

The subcommittee met, pursuant to call, at 3 p.m. in room 2118, Rayburn House Office Building, Hon. Jim Saxton (chairman of the subcommittee) presiding.

OPENING STATEMENT OF HON. JIM SAXTON, A REPRESENTATIVE FROM NEW JERSEY, CHAIRMAN, TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE

Mr. SAXTON. Good afternoon, folks. Why don't you have a seat? That is good.

Ladies and gentlemen, the Subcommittee on Terrorism, Unconventional Threats and Capabilities meets this afternoon to learn more about each of the services' information systems architecture, how they interface with the Global Information Grid, also known as the GIG, and how they interoperate with each other. The subcommittee is interested to learn more about the GIG and each of the services' architecture—and how each of the services' architecture will operate in a collaborative environment. We would like to know how the Department of Defense is working to reduce redundant noninteroperable and stovepipe systems and to eliminate the parochial interests to better support the Nation's warfighters.

As the Department transforms itself from an Industrial Age organization to an Information Age one, it needs to identify the critical elements of network-centric warfare, to assign roles and responsibilities for promoting it, and to describe how it will organize to implement transformational capabilities.

The subcommittee will examine defense transformation this year, and today's hearing begins that effort. We wholeheartedly support the Department's goal to have a Joint Network Centric Distribution Force, capable of rapid decision, superiority, and mass effects across the battle space.

However, there is much work to be done between now and achieving that objective. Realizing these capabilities will require great cultural changes in the people processes and military services as well as strategy to control DOD information systems to include managing interoperability issues among the services.

DOD's first step in creating the GIG architecture is a good foundation to build upon the GIG commercial-based technology that integrates legacy command control, communications computers, intelligence surveillance, and reconnaissance systems and permits full exploration of sensor weapon and platform capabilities for joint fires. While the GIG potential capabilities would be an enormous boost in supporting warfighters, I am concerned that warfighters may not be able to tap into these capabilities if individual services' architectures limit interoperability.

That is the focus of today's hearing: How are DOD and the military services designing information architectures to build a fully functioning network that every service man or woman may access and exploit, and how will these architectures resolve the interoperability issues that plague the services today.

There are several information systems issues that should be addressed during today's hearing. For example, how does the GIG architecture allow for the various service architectures such as the Air Force C–2 constellation, the Navy's Force Net, the Army's Future Combat System, FCS, Warfighting Information Network-Tactical, WIN–T, and the Marine Corps' expertise network to function with the GIG? How will these service-specific architectures interoperate with each other to provide a seamless transfer of data in communications?

I am concerned that the lowest level of compliance will be the result of these endeavors, rather than the maximum cooperation and collaboration between the services, because of the competing demands within each service. These and other fundamental issues must be addressed as the U.S. military transforms to defeat conventional and assymetric threats in the 21st century battle space. We cannot ask our young men and women to put their lives on the line if we do not provide them with superior means and tools to perform their duty. This is a responsibility that the subcommittee takes seriously, as do our witnesses I am sure. And we will continue our efforts to ensure proper oversight. Thank you.

[The prepared statement of Mr. Saxton can be found in the Appendix on page 47.]

STATEMENT OF HON. MARTIN T. MEEHAN, A REPRESENTATIVE FROM MASSACHUSETTS, RANKING MEMBER, TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE

Mr. SAXTON. And at this point, I would like to yield to the Ranking Member, my friend and partner, Mr. Meehan.

Mr. MEEHAN. Thank you, Mr. Chairman. Let me join you in welcoming today's witnesses. With "transformation" the watch word in the Pentagon, and the Information Age well upon us, IT investment decisions will provide the foundation for all future military capabilities. The disciplines of intelligence, command and control, and targeting all require accurate and timely information, and American industry is making information dominance a reality for the United States military.

It won't be easy to ensure the availability of information in a secure fashion anytime and anywhere. Some challenges are technological and others are organizational. The coordination of the re-

quirements and budgeting process should be of paramount concern. In the past, joint weapons system, planning and budgeting has not always succeeded. There is no denying it. Redundancies continued and joint programs have failed.

I understand the issuance of an IT portfolio management policy is soon expected from the Department. I am told that this policy will guide the investment decisions to ensure compatibility, interoperability, and the efficiency of DOD IT systems. But let's be honest, policies come and go. Without focused attention to execution, even the best policy will fail. Perhaps our witnesses can provide us with some additional insight with this regard.

And, Mr. Chairman, again I thank you for holding this hearing and I look forward to hearing the testimony of those witnesses before us. Thank you Mr. Chairman.

Mr. SAXTON. Thank you Mr. Meehan.

We have one panel of witnesses today. Our—and we will proceed with the panel, of course. I want to welcome our witnesses, who are the Honorable John P. Stenbit, Assistant secretary of Defense for Networks and Information Integration and Chief Information Officer for the Department of Defense; Lieutenant General Steven W. Boutelle, Chief Information Officer/G–6 for the Department of the Army; Major General Marilyn Quagliotti, Vice Director, Defense In formations Systems Agency; Rear Admiral Thomas Zelibor, Deputy for C4 Integration and Policy of the Department—Deputy Chief Information Officer for the Department of the Navy; Mr. David Tillotson III, Director, C4I, Surveillance and Reconnaissance Architecture and Assessment Department of the Air Force; and Brigadier General John R. Thomas, Director Command Control, Communications and Computers, C4, at the—and Deputy Chief Information Officer at the United States Marine Corps.

Ladies and gentlemen, welcome. I look forward to hearing your testimony, as I am sure the other members of the subcommittee do.

At the outset, I would ask unanimous consent that all members' and witnesses' written opening statements be included in the record. Without objection, so ordered.

I would ask unanimous consent also that the articles, exhibits, and extraneous and tabular material referred to be included in the record. Also, without objection.

Secretary Stenbit, the floor is yours.

STATEMENT OF HON. JOHN P. STENBIT, ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION AND CHIEF INFORMATION OFFICER FOR THE DEPARTMENT OF DEFENSE

Secretary STENBIT. Thank you very much, Mr. Chairman. It is indeed a pleasure to be here. I did take the liberty of bringing along with me one potential extra witness—not with an opening statement—Rear Admiral Nancy Brown who is a deputy J6 in the CS—but their role in the regulatory regime within the Department I felt would be appropriate as we got into some of these questions that you quite properly raised about how were we going to get from here to there.

Once again, Mr. Chairman, I am really pleased to be here to continue what were in fact a set of very interesting discussions be-

tween ourselves and the committee last year with respect to both formal and informal. I am extremely gratified to hear your endorsement of the—in your opening statement—goals and where we are trying to head.

And what we hope to do today is give you some confidence that we have a path, not particularly certain to get to perfection, but certainly one that is going to move us forward in this transformation as rapidly and as efficiently as we possibly can.

You quite rightly described the transformation toward net-centricity and why it is important, so I am not going to dwell on that. But I think today our real goal is to talk about the global information grid architecture and tell you how we are using this architecture to drive the three primarily departmental processes; one of which is requirements definition; the second of which, of course, is the budget; and the third of which is the acquisition programs. We have to succeed on all three fronts or we will not in fact get to the vision that we have both expressed.

So I think the best way to talk about this is to talk about the global information grid as the organizing construct for achieving net-centric operations and warfare in the Department of Defense. We define the GIG as a globally interconnected end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to the warfighters, policymakers, and support personnel. It is important for us to recognize that this GIG is actually a vision, an entity, and an architecture, and its application is different in those three definitions. I will see if I can get there.

As a vision, the GIG establishes the conceptual framework for the "to be" information environment of the DOD. It will provide information and communication services wherever they are needed in the DOD, be they warfighting or business in nature. And it will, in fact, move us toward net-centric operations. As an entity, the GIG comprises many systems that interoperate to provide the right information at the right place when needed. Thus, if you would like to think of it, it is a private World Wide Web. It is not the World Wide Web because we have significant requirements that are different from the normal Internet. We have security requirements. We have information assurance requirements. We have mobility requirements.

And actually, if we achieve our vision that virtually every element of the Department becomes part of this network, we actually need more addresses than are available in some sense in the general World Wide Web, if in fact every JDAM is going to have an IP address. So it is better to think of this as a private Internet rather than the World Wide Web, but it has many of the same issues. It is standards-driven. It is a collection of networks that work together, as opposed to one managed across the entire enterprise at a time, and that it allows the same transformation within the Department of Defense that has been going on in the commercial world both in the industries and government and others on a global scale; and that is the transformation toward net-centric world.

It is also an established and documented architecture that is the Department's enterprise architecture that defines the enterprise-

level information environmental blueprint. These are the kind of words that are common in the Clinger-Cohen ACT and the IT portfolio management world. The architecture comprises three perspectives or views, an operational view—if you want, think about requirements—a systems view—if you want, think about acquisition—and the specifics of a given program and a technical view, and if you would like, you can think there in terms of the interoperability and the kind of constraints that are on the system to make sure that it will in fact work end to end.

As such, the architecture represents the structure of GIG components, their relationships, and the principles and guidelines governing their design, operation, and evolution over time.

The responsibility for the GIG development and maintenance belongs to me in the Office of Secretary of Defense as the CIO of the Pentagon. The architecture is used to determine the interoperability and capability requirements, to advance the use of commercial standards, to accommodate the required accessibility, and also keeping people out that shouldn't be there.

We have a currently approved version of the GIG architecture which is version 2. Version 1, which was developed a couple of years ago, was not in fact moving toward net-centric, so we have a living document, if you wish, which will have a subsequent version which will refine these issues even further. But the GIG version 2 does represent a joint force and a coalition force net-centric perspective on information support. It also includes those ideas represented in the post–9/11 world with respect to the enhanced role of homeland defense special operations, continuity of operations, and in particular our outreach to our allies.

This year, the GIG architecture and its development process were very favorably reviewed by the GAO as part of its review of executive branch enterprise architecture, and is being worked to align with the Federal enterprise architecture as well. You will hear later from each of the services that their transformation initiatives flow from this overall DOD perspective, and I will let them describe how that connection works from their perspective.

As a result of the work done on the architecture, the Department has defined five key programs to facilitate this enterprise information environment. We talked about those quite a lot last year, and we really do thank you for your support that allowed us to move forward with those five key programs: the GIG Bandwidth Expansion, the Transformational Satellite System; the Joint Tactical Radio System; the Network Centric Enterprise Services; and the Information Assurances. Those programs, of course, have to meet the same architectural standards as all the other programs.

As a result of this work, in concert with the core DOD enterprise-wide programs, the services are planning and implementing a number of complementary programs required to realize that the end-to-end goal that you expressed so poignantly in your opening statement can be realized. These programs will in effect provide interoperable subnets of the GIG and will, when completed, become integral parts of the GIG, much as the World Wide Web becomes an ever-growing entity, even though there are independent management activities that work on the subsystems. And you will be hearing more about that later.

As I said earlier, we need to extend these transformations to our allies, and I think there we need to be realistic and that we are going to have to use legacy systems early, because they are not going to be as fast with this transformation as we are, but we are going to have to include them in this transformation as quickly as we can.

The primary means for verifying conformance to the GIG architecture—and are we in fact moving in the right direction—are embodied in two documents: "The Joint Technical Architecture" and the "GIG Architecture's Net-centric Operations and Warfare Reference Model." the JTA is a document that is cosigned by myself as the CIO and it was signed by Mike Wynne, the Acting Acquisition Under Secretary for Acquisition and Logistics. That is the document that in effect says if you are going to develop a program within the DOD acquisition system, you must meet these building codes in order to do it. The transformation of that Joint Technical Architecture from previous versions, which were mixtures if you wish of the old world and the new, to the new version 6 which is in fact a net-centric version, is crucial to the beginning of our ability to manage this kind of an opportunity. The Net-centric Operations and Warfare reference model defines in detail the specific operational attributes, system interfaces, and technical standards profiles. It is a reference document against which programs can be looked at, and in fact it is sort of the cookbook about how to be able to pass the oversight requirements of the Defense Acquisition Board and the Joint Requirements Oversight Board.

I might point out here that within the Pentagon we have a requirements process which is led by the military and the joint staff in general, and by the acquisition side of the house with the civilians in OSD and the services. The JTA and the NCAL are used as the core documents for both of those processes. In addition, the controller has been working on a Business Enterprise Architecture for the business domains, in order to be able to pull them together within the Department. That, too, is in conformance with version 2 of the GIG, and is, in fact, an extension to a "to be" architecture for the DOD enterprise of the future for those business processes.

There are other processes that help this along, such as architecture frameworks and data storage and some others which I will leave in the statement, but those are the key documents; JTA and the NCAL. As I stated previously, this architecture is playing an increasing role in the three of the Department's primary business processes: requirements, budget, and acquisition. The new requirements process initiated by the joint staff, the Joint Capabilities Integration and Development Systems, uses the GIG architectural description of information technology as the authoritative view of interoperability and information assurance for use in defining joint capabilities. They have also recently approved a mandatory Net-ready key performance parameter which applies to all new systems going through their requirements process. That particular KPP increases the Department's emphasis on information assurance and data interoperability through the NCAL and its application to new programs.

In the recently revised DOD acquisition process—now we are on the other side of the House—the GIG architecture is recognized as

the underpinning for all mission and capabilities architectures developed by the services and agencies. In addition, the Department requires the development of a GIG conformant C4I support plan for each program that in detail tells the information operability and the content needs and dependencies of individual programs. So now——

Mr. SAXTON. Mr. Secretary, because of the number of witnesses that we have, and we are going to be interrupted by votes sometime during this, could you summarize?

Secretary STENBIT. Okay, sure.

Mr. SAXTON. Thanks.

Secretary STENBIT. I am sorry.

Congressman Meehan talked about the portfolio management process which is about to come forward. That is another part of this. It is described in the statement. And we are in fact very grateful for your support of the horizontal fusion portfolio and programs. Those are used as experiments and have been very successful at pointing out how great it will be, once we get to net-centricity and those are complemented by a system engineering and test regime.

So, in summary, we are in the middle of a transformation. We have got some key programs moving forward. We have some regulatory processes and some documents, and we look forward to having you share your understanding and our understanding of that. And let me pass it to Steve.

[The prepared statement of Secretary Stenbit can be found in the Appendix on page 53.]

STATEMENT OF LT. GEN. STEVEN W. BOUTELLE, CHIEF INFORMATION OFFICER/G–6 FOR THE DEPARTMENT OF THE ARMY

General BOUTELLE. Mr. Chairman and members of the subcommittee, I am Lieutenant General Steven Boutelle, Chief Information Officer of the Army, the G6 of the Army. Thank you for the opportunity to provide testimony on the Department of Defense information systems architecture and interoperability.

Today we are an expeditionary Army, supporting the Nation on the global war on terrorism. But our Army is also in the midst of a massive reorganization creating modular brigade combat teams as fighting units that can rapidly deploy around the world. Our forward-deployed forces must have the capability to reach back from anywhere in the globe through global networks and tap intelligence resources and collaboration tools on a real-time basis. Forces will continue to deploy as part of an integral team of a joint force, and often as a coalition team, as we continue to fight the global war on terrorism.

As part of a joint or coalition expeditionary force, interoperability is not an option. Our existing systems that must interoperate are made interoperable. All of our new systems, as Mr. Stenbit has said, have a key performance parameter that requires them to be interoperable. The good news is that a lot of our systems now have achieved interoperability. Many of our communications systems and networks are based, as Mr. Stenbit has said, on the Internet protocol. That is the commercial IP Internet protocol version 4, foundation of the World Wide Web. It is a mandated standard by the Department of Defense Joint Technical Architecture and this

and other commercial-based technology protocols and standards are a foundation for achieving joint interagency and multinational interoperability.

The Army has nearly completed the migration to an Internet protocol or IP-based network as part of the larger joint network. In accordance with the DOD's Technical Architecture and current DOD guidance, we are moving to IP version 6 for a more efficient and effective network. In practical terms, interoperability exists today at the network level and extends through space-based and terrestrial systems. These transmission systems serve as part of our newly named LAN/WAREnet, which is the Army's portion of the GIG. So each service provides a portion and we provide our LAN/WAREnet, made up of the National Guard net, U.S. Army Reserve net, and then our active Army networks.

The DOD GIGs data strategy directs a more complete migration to commercial-based Web technologies which will further strengthen our interoperability across the joint interagency and multinational environments.

Network level interoperability is vital to all organizations within DOD. The example of this interoperability is a user with an Apple computer sending e-mail to a user with an IBM computer. Both computers have different operating systems, probably different e-mail programs. The network is comprised of piece parts from many manufacturers, Sun, Cisco, IBM, and Microsoft. However, the common and enforced standards such as those that reside in the Joint Technical Architecture ensure successful delivery.

This is obviously not as easy as building your own network at home. The soldier requesting artillery fire digitally to saving his buddies cannot wait because he hasn't been upgraded from a phone line to a cable modem.

Our security requirements add a complexity to the interoperability issues we are facing today. But we are accomplishing them. An example of the military application of network interoperability is the Joint Blue Force situation awareness or Blue Force Tracking you heard about in our last session, implemented in Operation Enduring Freedom and also in Operation Iraqi Freedom. While each service used different platforms and different computers to track blue or friendly forces, the network interoperability standards enabled commanders on the ground to enjoy near real-time visibility of friendly forces on dissimilar systems from individual trucks, tanks, helicopters, command centers, and even here in Washington in command centers.

As the Army transforms to the future force, we are developing a lighter, more mobile, more modular and strategically responsive organization, fully enabled by a more robust network of satellites, fiber optic cables, radios and tactical communications, battle command capabilities tied together; but these networks will be the bridge from our current to our future force, and enable expeditionary joint force commanders to fully conduct interdependent globally dispersed network-centric warfare. Battle command is the essential operational capability that fundamentally enable us for future operations.

Our chief of staff had 17 focus areas, one of which is networks. In fact it was his No. 2 focus area after the soldier. As we realign

into the new brigade combat teams and modular units, we are adjusting the architecture of these units to exploit the successes we saw in Operation Enduring Freedom and Iraqi Freedom and to realign and align with the Joint Technical Architecture. We are now, in fact, restructuring the Third Infantry Division at Fort Stewart since its return from Iraq, and we are redesigning that unit to be flexible, adaptive, and more joint.

Such systems as the Joint Tactical Radio System, the JTRS, the Warfighter Information Network—Tactical, the strategic tactical entry points, the teleports, and the Global Information Grid Bandwidth Expansion are absolutely essential to support those warfighters with secure simultaneous real-voice data, imagery, and video.

We are actively involved in synchronizing our information systems architecture. Our systems are being developed in accordance with the guidance of the Joint Technical Architecture in OSD which continues to provide adequate oversight.

We are in the midst of a global fight on terror. The future success of the Army depends on its ability to transform to a fully integrated force.

Thank you again, Mr. Chairman and committee members, for the opportunity to appear before you today. I stand ready to answer questions you might have.

[The prepared statement of General Boutelle can be found in the Appendix on page 76.]

Mr. SAXTON. Thank you very much, General.

General Quagliotti.

STATEMENT OF MAJ. GEN. MARILYN QUAGLIOTTI, VICE DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

General QUAGLIOTTI. Sir, thank you very much for allowing me to testify today. I have provided some charts to frame my remarks. If you would follow along, I would appreciate it.

On chart No. 2, I would just like to talk about things that we have learned coming out of Enduring Freedom and Iraqi Freedom. We have learned that we need to adjust our organization to take into account the new challenges ahead. One of those, we think, is the ability for the Department to have a joint acquisition organization.

As a result of the lessons we learned and direction from our civilian leadership, we are reorganizing to establish a joint acquisition organization as part of our agency.

The second bullet there indicates end-to-end engineering is the key future element that we must have in the agency. As you have already pointed out, the networks are incredibly complex and will cause us to do detailed engineering, end to end across the network. We are developing that capability.

In addition to that, another element that you talked about earlier is the ability to operate the GIG end to end, to support warfighting missions.

I would like to emphasize this by moving to the next chart, No. 3, that you have there. As you recall, General Franks did not move his headquarters forward during Afghanistan. And, in fact, he took quite a while to move his headquarters forward in Iraq. One of the

reasons for that is because of the connectivity that was provided back to his headquarters.

This is just a simplistic diagram that indicates that we have a lot of CONUS participation in ongoing operations. And this is not new. It really started during Kosovo, but it has grown through every operation where we leave more things behind, and we do what is called "split-based operation," or "reachback."

General Franks was able to command and control his forces from his headquarters back at MacDill. And also indications in this chart tell you the complexity of this, because as you look at the services involved in this, as indicated before, each service has a part of this network to operate. Yet no one is responsible for it end to end. As a result of that, DSA in coordination with the services is working on a new concept called Network Operations. And NetOps will give us the CONOPS and the TTP to operate the network from end to end.

Next chart, please. One of the challenges today that we have in the lower-echelon formations is the way that we have designed our systems so that they support a single mission. So as you see in this diagram, the information flow normally goes between sensor, those who decide whether to shoot, the weapons system that is located on the platform in a very linear way. There is nothing wrong with this design except it is not network centric.

If you will go to the next slide, what we see in the future is we have a common backbone today. We need to operate it as a common backbone and we, under the leadership and guidance of the NII, are establishing a post process where you post your data on the network and anyone who has access to the network can pull that information.

What this will cause in the future, if you turn to the next chart, it will allow us to do what is being termed joint forces integration rather than interoperability. And if you look at the information pattern on the left there, you will see that today an SOF team has a small amount of information available to them. And if you just follow it down the line, you can see that each warfighting entity there has a subset of information that is available in each individual system; each has a piece of that information but no one has all of it.

The future capability that we are looking for in network-centric warfare is the pattern emergence that you see there, which is to post all your information—on the right of the chart—is to post all your information on the network so that who has access to the network can pull that information and use it. Which means that the SOF team that might be out in the field, that has a network, would be able to get imagery that is available at the C–FLAX headquarters, the Combined Forces Land Component Command, or a joint headquarters. They would have the same ability to see what the higher echelon was seeing.

The program that allows us to move in this new direction is Net-Centric Enterprise Services. It basically imbeds in the network the capability to reach that information and deliver it to the end user. And then every program would post their information on the network.

So this is a totally different way of operating, and we expect that this will be a cultural challenge for us as we move through this program and as we learn and evolve into a new way of operating.

The next chart. DSA has many programs that are contributed to net-centric operations. But in the near term, the programs that we believe that must be executed properly to support DOD's ability to conduct net-centric operations are listed here.

And, Mr. Chairman, that is all I have. And thank you very much for the opportunity. I look forward to your questions.

Mr. SAXTON. Thank you very much. A very clear, and, I must say concise statement.

[The prepared statement of General Quagliotti can be found in the Appendix on page 63.]

Mr. SAXTON. Admiral Zelibor.

STATEMENT OF REAR ADM. THOMAS E. ZELIBOR, DEPUTY FOR C4 INTEGRATION AND POLICY AND DEPUTY CHIEF INFORMATION OFFICER FOR THE DEPARTMENT OF THE NAVY

Admiral ZELIBOR. Thank you, Mr. Chairman, and distinguished members. Appreciate the opportunity to appear before the committee today to discuss the Navy, and, I might add, in partnership with the Marine Corps, our approach to information technology architecture, which we call FORCEnet, and how we are interfacing with the Department's global information grid initiatives.

As the deputy for C4 Integration and Policy and the Department's Chief Information Officer Deputy for the Navy, I am responsible for the execution of policy processes and compliance with Sea Power 21 goals, which are our transformation goals.

I would like to take the next few minutes to tell you about FORCEnet and how it interfaces with the GIG architecture and our current challenges. FORCEnet operationalizes the concept of network-centric warfare for the Navy and the Marine Corps. FORCEnet serves as the underlying foundation for Sea Power 21, Navy's vision for aligning, organizing, integrating, and transforming to meet the challenges that lie ahead.

Sea Power 21 consists of three major pillars: sea shield, sea strike, and sea basing. The chief of Naval operations defines FORCEnet as the operational construct and architectural framework for naval warfare in the Information Age that integrates warriors, sensors, networks, command and control, platforms and weapons, into a network-distributed combat force that is scalable across the spectrum of conflict from the seabed to space and sea to land.

FORCEnet is not a program, but it is a forcing function for organizing, planning, and investing in the Navy's IT architecture.

DOD services and agencies are all working toward the same end state. But under the leadership of the Assistant Secretary of Defense for Networks and Information Integration, Mr. Stenbit, the services and agencies are working together to develop a consistent set of information technology policies, strategies, architectures, and standards.

For our architecture, a simple analogy to illustrate the way the Navy views this and our role in the GIG architecture development is the GIG initiatives like GIG Bandwidth Expansion could be

viewed as the national interstate highway system. The Federal Government builds this interstate highway system in coordination with the States, while the States build roads that connect to the interstate highway system. All users of this highway system employ the same traffic signals and signs for interoperability.

FORCEnet builds the Navy's roads to the GIG interstate, using common standards and interoperability such as the Joint Technical Architecture. Instead of developing our own architecture and standards from the ground up, Navy is participating fully in DOD's architecture and standards development process to ensure interoperability. The FORCEnet architecture is based on GIG architecture development and is the Navy's means for implementing seamless integration.

For example, the Navy fully participates in the development of all of the systems that Mr. Stenbit mentioned earlier, like the transformation of communications architecture, the GIG Bandwidth Expansion, teleports, the Joint Tactical Radio System, GIG Enterprise Services, Information Assurance Initiatives, and Internet Protocol version 6. We do have challenges. A major challenge for us is maintaining legacy architecture while defining future ones and migrating to these future architectures.

Synchronizing the integration of our existing systems into joint architectures, while ensuring we remain connected with our allies and coalition partners, continues to be one of our biggest priorities. Additionally, we are in a process of developing an integrated road map for both tactical and nontactical networks.

In summary, the Navy remains heavily engaged with ASD NII and others in creating a joint interoperable GIG architecture. Through agreed upon standards and business practices, we are breaking down the traditional stovepipe approaches and are working toward achieving joint and coalition interoperability.

I appreciate your efforts to help us be responsive to this changing world and in supporting our sailors, and I thank you again for the opportunity to be able to address you, and I look forward to your questions.

[The prepared statement of Admiral Zelibor can be found in the Appendix on page 86.]

Mr. SAXTON. Thank you very much, Admiral.

Mr. Tillotson.

STATEMENT OF DAVID TILLOTSON III, DIRECTOR, C4I, SURVEILLANCE AND RECONNAISSANCE ARCHITECTURE AND ASSESSMENT, DEPARTMENT OF THE AIR FORCE

Mr. TILLOTSON. Yes, sir. Thank you, Mr. Chairman. Members of the subcommittee. Like my colleagues, I am very pleased to be here today to have an opportunity to speak to you about the Air Force's contribution to the global information grid and net-centric warfare.

I want to start by first taking an opportunity to thank you for the continued support of the men and women of the Armed Forces. The work of your committee and others is very important in our ongoing efforts. I say the contribution to the GIG, like my service colleagues, I need to reemphasize Mr. Stenbit's point. We depart from—not depart from but take from the Global Information Grid Architecture and its subcomponents as our departure point for de-

signing architectures and designing the standards to which we build.

The Air Force's contribution to this concept is the C2 constellation, which are the Air Force components of the GIG. The C2 constellation is a family of C4ISR systems which share information horizontally and vertically. I think General Quagliotti said that much more cleanly than I did when she talks about the issue of sharing information not just in a linear fashion, but sharing it across and between the systems as well. It is both an operational construct and an architectural framework and, much like the Navy, C2 constellation is not a program. It is a way to drive Air Force programs to conform to the net-centric standards that have been handed down by the Department and the joint staff. And our objective is to provide decision superiority and air and space dominance in support of the Joint Force Commander.

Our key elements of this constellation include the various platforms and sensors the Air Force contributes to the joint war fight, key programs that support command centers like the Air Operation Center which is the JFAC headquarters, Joint Force Air Component Command or headquarters, and the distributed common ground segment system which provides a global backbone for processing and disseminating ISR information. And I will be happy to address questions on either of those efforts later.

In addition, we provide transportation layer components of the DOD GIG under an effort we call ConstellationNet. We envisage, much as the GIG does, a seamless airspace and terrestrial network that allows information exchange and a free flow of information amongst commanders and warfighters to ensure that we can create the right effect at the right time in the right place in the battle space. Key elements of this include the Air Force's portion of the GIG Bandwidth Expansion, essentially that the program is working through the services.

The Joint Tactical Radio System. We need to be able to expand the IP framework to airborne platforms. And we see the Joint Tactical Radio System as a key element of making that expansion happen. And included in that is the installation of beyond line of sight terminals on large platforms so that we are able to extend what is essentially now a current line of sight environment to a globally integrated framework for airborne platforms.

And, finally, we are responsible both as a service and as the DOD executive agent for space for providing a large chunk of the space segment of the GIG and including programs like the Advanced EHF Satellite, Wideband Gapfiller System, and the Transformational Satellite Program, which actually winds up extending the IP network into the space segment.

Each of these MILSATCOM programs represents a progressive expansion of the Global Information Grid both in terms of capacity, protection, and the ability to provide IP routing into space. And again I will be happy to address elements of that. That program in particular derives directly from a jointly held architecture, and may be a good example of how we are actually running multiple service programs under a joint oversight through the DOD space executive.

I want to conclude by saying the Air Force, like the other services, is committed to realizing a vision of providing a comprehensive terrestrial airspace and information capability that is global, robust, survivable, interoperable, secure and reliable. That is the key underpinning we are talking about. Nice set of words, but the challenge will be getting there. We believe that the architectural foundation and the standards foundation that the Department has laid down and that the services are extending serves as the fundamental underpinning to make that happen. And I think you will be satisfied as you ask us questions that we are in fact committed to realizing the vision of interoperability.

Thank you for your giving me the opportunity to be here and I look forward to your questions.

[The prepared statement of Mr. Tillotson can be found in the Appendix on page 99.]

Mr. SAXTON. Thank you very much, sir.

General Thomas.

STATEMENT OF BRIG. GEN. JOHN R. THOMAS, DIRECTOR COMMAND, CONTROL, COMMUNICATIONS AND COMPUTERS, C4, AND DEPUTY CHIEF INFORMATION OFFICER, UNITED STATES MARINE CORPS

General THOMAS. Good afternoon, Mr. Chairman and distinguished members of the subcommittee. I am Brigadier General John Thomas, Director of C4 and Deputy Chief Information Office, U.S. Marine Corps. Thank you for this unique opportunity to appear before the committee to discuss the Marine Corps' involvement in DOD system architecture efforts, how we are leveraging it to fill new information technology capabilities and to facilitate the horizontal fusion of information across the battle space.

Now more than ever, we are stressing interoperability in all of our warfighting endeavors to include our information technology programs. Today's operating environments are defined by joint and coalition operations. The Marine Air/ Ground Task Force concept has taught us as Marines the real power and necessity to operate as an integrated joint combined arms team. Our expeditionary nature, together with experiences from OEF and OIT, reinforces the principle that we must emphasize jointness in our operational mindset in the systems we acquire.

To that end, our IT enterprise must not only be internally consistent and interoperable, it must be also be interoperable with the rest of DOD. We are working closely with OSD, the joint staff, the combatant commanders, and the other services and agencies to synchronize our architectural efforts across a variety of missions and mission areas to achieve this goal.

The Global Information Grid is the DOD framework for achieving net-centric operations and warfare. Aligning with the Federal Enterprise Architecture, the GIG architecture is the standards that the components and the services and agencies are adhering to. As already has been stated by Rear Admiral Zelibor, FORCEnet is the Department of the Navy's component of the GIG. And currently we are working with the Navy to identify the essential command and control and IT capabilities of FORCEnet.

The Marine Corps Enterprise Network is the Marine Corps component of FORCEnet and the Global Information Grid. It is our enterprise framework for IT, supporting all information exchange requirements for marine warfighters and our supporting establishment. It is our end-to-end IT capability and infrastructure, spanning both our warfighting and business domains for sharing information.

The Marine Corps' transformation to net-centric force is inextricably linked to the evolution of FORCEnet and the GIG. As both evolve, we are coevolving our architecture and adjusting our underlying programs to leverage transformational capabilities. And a number of them have already been highlighted here today.

A critical enabling initiative for the Marine Corps in its net-centric transformation is the Marine Corps Enterprise Information Technology services. This is our framework for realigning, collapsing, and consolidating all of our IT environment. It realigns the Marine Corps environment of applications, databases, networks and facilities into an integrated layered architecture to deliver capabilities based on a common infrastructure and shared services. Our goal is to leverage the capabilities inherent in programs like the GIG Net-Centric Enterprise Services and the Navy/Marine Corps Internet. It supports IT portfolio management, addresses technology, processes, standards, work force and governance, satisfying our IT objectives that are laid out in the Navy Marine Corps strategies.

In conclusion, the Marine Corps is rapidly becoming a net-centric force through the application of joint standards and adherence to a single DOD architectural framework.

Mr. Chairman and members of the subcommittee, thank you again for your support, and I will be happy to answer any of your questions.

[The prepared statement of General Thomas can be found in the Appendix on page 92.]

Mr. SAXTON. Thank you all very much for kicking us off here with your great opening statements. Let me just ask what I think, at least for me, is a very basic question here.

We all as Members of Congress very much appreciate and agree with the objectives that you have set forth in the use of a technologically advanced system to increase our capabilities. That goes without saying. Now, the Air Force C2 Constellation was—is a system which has been developed by the Air Force. The Navy's FORCEnet is a separate system that has been developed by the Navy. The Army's Future Combat System and Tactical Win-T is a different system. And the Marine Corps' Enterprise Network is yet a different system.

And I think what I would like to know, or what I would like to walk away from today's hearing with, is an understanding of how we are going to in reality bring these systems together to accomplish the great goal that we all have.

And what I would like to do is start with General Quagliotti.

General QUAGLIOTTI. Quagliotti, sir.

Mr. SAXTON. Quagliotti. Thank you. I am sorry.

And then go to each of the services and then finish up with a conclusion with Secretary Stenbit. So, ma'am, if you would like to start I would appreciate it.

General QUAGLIOTTI. I know it is difficult to hear all these different names and understand that it is really the same network. It really is the same network. The way the network responsibilities are broken down is that DSA is responsible for wide-area networks, and services are responsible for post, camp, base and station, networks. And services are also responsible for deployed networks that support lower-echelon forces. So, although we are calling it different names, it is really the same network.

The challenges, as you highlighted earlier, really have to do, how do we operate this at a global level so that we have an information sharing from top to bottom, from side to side? The best way I can describe that is to tell you that we have done a mission analysis. We have looked at the functions that should go across from bottom to top of the network, and that is what I alluded to before in the NetOps concept. And all the services are on board with that.

We are getting ready to stand up an organization to do this and establish a global command and control system for networks so that they will operate end to end. I hope that answered my part of the question.

Mr. SAXTON. Let me just amend my question just a bit. What plans do you have to tie or replace existing legacy information systems into the service, into your plan?

General QUAGLIOTTI. Uhm——

Mr. SAXTON. In your system.

General QUAGLIOTTI. DSA is really not responsible for that part of it, sir, and so I would say that our responsibility is to build out the infrastructure. We are doing that with GIG BE and we will phase in the DSN pieces into the GIG BE as we roll out the program. So we do have plans to do that. There are road maps to get that done.

Mr. SAXTON. Thank you. Mr. Tillotson.

Mr. TILLOTSON. Yes, sir. Thank you.

I think, playing on General Quagliotti's point, it is not different systems. And C2 constellation, as I said in my opening remarks is not in fact a system. It is an architectural construct that allows us to organize our systems and bring them together to meet the net-centric goal. So the systems that underpin that, for example, the GIG BE component, is much as General Quagliotti described it, my portion of that highway system, if you will. I am looking for the point where DSA stops delivering the product and I start delivering my base modification and upgrade. The standards I use to do that are straight commercial standards. I will use straight commercial products to deliver that capability. So in this case, I will buy from a portfolio of products that, quite frankly, we hope to take advantage of more kind of commercial buys on.

At a more specific level, you asked for an example of ways that we could start to retire or reduce service-specific components. And while it is very much in its infancy, the problem that General Quagliotti mentioned earlier, Network-Centric Enterprise Services has embedded within it a number of key initiatives that we in the Air Force are, quite frankly, looking forward to with high interest.

One of them, as an example, is the provision of collaboration services.

Right now within the Department of the Air Force alone, I can point to 10 to 15 collaborative tools and pieces of software that exist across my networks that various agencies and entities use. DSA is proposing to move that forward on a more enterprise scale and, quite frankly, I just presented to our CIO and our chief of communications a proposal that said we are going to throw our efforts behind that, start to phase out and wean ourselves from our systems. And we are putting a warning notice out to our MajComs and senior commanders saying, "Stand by. As soon as this program kicks off, I am going to force you on to this standard."

So there is a specific case where once—as the infrastructure is built, I am looking ahead to make a conscious decision to eliminate portions of my unique systems, if you will, or at least the collection of systems that aren't even unique to the Air Force but represent the plethora of systems that are proliferated and move to a commonly agreed standard.

But I think the key in moving this forward is in fact to have that happen, we have to be able to put something forward, demonstrate it, and then move toward it. And because we are operating in a framework, an understood framework which the architecture foundation work that NII has started and the services have continued to flow down, I now have a very real means of having that conversation.

We are doing it also laterally. Within the construct of the C2 Constellation, the Air Force put forward a proposal, took forward an initiative to replace its distributed common ground station, which is within our ISR framework, our ISR processing systems, to upgrade it because we were basically reaching end of life. We took a proposal forward that met the open systems standards of the network-centric vision and the DAB endorsed that as a lead-the-Department-exercise or lead-the-Department-activity that, quite frankly, the other services are now supporting. Our requirements were adjusted to reflect all service requirements, and we are now issuing and have issued a request for proposal on behalf of the Department as the lead agent. So I think these activities are having real consequence.

Mr. SAXTON. Thank you.

Thank you. General Boutelle.

General BOUTELLE. Yes, sir. I think General Quagliotti has made a great point on there. And the three networks, Constellation Net, FORCEnet, and our LAN/WARnet, which has all the pieces, are essentially one network. It is much like Sprint, AT&T, and Verizon. It is not in Verizon's best interest to build a phone that can't call somebody who has an AT&T phone. They all use the same standard. Much the same as ours. We are all using the standard, and that standard was put out by OSD and the Joint Technical Architecture, and that happens to be IP Version 4 right now, Internet Protocol Version 4. And they have also put out the Network Centric model, the NCOW model that we are using. So as far as anybody driving that together, you don't have to drive it to get them, any more than Verizon would want to go off on their own and not talk to an AT&T phone.

The network is relatively simple once we agreed upon the standard, and in fact the standard is a commercial standard. They adopted the commercial standard. So I can send an e-mail or a video or imagery from a military network to a commercial address if I desire. All the same standard.

At the next level, at the next level where you get the application, what hangs off it? A fax machine, an answering machine? Once again, you want to meet the standard to ride the AT&T network or Verizon, or in our case a LAN/WARnet or Constellation Net. But when you get to the next level of the applications, the Air Force application working with the Army, that is the piece that is a bit more onerous, but in fact I think we are making great progress on the requirement side with our Joint Staff and our JROC and Functional Capability boards as we drive those together on information requirements of what should interoperate with what.

Now, we have a lot of legacy stuff out there, truth in lending. We didn't have a joint technical architecture until 4 years ago, 5 years ago, and now we are all building——

Secretary STENBIT. And it didn't constrain you very much.

General BOUTELLE. It didn't constrain us very much. We have had that discussion, Mr. Stenbit.

Now that we have one that is being converged and actually making much more restrictive, it is driving us to bring those systems into that common standard. But we have a lot of legacy out there. And many of you, most of you have visited Iraq, and you saw a lot of legacy and you saw a lot of commercial off-the-shelf. The commercial off-the-shelf that we took over there meets the common standard. Some of the legacy stuff, a lot of it we put black boxes in, but we have to interface, and that is a painful expensive process.

Mr. SAXTON. Thank you, sir.

Admiral?

Admiral ZELIBOR. Yes, sir. I won't expound any more that we are all on the same network. I think that point has been made. But what I will talk about, is, okay, how do you get compliance with those kind of standards. And one of the things that we initiated in the Navy and the Marine Corps was a FORCEnet compliance checklist. And at three different levels, the operational, the requirements, and also the technical level, we have put together a document that everybody will have to conform to in order to be in compliance with the GIG architecture and also the Joint Technical Architecture. So I think that is a big step forward. And if it doesn't pass the check during that process, then the system, or whatever it is that is going forward, will not be approved.

Also, I just want to say one thing about the systems. We are no longer viewing individual systems. I view the network as the system, and individual programs then plug into that, and they have to be able to communicate across that domain. And that is the approach that we are taking on this.

And I will pass to John then.

General THOMAS. Just a couple comments, sir. I would just add that, first, FORCEnet is not a system, it is a framework. The Marine Corps Enterprise Network is not a system but a collection of system, or systems of systems. As you take a look at the future,

and moving to a net-centric environment—I will give you an example.

We have got thousands and thousands of radios that are out there right now supporting our forces in OIF. Those are all, many of them are circuit-based radios. If we are going to truly transform the force, we need to move to a network radio as an example. That network radio is JTRS. So when you start to take and dissect the network, there are many components and many systems that make up the network, and again they are all a part of the global information grid.

Mr. SAXTON. Thank you very much.

Mr. Secretary, let me just clarify what all this is. We have got two votes coming up here, the first one just started. It will last about 17 minutes, and then the second vote will last 5 minutes. So we will have to run off here in about 10 minutes.

Secretary STENBIT. I won't take that long, sir

Mr. SAXTON. No, that is good. I was going to say, everything seems to have been fairly consistent among the answers so far. And so if you could summarize, perhaps, Mr. Secretary, that would be good.

Secretary STENBIT. Well, it sounds as if it is all a well-rehearsed issue. I think I need to put some perspective on this. We have done this in the past. We built voice systems that interoperated the same way. We had a long-haul system at DISA, we had service voice systems.

If it is just commercial, it turns out to be easy. Then we put in secure voice on top of it, and that started to make it a little harder because some of us use different voice coders and so forth. We have used this same technique in the past to get this kind of a job done. I guess we failed to tell you that particular analogy in the past. I think it is key for you to understand, from my point of view, we could not have been as proscriptive and narrow in the standards we will allow until we were confident that we were going to have the base programs there to provide the bandwidth to allow us to go net-centric.

So had you had this hearing last year, you would have not heard what you heard today because we didn't know with sufficient clarity that we were going to be able to kick off the transformational communication satellite, that we were going to be able to build the GIG Net with expansion program.

So it is the very fact that we built those core programs—and thank you very much for your support in allowing us to move forward on those—that we are now able to have the confidence to start to use the regulatory regime that we used in the past for voice and for data and for other things to now use that same process on the IP world.

So I think that is really what you are hearing is a time warp of our confidence we are going to get there, and now we need to get on with the program of adapting our regulatory regime to the future instead of the past. I hope that helps.

Mr. SAXTON. Thank you very much.

Mr. Meehan.

Mr. MEEHAN. Thank you, Mr. Chairman. I will be brief.

Secretary Stenbit, the Department says it wants better coordination among IT requirements, budgeting, acquisition. But since the passage of Goldwater-Nichols Act of 1986 and the creation of the Joint Requirements Oversight Council, jointness has been an institutionalized goal with formal mechanisms to achieve it even as the Department identified the development of information technologies as a priority.

How is the current effort to better coordinate joint initiatives an improvement over what we have done in the past, and why should we have confidence that it will prove more successful?

Secretary STENBIT. I am going to ask for some help from my friends. But one of the ways I would look at that is because we are now in a commercial standard world, we really are borrowing from the World Wide Web and other issues, more people are able to instantaneously join each other. In the past, when we had very special purpose systems that we had to work very hard to make interoperate, it was very difficult to join the club. And so actually I am very much more optimistic that the information underpinning of our jointness is easier today than it was in the past. Not because we are geniuses, but because we are now able to use commercial standards. And everybody buys Microsoft and everybody buys IP, and it is not that difficult anymore.

I think at this point, if I may, we have talked from the service and acquisition side. If I may have Admiral Brown discuss a bit about the requirements end, because it is just as important that the warfighter requirements reflect these same requirements. Is that okay with you?

Mr. MEEHAN. Sure.

Secretary STENBIT. Please, Nancy.

Admiral BROWN. I think what you have asked is a very significant question. And you mentioned that JROC process. And there is probably no one at the table that would disagree with me to say that the old process emphasized service-centric systems. And we knew that there were some real shortcomings to that system, and so we have implemented a new system that we call the Joint Capabilities Integration and Development System, or JCIDS. And the Chairman of the Joint Chiefs of Staff signed that out in June, and we have started on a new path of how we determine what warfighter capabilities are, where the gaps are, where the overlaps are, and what are the areas that we need to emphasize in determining how we move forward to this net-centric environment. And the JCIDS is really based on a top-down process. It starts with the national security strategy, flows into the national military strategy, and then we have joint operations concepts. And those joint operations concepts along with the other documents provide the conceptual and the architectural framework for how we are going to move forward.

We have developed in conjunction with this five or six functional capability boards, and they review all new systems that are coming forward. They are also doing significant analysis work on determining, through integrated architectures and what the—how the warfighter has told us they are going to fight in 2015, where the gaps are and what we have today and what we need to be able to

fight that warfight that the combatant commanders have told us that they are going to need.

And we use those functional capability boards to do those things and to validate things as they come forward to the JROC that this actually is net-centric, it fits into the integrated architecture that all the services have agreed to that NII has provided through the GIG architecture framework. And only those things that are endorsed by the FCBs then go forward and get funding and approval through the JROC process.

So I think you will see that that is a very different process.

And Mr. Stenbit also mentioned the net-ready KPP, which goes hand in hand with our new JCIDS process, where we validate through four pillars information assurance, we use the Network Centric Operations Warfare Reference Model which was provided to us by NII. We use key interface profiles to determine whether or not a system is net-centric. And we are looking not just at new things, but we are also looking at legacy systems. How can we make that net-centric, or does that need to transition to a new system that is coming on-line, and what is that transition path.

So I hope that addresses your question.

Mr. MEEHAN. Yes, it does. Thank you very much.

Thank you, Mr. Chairman.

Mr. SAXTON. Folks, we are going—well, we already have run off. We are going to go vote, and we will be back in 10 or 15 minutes.

[recess.]

Mr. SAXTON. Okay. We will get started again.

I know that Mr. Larsen just hit the chair there, but he and I were chatting on the way over the vote and he has some interesting questions and thoughts.

Mr. Larsen.

Mr. LARSEN. Thank you, Mr. Chairman. And I guess my return indicates the value of showing up. I mean, I have some questions. My first question is a general question. I am not sure it is answerable as much as it is maybe reemphasizing the point of this hearing today and why the chairman sought to call it. So I will ask it rhetorically, I suppose, but then I have a follow-up that I think is a specific question that is maybe answerable.

The rhetorical question is this: At what point could, say, the Admiral give the General's presentation? And at what point could Mr. Tillotson give General Thomas' presentation to us today? And in other words, just how much are you all coordinating to the point where someone else's work is—that you know someone, another service's work so well that we can be assured that the steps that Secretary Stenbit is coordinating on the GIG is in fact becoming that integrated? And that is the general sort of rhetorical question.

Mr. SAXTON. Ask them

Mr. LARSEN. All right. Well, since I am saying the word general, General, you get to go first.

General BOUTELLE. I think of course some of it depends on your background and how you have come up. But at the highest level, we probably could do it today as long as we are talking about at the joint architectural level and major programs.

Now, as you peel the onion back on any individual service, you will find varying levels of knowledge. You know, we work very

closely with—I do—with the ESC, HANSCOM Air Force, very closely with the Marines, because they know their ground combat arms. I couldn't peel the Admiral's back as close as I could peel ESC, HANSCOM's and the Air Force's back. But at the highest level you would probably find pretty good commonality today of names of major systems and how they work together.

Mr. LARSEN. Admiral.

Admiral ZELIBOR. Yes, sir. I would agree with that. And, you know, at the upper level we are doing that today. And there is an effort that was started about 6 to 8 months ago where we were doing C4ISR integration talks at the high level. And it initially started with just the Navy and the Air Force, and we were focused around the time sensitive targeting thread. But now the Army and the Marine Corps are also involved in that. As a matter of fact, General Boutelle and his group will be hosting the next one, where we are trying to break down the language barrier so we understand what are the things more at the—the individual programs that really are affecting this. So I think we are on that path to do that, exactly what you say.

Mr. LARSEN. Does anyone else want to offer?

General THOMAS. Let me follow up on that, just if I might. I will tell you, those of you that really know the Marine Corps recognize that we are the smallest of the services sitting at the table, but we have got the biggest budget. That is a joke. And so what we do is we obviously leverage, you know, the work that goes on in the other services to the maximum extent possible. And I can give you numerous examples of where, you know, the development takes place in one of the other services and we buy or procure through one of their contracts. And we do that routinely.

Not only do we do that. When you have—when you take a look at it on the major programs that the Army is developing right now, you have mentioned some of them, the FCS, WIN–T, and so forth, the Marine Corps is heavily involved in that and participating in that process to fill the capability because we are going to take the best that the Army has developed and employ it if we can.

On the Navy side of the house, I will tell you, if you take a look at FORCEnet, FORCEnet is another good example. You know, the FORCEnet capabilities list that is proffered as a part of FORCEnet is a combined effort on the part of the Navy and the Marine Corps. The concept, the operational concept that supports FORCEnet is signed off by the Commandant of the Marine Corps and the Chief of Naval Operations. So I mean, we are working very closely on all of these initiatives across the board.

General BOUTELLE. I have to tell you, when I was a colonel I was the program manager for the Marines and the Army for field artillery, multiple launch rocket systems. And as a PEO, I also built their radio satellite systems as an Army officer and had Marines assigned within my organization

Mr. TILLOTSON. And certainly I will endorse the comments at the table. I have participated in those same forums that Admiral Zelibor mentioned, where we started off with the Air Force and Navy dialogue here at the headquarters level largely, but also with the senior commanders of our development agencies.

And I think the characterization General Boutelle makes is correct; at the top level we could all speak reasonably well about the other's major systems. What is even more encouraging, from my point of view, is as much as that is useful and important to set direction, we are seeing the same thing take place at the next echelon down. So at the detailed engineering level there is a very active dialogue going on between Spy War, C–COM and ESC, HANSCOM at the details level, at the no kidding, let us connect the wires, make the nuts and bolts, walk and talk level. And so that dialogue is now taking off as a result of the start at the air staff level. And it is connected in turn to JF–COM recently as they have started to stand up their architectural efforts.

So what most encourages me is not just the fact that those of us sitting here at this table could say that, and say that with candor and honesty, but more importantly I can pull in a group of colonels at the next echelon down, have them sit here, and probably really bore you to tears with the kinds of details they are working on.

And that is positive. That is the question I think that, put on the table, of how is this really going to get institutionalized, something beyond a policy memo.

Secretary STENBIT. I would like to reflect back on what I answered to Congressman Meehan. It is easy for us to say what we are saying today because we are using IP as a goal, Internet Technology. If you had asked that question 25 years ago, the optimization of radio in the Army, which needs to work over the hills and in trees, which is different from the one in the Navy, et cetera, would have caused the end goal of being able to communicate with voice, for instance, to be a little too ethereal, so it wasn't worth the effort.

The fact that you are going toward a net-centric issue and we have the joint tactical radio system which allows you to go backwards to whatever your radio optimization is, and then go forward in the net-centric world, I think is an enabler for us to be able to be as positive as we are.

So here is a case where technology has broken down some potential bureaucratic barriers that would have been there if the technology hadn't have come along

Mr. SAXTON. Thank you. Let me ask a follow-on question to my first question. Several of you just mentioned understandings, capabilities, and cooperation at the highest levels—or at high levels, I guess maybe you said. Keeping in mind my original query, how will this cooperative effort, understandings, activities be—how will they permeate through the force structure?

Secretary STENBIT. Let me start by—the word high level was used several times, and I believe that meant at the standards level and at the detailed communications level. If you think of this in the IT world and the layers of the IT world, it is the other way around. We are very confident at the transmission level and the services level, going to IP and net-centric enterprise services.

I think General Boutelle remarked in his opening comments it is when the applications have to interoperate where the complexity will be greater, because the actual concept of operation of how military forces are operated by the Army is different from what happens in the Navy and much closer and much more closely aligned.

So even as you go further down into this process, which means the actual operation, or if any information stacks, you go up toward the applications, I believe you will hear the same things, which is the Army and the Marines are closer than the Army and the Navy. The Air Force and the Navy, when they are doing airplanes, are closer by definition.

I used to laugh that the Navy was closer to the British Navy than they were to any U.S. service. I think we have overcome that. But there was a tradition of that in the past. So they have specialty requirements, sir, and I think they should speak for themselves. But at the fundamental ability to interoperate and be able to pass data back and forth, we are pretty comfortable. I don't think anybody is going to use the same software for the same job across the entire Department. It is probably not even the appropriate thing to do.

Mr. SAXTON. Throughout the force, what will be the basis and standards upon which decisions are made about technical acquisitions?

Secretary STENBIT. The two basic standards are the Joint Technical Architecture, which is a book, and the net-centric Operations in Warfare reference document, which are a set of ways to look at how you put those standards together in various scenarios. Those have to be living document. Commercial standards will change, our standards will change. So there will be an evolution to that. Those two in conjunction with the architectural frameworks of the GIG, at the system, technical, and operational level, will in fact be the issue.

But, Steve, maybe you can talk about your checklist when you go through a system.

General BOUTELLE. I think this Joint Technical Architecture you have heard so much about is a very interesting document. When we received that document from OSD, from Mr. Stenbit's office, it says: Here is what you are authorized to buy today, these standards. And in the second part of each chapter says: And here is what we are considering putting in next year's edition of the standard.

And each of the services comes back and says, I kind of like it, I don't. Have you thought about this?

So we really have a period of time to negotiate, where is industry and commercial technology going? And then hopefully we get it back next time they have incorporated the services' recommendations. And then that primarily is all of the services looking at what is out there commercially, what is coming down the line, what is Cisco building or Juniper or Sun, or whoever it may be, IBM and, looking at that, saying where are these technology and protocols going. And then we input it, and hopefully when it comes back we are all headed in the same direction.

Mr. SAXTON. General, what will keep the lieutenant colonel at base X from saying I have got this job to do and I need a system to do it. And he goes and gets one that is not compatible. How do you——

General BOUTELLE. I think it is like anything else in our business or your business, and it is a resourcing.

Mr. SAXTON. Yes, sir

General BOUTELLE. And at least in the Army, what we went up against that last year—we review right now in the CIO—and a lot of that is because Clinger-Cohen is a very strong, strong document. We review every purchase over $25,000 in the Army. And if they go off on a tangent, we remove the money. So it once again comes back to resourcing. We watch the resourcing very carefully and the buys. And that is really the strong point we use.

Mr. SAXTON. Thank you, sir

Mr. Kline, sir.

Mr. KLINE. Thank you, Mr. Chairman.

And thank you very much, lady and gentlemen, for being here today. Every time this subject comes up we are by necessity forced into a discussion of leveraging and facilitating and nets and architecture and systems and net-centric and so forth and so forth. And I would like to—I have got a couple of questions, but I want to start with saying how much I appreciate the comparisons or analogies used today about highways, major highways and streets feeding into them. And, more importantly, about General Quagliotti's description that said that—in fact, actually the Secretary and I think the General both said this is like a private World Wide Web. And the General said that we are looking at a, quote, totally new way of operating.

But it sounds to me like, in the larger picture, what you described, General, was what we see every day on that not private World Wide Web. That is, people have a Web site, information goes up there; if you want it, you go to the Web site and take it down. Is that what you are describing?

General QUAGLIOTTI. Actually, it is more sophisticated than that, sir. The way I would describe it is this way: We will have services embedded in the network, and so instead of hauling around a set of servers at a headquarters, for example, you won't really have server forms anymore. What you will be able to do is if you want to download an application for a certain mission that you have to do, you will be able to do that off the network. And you will be able to then pull data elements from several different locations and present those elements on a screen to do that mission. So right now what you have on the World Wide Web is really word documents that are available to people. And what we are really talking about——

Mr. KLINE. Or music, for example?

General QUAGLIOTTI. Right. But what we are talking about is data elements. You put the data in once on the network, and then you are able to construct or compose the picture that you want to see based on the application that you are using and the data that is available on the network.

I don't know if that helps describe it.

Mr. KLINE. Could I just sort of by a nod of the head or a simple yes or no, is that what—is that description what all of you have been talking about for these last couple of hours? Are we all agreeing that that is in fact what we are talking about?

Mr. TILLOTSON. Yes, sir.

Secretary STENBIT. Let me give you two analogies. One thing that happens that we have to be able to do faster than the commer-

cial Web is, if you get married and you want access to your wife's bank account——

Mr. KLINE. Good luck

Secretary STENBIT. It is very much more complex than just doing a new password. You have to go get a notary to sign something and send it in. We can't afford to do that. We have to be able to dynamically assign privileges that are different because the job changes in seconds as opposed to—so there is a case where that is a harder problem for us than the commercial one.

There is another case, which is—I think it is General Jumper who says there are no hourglasses on our systems. You can't wait for that little thing to show up on your screen while you are waiting to shoot somebody.

So we have some different requirements, but intellectually you are correct, it is the same general thought process.

Mr. KLINE. With the more difficult problem of security and having to have that security access immediately

Secretary STENBIT. Yes

Mr. KLINE. Okay. Thank you. But there is a sort of a nodding of heads, though, that that is what we are talking about, going to a site and being able to pull down information, data, photographs, everything, and consolidate them for your use. Is that correct?

General THOMAS. Actually, that is true. But I think, sir, that the other thing that we would put emphasis on is establishing the authoritative data. General Quagliotti talked about it. And that was, once you post the data, then you know that that is the authoritative source for that, whatever it is might be tracking information. On the Web right now you can't do that. I mean, you put in your Google search and you get tons of hits, but you don't know who the authoritative source is. That is a challenge that we are dealing with as a part of the effort

Mr. KLINE. Got it.

Mr. TILLOTSON. And a final point, to extend your analogy. If I use the Web environment like that you are talking about that you use every day, you go look for things. We also want to add the layer that says, I would like to define the kinds of things that are important and have the system go look for things and then go at it.

If you will, it is more analogous to the things we see in the stock market where you have automated trading routines that watch trends and cue the operator to say, okay, you need to go buy, sell, do that.

So there is a layer of that that actually has some commercial basis that we can begin to exploit as well.

So this is not, again, new technology; this is an issue of applying a commercial standard at a next level. Kind of, if you will, tailoring your Web page.

Mr. KLINE. I guess that is why I was struck a little bit by General Quagliotti's statement that this is a totally new way of operating.

General QUAGLIOTTI. It is.

Mr. KLINE. It doesn't sound like it, but perhaps it is

General QUAGLIOTTI. No, it is.

Admiral ZELIBOR. For the military.

Mr. KLINE. For the military, I will accept that. I think she is saying no.

General QUAGLIOTTI. I guess if you look at my information chart that shows the level of information that is exchanged and available to people on the network today and the way it will be available when we finally get this done, that really implies a different way of operating.

For example, if you are a private today and you have access to a network, you don't get the same information as a four-star general. There is different—there is different levels of information that are available to people based on their job, their duty position, their function. So what we are talking about is a change in the way we operate in that the information is available if you are given access to it. So——

Mr. KLINE. Right. The general may be given access to things that the private isn't. And in a perfect world it might work the other way.

General QUAGLIOTTI. Correct. But today——

Mr. KLINE. I was just making sure the generals were awake.

General QUAGLIOTTI. Sometimes that is true. Today, what we have is not so much that we don't want to share the information, but that the soldier who is looking for the information just can't get it because it is tied to an application—the data is tied to an application that is operating in a linear way on the network.

Mr. KLINE. Got it.

General QUAGLIOTTI. So what that means, sir, is that the guys on the top of the organization and the guys at the bottom of the organization have the same information. And how does a leader change the way they lead when the led has the same information that they do potentially? That is what I am talking about.

Mr. KLINE. Okay. Thank you.

I am sorry. Admiral—I should have thrown admirals in there. I am sorry

Admiral ZELIBOR. That is fine. One thing that Marilyn brought up that I think is important, and that is she threw out a term called "composability." and that is something that the Navy is really looking at in FORCEnet as one of the ways that we can do business differently. It is a culture change. And when you look at any capability that you try to field, you can look—visualize this as a pyramid. At the bottom you have a platform, and then you have some sensor or weapon that goes on that platform. Then you have a communications layer. Then as you go up you have some kind of computing layer. Then you have an application layer, and there is some kind of human interface.

Well, in the old days we would build capability A through Z, and they would do very well at vertically integrating all those layers in that pyramid.

And then as an afterthought we would say, how do you—now we want these two things to talk to each other, so you do middleware or something. It gets very expensive and it is very difficult to do.

Well, composability is a concept that is pretty interesting, because at each one of those layers, if you have a common way of capabilities talking to each other, let us say at the sensor weapons layer you use XML language, at the coms layer you have IP. We

have already told you that. All the way up to the human interface, which is point and click, drop and drag. These are all things that we know. If we build to those standards, now you can compose capabilities on the fly. And that is where the real power of network-centric warfare comes, because if you can compose capabilities, then you can compose operational forces and then you can compose your doctrine or training. It is really an interesting way that this could happen in the future when you look at it.

Secretary STENBIT. You have got a pretty complex, yes, but there are differences. I think that is the key we are trying to emphasize. But in general you had the right framework of the commercial IP Web.

Mr. KLINE. Thank you. Understanding that there are some complexities and perhaps may be more sophisticated,I am going to strain my chairman's patience for one more question, if I could. And I am sort of following up on the chairman's question about how do you keep the lieutenant colonel or the major or anybody else from going out and buying his or her own hardware and/or system, arguably? And I think back to 15 years or so ago when we had enterprising lieutenant colonels and majors in the Marine Corps who discovered that they needed to be able to talk to people, and a cell phone, which back in those days was bigger and blockier, would be a good thing to have. And they went out and bought them with O&M funds.

And, General, your response to the chairman's question was, well, we are going to keep our eyes on resourcing; and if it is over $25,000, we are going to know about it and we will step in. Now, I admit that it would be hard to set up a local area network or much less a binary network, with $25,000, but not difficult to go buy hardware and software for an office or two offices or three offices. So I am still sort of pursuing that question.

General BOUTELLE. Great question

Mr. KLINE. And if you can just put my mind to rest there

General BOUTELLE. Most of us are working enterprise contracts. Now, we signed an enterprise contract for Microsoft products about 3 months ago for 6 years, and we are standardizing on Microsoft products across the Army

Mr. KLINE. Excuse me. Across the Army?

General BOUTELLE. Across the Army. The Air Force is working with us, they are going to do the same thing, although we have found as we have looked at it, does it make sense to go larger and make one big one? No. When you reach about 10,000, you max out on cost efficiencies. But we are doing it across the National Guard, the Reserves, the active duty component Army, DA civilians, and all Army supporting commands. We signed that contract for 6 years. That is being implemented now. The first packages went out worldwide in January. And so we will standardize—although we will still have some other products out there, we will probably be about 97 percent Microsoft. And we have already directed out of our G3 that anything that is not the latest versions will be taken off-line on January 30th because we have some security issues we are very concerned about and we are trying to bring the whole Army worldwide up to the same level.

So what we have done is we have direct funded that. We pulled money back from the commands and direct funded that Armywide. And the next thing we are doing is we are copying the Air Force on their centralized buying on hardware. And so we are working very closely with the services on enterprise buys.

Mr. KLINE. Well, that at least partially answers the question. If the enterprising lieutenant colonel—I am not sure why I am picking on them today, but they are an enterprising lot—goes out and buys something, it at least would probably be a Microsoft. But it doesn't answer the question of what about the Navy? What about the person at Joint Staff? The question is still the same: Is there something department, DOD wide that would discourage that from happening, and do it in a way that doesn't keep us from growing? I mean, I would argue that if we were relying on the JROC system to buy computers 10 or 15 years ago, if we hadn't had people go out and buy them, we may not have the mess we have today, but we would still be using typewriters and hand-cranked Xerox machines.

Secretary STENBIT. You hit it exactly on the head, which is there is a balancing act here between ossification of a bureaucracy to save money but actually costs more by filling in the forms and, unfortunately, sometimes costs more than just money.

I think you have heard the leadership at the table say we are going top-down. The big acquisitions, the big expenditures of funds, we are going to control as best we can. Nobody should tell you that we can control every purchase of a GPS receiver or a cell phone or whatever. Many people buy it on their own money. That is also something that is wrong if we can't in fact provide the right kind of funding to be able to have somebody have a GPS when they need one.

All of the services are doing that differently. We all have the same techniques. Steve talked about ordering agreements that we try to get, make it more attractive to them to buy if they are going to do it in a decentralized way, stuff that is approved, if you want to think of it that way. We have other problems like collaboration tools where it doesn't work if you don't talk to each other. So we get a lot more ruthless about that, that you must take one that meets our standards; and if you don't buy the right one, we are not going to collaborate with you. So there are forcing functions. The Navy has an amazingly forward-leaning outsourcing which is quite notorious, for both good and bad things called NMCI. But it is a technique that the Navy is using to try to grab hold of what used to be the enterprising people doing everything differently and having some configuration management. That program has had some difficulties, I think everybody knows that, but it has had some amazing successes, which is we now have much better security, for instance, and trust in the Navy desktop environment than we had before.

Each service is doing it differently. The point you are bringing up actually adds up to quite a lot of money.

General THOMAS. Sir, I would like to give you a Marine perspective, sir, which is perhaps a little bit——

Mr. KLINE. Easier for me to understand?

General THOMAS. It will perhaps bring you up to date on the Marine Corps side of the house.

We now do centralized IT procurement. All IT procurement is centrally controlled with a CIO at the top of that. We have a waiver process, so if we have a command out there that wants to spend their O&M dollars to buy IT, they in fact must come through my office to get approval to do that. And when that happens, it is my responsibility to ensure that we have looked at the architecture, we understand the "to be" architecture, and we make a decision based on that. So we have a process established there. We also have published what we call a software baseline to all of our forces, both operating and supporting establishments side of the house, with a list of approved software products. And these items make the list because we have enterprise licenses. We leverage the enterprise sustainment or enterprise software initiative that OSD sponsors that they have collectively come up with enterprising licenses for DOD that we leverage. We have a governance process where the operating and supporting establishment play in. They sit at the table as we are deliberating on policies that we are implementing to take and enforce these standards that I have talked about.

So I think we are a little bit more ruthless in our approach across the board.

Mr. TILLOTSON. In addition to the procurement activities, I think as everybody has talked about and we are all implementing, there is one other step, and General Quagliotti referred to it

Mr. KLINE. Could I interrupt for just a second? And you are next anyway. I would like to find out, if you are not as ruthless as the Marine Corps, what you are doing. We got an answer from the General, but, I mean, the Marine Corps has now centralized that procurement and I am just sort of interested in what the Air Force and——

Mr. TILLOTSON. No problem. In fact, General Boutelle mentioned it as well. We have an Information Technology Commodity Council that has been established to do commodity procurements across the Air Force. We have provided that at this point in the highly encouraged mode, but we are moving rapidly to the you must buy mode.

Mr. KLINE. That is not quite ruthless yet?

Mr. TILLOTSON. It is not quite ruthless yet, but it is about to be ruthless. Part of the reason is we are within certain domains, within certain activity spaces and sets of equipment, we have pretty much made it—not pretty much. We have made it mandatory to go look and buy these things off of this procurement buy. And, quite frankly, it is so fiscally attractive that we really haven't had any trouble getting the enforcement at the top level in the sense that the price break is so significant that at least one of our major commands tripled their buy with the same budget. So there is nothing like a positive inducement as well as a negative inducement. By doing that step, we created a very positive impact, and more importantly, all the commands are coming back and saying we want more of that because there is high payoff.

But that still doesn't quite get at your question, which is, okay, so I am still Lieutenant Colonel Joe Bag of Doughnuts, and I can still go to my local store with my procurement card and I can still

buy my computer. I can do all of those things, and I can still do that. There is a final step that we are all working on that I don't think we have addressed. So I was kind of not trying to avoid the one question, but let me jump to the other side of the street.

It is the net ops piece. The Air Force has been working very actively to consolidate network control centers at the MAJCOM level. And that provides not just an external looking defense, but also provides monitoring of the performance of the network and an active program to test the security of the network. And part of that activity is aimed at finding people who have attached themselves to the network in an uncontrolled and unconfigured fashion. And that information assurance component is as much an essential part of this activity as anything else we have talked about.

So part of the reason for the ruthlessness in configuration control is all the kinds of fiscal good stewardship issues that we have all recognized, the power of the dollar, et cetera, et cetera. Quite frankly, that is equally balanced in our minds on the Air Force by the compelling need of needing to provide this private worldwide network as opposed to the publicly accessible worldwide network that we live in in our day-to-day existence. So our consolidation efforts have looked at forming a series of—we actually have an Air Network Ops Center that—and part of our growth path on the GIG–BE is to provide these Network Ops Centers working in conjunction with DISA that provides oversight and visibility into who is using the network, how they are connected, when they are on it; and, if we detect presences on the network both external and internal, then how we go after them.

So there is an enforcement mechanism that prohibits and a discipline that is instilled to say, when that lieutenant colonel goes and buys his or her computer, it still has to go through a configuration check. And commanders are literally the folks who are charged and accountable for making sure this doesn't get connected. So there is another side to this enforcement mechanism down at the detailed level.

Mr. KLINE. Okay. I am really guilty of hogging my time here, but, General, you pretty much answered the question in your earlier discussion about controlling resources. But could you just—do you have a central clearing authority like General Thomas does in the Army?

General BOUTELLE. We centrally clear those. And we also have the same thing on the Network Operations Centers, and we also have a CIO executive board which is much the same as the other services have to bring the CIOs in. So it is a series of processes to go through.

Mr. KLINE. Okay. And Admiral?

Admiral ZELIBOR. Yes, sir. We do, and we are probably as ruthless as the Marine Corps, but we are not quite as mean as those guys. That is their job. But we have two parts that we do. The first one that Secretary Stenbit mentioned, NMCI, nothing goes on that network. It can't. It won't even allow you, because of our Network Ops Centers you cannot put an application on there. And without the thing—it will just reject it. It can't happen. And what we have gone from, the Navy was like the other services I am sure, we had about over 1,000 different networks inside the Navy. We had al-

most 100,000 applications. We have been very ruthless about cutting that down. And when you really look at it, you know, every application, I don't know what the ratio is, but equals lots of servers, and lots of servers equals lots of money. Well, we have reduced from around 100,000 applications down to around 6,000 now with the goal of going down to 2,000 applications. And we are doing that by really being very strict on what are the business functions that we need to do on our nontactical IT side that will fit within that NMCI framework, which is I think very important.

The second thing that we are doing is what I will call a capital planning process. It is the first time I think that we have ever gone out and really tried to categorize both the nontactical and tactical IT in one place where we are putting strict rules and guidelines that of what you will and will not buy. And it is centrally—there is central oversight, and it is something we call the C-Enterprise Board of Directors. And as the CIO for the Navy side, I report directly to that C-Enterprise Board of Directors, who is chaired by our Acquisition Executive and our Vice Chief of Naval Operations, And nothing goes unless those guys say it.

Mr. KLINE. Thank you. That strikes right to the heart of it, that you are putting out rules about what you can and cannot buy. And thank you very much for your answers. I appreciate your patience with me.

And, Mr. Chairman, I really appreciate your patience.I yield back.

Mr. SAXTON. Well, I owed you.

Mr. Larsen, do you want to jump in here?

Mr. LARSEN. Thank you, Mr. Chairman.

I want to ask a question that is probably first most appropriate for Secretary Stenbit and perhaps for General Quagliotti regarding legacy systems. In someone's testimony they mentioned exactly how we are planning to take care of legacy systems. We have talked about how—I will use another analogy. The GIG is sort of the sun around which each individual world revolves. And you visit the GIG in order to get to the next world, and on top between each other, I think we have established that, that analogy, certainly in terms of the highway system. But if you have these legacy systems say down the organization within each organization and you are having to then—it sounded like I thought I had heard you, it sounded like you were going to be essentially reprogramming these systems to be able to travel from place to place. Do you—what is the cost of doing that? And do you lose the effectiveness of creating that integrated system that we are trying to get to through this reprogramming of the legacy systems?

In other words, if the Navy's legacy systems and the Army's legacy systems are so different, so old and so different, how do you get them to catch up with where everyone else is higher up the chain?

Let us start with the Secretary first, from a global view

Secretary STENBIT. I don't think you should think of it as higher up the chain. I think it is happening at the bottom as well as—actually, probably faster at the bottom than it is at the top. The Secretary doesn't have a computer in his office, to my knowledge, at least. But it is inverse with age. It is okay.

Your question is an extremely good one. We are not going to be able to replace all of the Defense Department's electronics gear instantaneously. So what we are talking about is the process at the leading edge of this business, which is what are we going to do this year with the money we have? We are going to emphasize moving toward net centricity, and we are going to deemphasize moving forward on other kinds of systems. That doesn't allow us to just junk them all instantaneously. As a matter of fact, probably quite a lot of the discussion that will go on between the Department and the Congress will be over how much—because we are risk averse. You know, we have to go out and fight wars. So how much are we going to continue to put into legacy even though we know that there is a better world out there is an important attribute. Our goal is to get to the future as fast as we can. Once we are there, we are going to have to adjust to look backwards to people who didn't go as fast as we did.

Let us pick our allies is a great example. I talked about that in our statement. We can't do operations without allies, and they are not going to be anywhere near as fast as we are about moving forward. So even when we are in the forward leaning posture, we are going to have to learn how to look backwards. The good news is the technology allows us to emulate. So you can make an IP thing look like a voice circuit; in fact, voice over IP is exactly that. You can't make a voice circuit look particularly like a data centric network.

So your point is exactly correct. Part of the force, that which is net-centric will do better, be able to perform better than the part that is in the legacy world. But there have always been parts of the force that have a better tank or a better airplane than some other part.

So it is the same general problem. The only good part about that is that these are commercial standards so that everybody can get with the program I think easier than it would have been in some highly complex way. I think each service is going to deal with this differently.

General QUAGLIOTTI. If I could add to what the Secretary just said. It is that we have an active program in DISA to review everything that we are spending money on with an eye toward killing those things that we no longer need to spend money on, and putting the money toward network centric solutions. And I think that you have to have an active program, it has to be a detailed review of everything that you are doing to make sure that you are reorienting your whole organization toward a network centric solution. And you really have to aggressively go after it, because people who own programs are very proud of what they do, and they don't want to give them up. So it has to be a leadership issue of really going after it.

Secretary STENBIT. I think one way to look at it is you need to cut the R&D off at the legacy programs first and ruthlessly. The procurement is second.

Mr. LARSEN. This is a follow-up question. This is yet another analogy, and I am sure the Admiral will appreciate this. There is a scene in Master and Commander: The Far Side of the World, where they are actually going through the—around the Cape. And I forget which mast breaks off, but one mast breaks off, and there

is one of their sailors on it and it is dragging the boat back, it won't let the ship go forward. And at some point he makes a decision, they are going to cut this mast loose and in this case lose a sailor. But they have to do it to move forward.

At what point then—have you thought through, at what point, you know, you cut the mast loose on somebody's legacy system so that we can move forward?

Mr. TILLOTSON. I think the Secretary hit the nail on the head. Each of the services is looking at their programs through a capital investment planning process to make those very decisions. Based on what we need to achieve, based on what functions we need to maintain, based on which of those systems are critical; which can I immediately jettison all together because they are duplicative. Which can I cease R&D on, because I—although I have to maintain it, I don't have to make it any better, and those that I unequivocally have to maintain. And we are all pretty seriously bending things into those categories and saying these are the ones I am targeting to move forward, these are the ones I am targeting to hold. And I will cease R&D, but at least I have got it maintained. And then the good news is there is probably enough out there, enough chaff out there that we can go, and I think Admiral Zelibor had some very good statistics from where the Navy put things on the table, but we do as well, saying I have got X number of systems doing the same thing, I can just start by making some of those go away.

So a detailed capital investment planning process where portfolio review, which is what we are calling it in the Air Force, from the CIO level down across all the activity base is really the way we are tackling this problem to free up, to address and free up the resources to move forward. And I would reinforce General Quagliotti's point. This is not a bottom-up process. This part of the process is very much leadership top-down. Within the Air Force, this group, this team is being headed right now by the Air Force CIO and the DCS warfighting integration. We report out directly to the Chief and the Secretary on this matter. And there aren't a lot of in betweens about it.

Mr. LARSEN. Anybody else want to comment?

General THOMAS. I will just jump on a couple of comments.

First of all, I mean, we recognize that there is a delicate balance between legacy and future. And my comment is when somebody asks me the question, I always say today's legacy system was yesterday's future system. So you are going to always be caught in that delicate balance.

Going back to Admiral Zelibor's comments earlier relative to applications, there is an example where the Navy reduced from 100,000 or so applications with a goal of going down to 8,000 and even further. Likewise, on the Marine Corps side of the house, we started out with over 8,000 applications and our target is 500. We have already reduced it close to 80 percent now already.

Now, there are some users out there that had to give up some capability as a result of that effort. And, again, you know, what we said was is that if there is another application out there that satisfies 75 percent of your requirements, then that is better for you to move to that one than to pay for two applications where both are

achieving about 75 percent of the capability out there in the applications.

So we are making those kinds of trade-off. We are doing that, going through that same process on the systems side of the house, whether it be trying to decide to take and drop a legacy radio and wait for JTRS to be filled. We are looking at all that. We have our transition road maps that tell us when the break-even point is relative to a specific system. So we are looking at all of that.

Admiral ZELIBOR. There is two ways that we are doing it, and I will do it from the warfighting side since I already mentioned the nontactical IT side. And in our requirements process, we have—we do campaign analysis to show where our requirements needs are, where there may be gaps or, what is more important, where there may be redundancies. When we do that campaign analysis, then what we are doing is we are working with our systems command, which is SPAWAR out in San Diego, and they are doing a systems analysis on, okay, what is it that we can really get rid of here so that we can start moving on to the future, because we want to be able to recapitalize and start getting out there. And between those two things, it turns into a pretty interesting process where, when you start peeling back that onion and you look at the functionality that you need at each warfighting level, of how many programs you may have that all say they are doing the same thing. And so that systems command analysis then really helps us in making those rational decisions.

The part where it gets difficult is when you look at—we have some systems in the Navy that are just two.dot.four systems. I mean, it is just amazing that basic messaging. But when you look, you can't just say, well, you are not going to do that anymore, because you have to make sure that the capability exists for us to move on on those particular ships, but more importantly, the Navy probably does a significant amount more of coalition work in the sea side than maybe the other services have to deal with. And so I can't necessarily just cut the umbilical cord and expect that our coalition guys to be along with us. But I also don't want them slowing us down too much. So there is this balance that we play.

Mr. LARSEN. General, did you want to comment?

General BOUTELLE. Just a quick one. In the resourcing, you know, we just put together this week, I was working on OIF–2 for Iraq. We still have 20,000 radios out there I had when I was a second lieutenant 33 years ago. But we stopped buying them waiting for the JTRS. So you make a—first of all, it is a long buy when you buy as many as you do for the Army.

The second is, a lot of your major platforms, you just can't throw away. The M1A2 tank is not a bus tank; the M1A2–SEP. The SERUP–J847 hasn't got a bus in it, but when it goes to recap we will probably bus it.

So the major end items like that doesn't make much difference, because you know you are not going to build a new tank today or next year or in probably the next 20 years, so you end up recapping those, bringing those on. And in some cases you wait for a future system.

So there is a lot of things you go through, and we are all going through our programs program by program to decide what to do with each one.

Mr. LARSEN. Mr. Chairman, two more questions for Mr. Stenbit.

Mr. SAXTON. Sure. Just make them quick, if you can.

Mr. LARSEN. First off, I—actually, I will boil it down to one question. And this is either a soft ball or a curve ball, I don't know, sort of the $100,000 question.

What you have heard today, is any of this a surprise to you?

Secretary STENBIT. No. The issue is that we are in a transformation. That means that we are accelerating change. The obvious nature of how great it is going to be at the other end is gathering steam quite a lot. And I was very gratified to hear the chairman's opening statement, which quite clearly put us both on the same side of that. We are going to someplace which is good; now we are going to discuss how we are going to get there.

There are all kind of complexities. We are not going to do it the same way. It is not appropriate that the Army do it exactly the same way the Navy does, because there are specialty issues. But at the big picture, and even at the little picture, because of this fundamental commercial soundness, I am very confident that this evolution is well under way and is going to do quite a good job. No, I am not particularly surprised. Some of the detailed stories are interesting.

Mr. SAXTON. Mr. Secretary, thank you very much.

Mr. Larsen, great questions.

Mr. Secretary, all of you seem to be on the same page in terms of explaining your success in developing interoperability to the point where I think it is fair to say that you sound like it is not a problem. Can you—or you think it won't be a problem. Can you then explain why there is a need to fund pilot programs to resolve interoperability between systems? Specifically, the net-centric Enterprises Services Program and the Horizontal Fusion, which, if I recall—I can't recall the exact numbers that you have requested, but it is probably somewhere between the two systems, between 100 and $150,000 million.

Secretary STENBIT. Right. I actually believe it is probably higher than that, maybe 200. But——

Mr. SAXTON. We will take the higher number just for emphasis. And tell us why, if the interoperability issues are kind of behind us, why we need to spend this money.

Secretary STENBIT. Well, there is two issues, because those two programs are doing different things. The net-centric Enterprise Services is in fact the enabling device to allow most of what we were talking about. So it is crucial to our ability to achieve the interoperability that you have heard. If we are not able to in a common way across the enterprise assign access, assign privilege, find data, discover data, it is those services that is in fact the exact output of the net-centric Enterprise Services contract—program.

So absent that program, you would not hear the optimism that you heard from this particular group. It is in fact one of the five linchpin programs.

The Horizontal Fusion Program operates at the next level up, which is the applications level, which is where we all think and be-

lieve it is going to be a little bit more difficult, which is, assuming we get to a well-integrated transport layer and data layer, how do we then maximize the achievement of the benefits of such systems at the application level and as General Quagliotti talked about, how do we optimize this change in how we do business so that we have learned how to do it.

And that is the purpose of the portfolio of the Horizontal Fusion Program, which is to take several ongoing processes that are not net-centric, and put money into them to create them—to move them to be in a net-centric world so that we can then put them together in groups and discover the dynamics of how that works.

Secretary STENBIT. So I don't mean to miss—change how you asked the question, but the NCES is crucial to the issue of the interoperability of the enterprise. Without those services, I don't believe we would be anywhere near as optimistic as you heard today. So we basically testified assuming that we were going to continue to get support on that.

Horizontal fusion, as I say, is a set of experiments—a portfolio of experiments not to test interoperability but to test what happens when you take a program which is not net-centric and put it into the net-centric environment. So I personally believe both of those are very important and hope that you will continue to support them. It allows us to test how the culture changes, I think is the right way to put it.

Mr. SAXTON. Thank you.

I have two more questions, one for—that I would like to address to General Boutelle. There has been a strong connection drawn between FCS and the Internet and the general Internet program, and I am curious to know how strong that connection is. I understand that there must be a connection because future combat systems will essentially work and draw information and give information to the entire network. So how closely are they tied together?

General BOUTELLE. The future combat system has really traded——

Mr. SAXTON. Is what.

General BOUTELLE. Has really traded armor for the net-centricity and for data and information and intelligence. What they have done is—you know, it is a family of three things. You have manned vehicles, unmanned ground vehicles, unmanned aerial vehicles. But all of those are tied together and enabled by this satellite system such as teleport, advanced DHF, the TCS TFAT system, the step sites, the GIG bandwidth expansion. If they don't operate within that system, if that is it not out there providing them that pervasive network and information that they have been talking about here, if all that information is not coming from sensors and intelligence platforms and resources, FCS will be unsuccessful. It is more a C–4ISR system than it is an armored system.

Mr. SAXTON. The FCS system that I have seen described in the past has been explained in terms of conventional warfare. How does the FCS work or how do you expect it to work in terms of asymmetrical warfare, the war against terror, scenarios like we see in—that we are seeing now in Iraq, for example?

General BOUTELLE. I think the FCS strength is when you made that smaller—much smaller platforms, not the heavy armored plat-

forms, not the M1 Abrams tank, not the Bradley but smaller platforms, and then you enable it with unmanned platforms.

First of all, the mobility of it will be tremendous. You can put it on C130's, small airplanes, move it very quickly to get you there. But, once again, your enabling against asymmetrical warfare will be the information flow and the intelligence flow for you to be able to close upon whatever particular target you are after. You have traded off that heavy weight armor and size for a very small platform.

Mr. SAXTON. And what kind of armor will they have? What do you think?

General BOUTELLE. I am not going to broach that now. I have worked with it. Very honestly, I don't spend that much time on the armor side. It is on the network side and the C–4I side and the sensor side. But we have traded off the heavy armor we had.

Mr. SAXTON. Well, this probably isn't the place for this, but I just got back from Iraq over the weekend and the number one problem that we have is finding the bad guys. The number two problem we have is protecting our people, because they don't have armor.

So I hope that we are not, you know—again, this is not the forum to discuss this in. This is a different strategic kind of a question. But I am just very much concerned, and having you here today I just wanted to express these concerns about assumptions that we are making about the threats that we are going to face may not be true, as demonstrated by our building to fight wars that are history.

That is what—our guys are getting killed today in Iraq because we collectively—and I am not blaming you—we collectively made some bad assumptions. Maybe it was—maybe we made the best assumptions that we could, but I see a warfare—a potential for types of warfare in the future that may—light vehicles that are not armored may not be suitable for.

So I hope that somehow we can keep that in mind and—in the trade-off of information technology for armor. That is a question in my mind.

General BOUTELLE. I think your point is very valid. The only thing I would add to it is, regardless of what you do with the platform, the C–4ISR piece, the network piece could be employed over existing heavy platforms as well as light platforms. So I think the real value that you are going to get out of FCS is the sensors, the networks, the networking information; and whether you applied it to a heavy force like you need in Iraq or a future FCS force, it would have great leverage in either one as an enabler.

Secretary STENBIT. Sir, I know we are getting close to the end, but I want to be positive about what you just said. Because of the horizontal fusion program constituent parts that we did last year, we had a program demonstration where we put together a lot of those in an exercise last August which was called quantum leap. I believe you were—oh, you didn't come. Some of your folks from the Hill did come over and take a look at it.

Out of that very process came some ideas about how to do a better job of combining the local intelligence in the Army units in Iraq with the more national intelligence that is coming from some stuff that I don't want to talk about here. Actually, we are about to

move some of the quantum leap, or some of the horizontal fusion algorithms, in a net-centric environment into Iraq to allow the people that are having troubles with these IEDs going down the road.

It is a way to put information in to help them, if you would, put little red dots on their maps that say somebody said that is a bad place to go. Today, that is very difficult to get those data around. So there is a case where right now, today, we believe it is worth the time and effort and money to put in information in order to protect the existing infrastructure of vehicles, which is different from the question you asked because the assumption is we are going to be able to do that so much better we are going to be able to change the vehicles.

But I wanted you to be optimistic that we have some ideas right now, today, that are about to go over there that have the attribute, which is you take a given set of vehicles and make it a safer place.

Mr. SAXTON. Okay, I will buy that goal.

Secretary STENBIT. Well, we hope it is going to be this summer or within months. So I am not talking about long-term future.

Mr. SAXTON. Good. Okay. I would like to talk to you about that in private some day.

Secretary STENBIT. Be happy to do that.

Mr. SAXTON. Thank you. Thank you.

We have raised concerns with Internet Protocol Version 6, IPV 6, and whether it will provide the same quality of service that the Department's computing network protocols presently provides. Why did you make the IPV 6 decision without conducting tests at scale to provide this architecture—to prove this architecture at the very least reproduced existing quality of service?

Secretary STENBIT. The decision is that we are going to do scale level tests in 2004, 2005, 2006. Because we said we weren't going to pull the switch until 2008 when we had, in fact, done scalable tests where we took subsets of the Department's infrastructure and moved to IP version 6 and made sure we understood how far that was.

So this is a policy that says we intend to move to IP 6 in 2008. We don't want people buying IP 4 from now on because we think we are going to have to save the money to be able to invest in IP 6. But we are not going to enforce that in a rigorous and tough way without having large-scale experiments.

Mr. SAXTON. My helper is writing as fast as she can. Sorry for the delay.

Will the testing be—where will the testing be conducted, and how realistic and rigorous will the testing be?

Secretary STENBIT. We have asked the services to nominate subsystems that are appropriate and scalable. The NMCI is one which we are considering, which is a 400,000 node network which has excellent configuration management, so we can find out at that kind of scalability.

The Missile Defense Agency, which is a sort of a closed command and control system, is willing to consider being one of our tests. So we are going to—SIPRNET is a place where we might go do this kind of a test. We are looking for pretty large-scale existing systems to take the step earlier so we can understand what it is like.

Admiral ZELIBOR. I can help with that, if you want.

In addition, sir, there is three—we are using a test bed within the Navy that is really part of the GIG test bed, and there is three parts to that. You have a thing called the Boston South Network; the Advanced Technology Demonstration Network, which is based at the Naval Research Laboratory here in D.C.; and then SPAWAR that is in San Diego is also part of working—is actually the lead for the Defense Research Enterprise Network. All of those things are being connected, and there is very rigorous testing going on for IPV 6 there; and, also, looking at what I will call dual stacks, where you look at the interoperability between IPV 4 and IPV 6 in that research network.

So that is—there is a lot of effort going into that to make sure we have the appropriate testing for this.

General BOUTELLE. And, Mr. Chairman, we have our facility at Fort Wachuka, which we call our Technology Integration Center, where industry brings in and basically funds their products. We are doing IPV 6 there, and we will be doing a large-scale IPV 6 at Fort Hood for our tactical users at our single tactical support facility.

Mr. SAXTON. Well, thank you very much. At this point, I would just like to say that we have probably some other questions that we would like to submit for the record. If you would be kind enough to——

Secretary STENBIT. Be happy to.

Mr. SAXTON [continuing]. Get back to us on those.

Let me just thank you all for being here today; and let me say that we, Members of Congress, are very much in support of your goals. I have been able to experience IT, which I have seen that has been extremely useful from San Diego to Tampa and from Qatar inside of battle space; and it is impressive.

Having said that, like most Members of Congress, we don't really understand what you do; and we are trying hard to do that. As you know, there are some of us who feel more strongly about that than others; and, as a result of that, we had quite a debate last year, which I am personally going to try to avoid this year. So the clearer you can make things for Members of Congress on an ongoing basis and get people to see what IT can do that most Members of Congress don't know at this point, I think it would be extremely helpful to us moving forward.

So thanks for what you do. I hope we didn't seem contrary today. We didn't mean to be. We just want to get these answers out in the open for everyone to understand, and we look forward to working with you as we move through this cycle.

Secretary STENBIT. Sir, we appreciate the opportunity. It is a complex subject, and it isn't easy to describe because it is too technical. I want to personally once again thank you very much for your support and your staff's support.

Last year, we had a lot of very detailed discussions. We are open to do that. We hope we don't bog down your entire system, but unless we talk about it we are not going to be able to understand exactly what your worries are. We are prepared to continue to do that, and I admire the persistence of your staff in continuing to try to learn from us and your Members as well. But we really do ap-

preciate your support because, otherwise, we couldn't be on this path. So now we are trying to figure out the best way to get there.

Mr. SAXTON. Thank you very much. The hearing is adjourned.

[Whereupon, at 5:40 p.m., the subcommittee was adjourned.]

APPENDIX

FEBRUARY 11, 2004

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

FEBRUARY 11, 2004

Statement of Chairman Jim Saxton
Subcommittee on Terrorism, Unconventional Threats and Capabilities

---

Subcommittee Hearing

"Department of Defense Information Systems Architecture: Are We on the Right Path to Achieving Net-Centricity and Ensuring Interoperability?"

February 11, 2004

Chairman: Gavel down. Brings meeting to order.

[Makes the following statement.]

Good afternoon ladies and gentlemen. The Subcommittee on Terrorism, Unconventional Threats and Capabilities meets this afternoon to learn more about each of the service's information systems architecture, how they interface with the Global Information Grid (also known as the "GIG"), and how they interoperate with one another. The Subcommittee is interested to learn more about how the GIG and each of the service's architectures will operate in a collaborative environment. We would like to know how the Department of Defense (DOD) is working to reduce redundant, non-interoperable, and stove-pipe systems, and to eliminate parochial interests to better support our nation's warfighters.

As the Department transforms itself from an industrial-age organization to an information-age one, it needs to identify the critical elements of network centric warfare, to assign roles and responsibilities for promoting it, and to describe how it will organize to implement transformational capabilities. The Subcommittee will examine Defense Transformation this year, and today's hearing begins our effort.

We wholeheartedly support the Department's goal to have joint, network-centric, distributed forces capable of rapid decision superiority and massed effects across the battlespace. However, there is much work to be done between now and achieving that objective. Realizing these capabilities will require great cultural changes in the people, processes, and military services, as well as a strategy to control DOD information systems to include managing interoperability issues among the services.

DOD's first step in creating the GIG architecture is a good foundation to build upon. The GIG is commercial-based technology that integrates legacy command, control, communications, computers, intelligence, surveillance, and reconnaissance systems, and permits full exploitation of sensor, weapon and platform capabilities for joint fires.

While the GIG's potential capabilities would be an enormous boost to supporting our warfighters, I am concerned that warfighters may not be able to tap

into these capabilities if individual service architectures limit interoperability. That is the focus of today's hearing—how are DOD and the military services designing information architectures to build a fully functioning network that every serviceman or woman may access and exploit, and how will these architectures resolve the interoperability issues that plague the services now.

There are several information systems issues that should be addressed during today's hearing. For example, how does the GIG architecture allow for the various service architectures such as the Air Force C2 Constellation, the Navy's FORCEnet, the Army's Future Combat Systems (FCS)/Warfighter Information Network—Tactical WIN-T), and the Marine Corp's Enterprise Network to function within the GIG? How do these service specific architectures interoperate with one another to provide a seamless transfer of data and communications? I am concerned that the lowest level of compliance will be the result of these endeavors, rather than maximum cooperation and collaboration between the services because of competing demands within each service.

These and other fundamental issues must be addressed as the U.S. military transforms to defeat conventional and asymmetric threats in the 21st Century battlespace. We cannot ask our young men and women to put their lives on the line if we do not provide them with the superior means and tools to perform their

duty. This is a responsibility that the Subcommittee takes very seriously, as do our witnesses, and we will continue our efforts to ensure proper oversight.

Chairman: Yields to Mr. Meehan for any opening remarks he may wish to make.

Mr. Meehan: Makes opening remarks.

Chairman: [Makes the following statement.]

We have one panel of witnesses for our proceedings this afternoon. I want to welcome our witnesses who are:

- The Honorable John P. Stenbit, Assistant Secretary of Defense for Networks and Information Integration and Chief Information Officer for the Department of Defense,
- Lieutenant General Steven W. Boutelle, (pronounced "Boo-tell") Chief Information Officer/G-6 for the Department of the Army,
- Major General Marilynn Quagliotti, (pronounced "K-wag-lot-ee") Vice Director, Defense Information Systems Agency,
- Rear Admiral Thomas E. Zelibor, (pronounced "Zel-uh-bore") Deputy for C4 Integration and Policy and Deputy Chief Information Officer for the Department of the Navy,
- Mr. David Tillotson (pronounced "Till-ot-son") III, Director, C4I, Surveillance and Reconnaissance Architecture and Assessment Department of the Air Force, and
- Brigadier General John R. Thomas, Director Command, Control, Communications and Computers (C4) and Deputy Chief Information Officer, United States Marine Corps.

Welcome, Ladies and Gentlemen. I look forward to hearing your testimony.

At the outset, I ask unanimous consent that all Members' and witnesses' written opening statements be included in the record. Without objection, so ordered.

I ask unanimous consent that all articles, exhibits, and extraneous or tabular material referred to be included in the record. Without objection, so ordered.

Secretary Stenbit, welcome. Please proceed.

Witness: Makes opening statement.

Chairman: [Yields to Mr. Meehan for the purpose of asking questions of the witnesses.]

Mr. Meehan: Asks first round of questions.

Chairman: [Upon the expiration of Mr. Meehan's time] Asks first round of questions—on next page.

Chairman: [Upon the expiration of your questions] Recognizes Members for the purpose of asking questions of the witnesses.

Discussion with the witnesses.

Chairman: [Upon the expiration of questions for the panel] Before we close, I would just like to take a moment to thank everyone for attending the Subcommittee's important oversight hearing. Thank you to the witnesses, Congressman Meehan and the other Members for participating. I would also like to thank my staff for organizing this hearing. I believe it has been a very productive and informative session.

Chairman: The subcommittee stands in recess subject to the call of the chair.

[Gavel down.]

FOR OFFICIAL USE ONLY
UNTIL RELEASED BY THE
HOUSE COMMITTEE
ON ARMED SERVICES

STATEMENT OF

JOHN P. STENBIT

ASSISTANT SECRETARY OF DEFENSE

FOR NETWORKS AND INFORMATION INTEGRATION

AND

DOD CHIEF INFORMATION OFFICER

BEFORE

THE HOUSE ARMED SERVICES COMMITTEE

TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES

SUBCOMMITTEE

FEBRUARY 11, 2004

FOR OFFICIAL USE ONLY
UNTIL RELEASED BY THE
HOUSE COMMITTEE
ON ARMED SERVICES

Mr. Chairman and Members of the Subcommittee:

Thank you for your support of our programs. I am glad to continue the many fruitful discussions we had last year about our goals, programs and progress. I am particularly pleased to appear before the subcommittee today to discuss the Department's Global Information Grid architecture, the enterprise architecture for the Department and its communications and information technology investments. In addition to articulating the vision and the basic principles underlying it, I will set the stage for the Service initiatives that will be discussed later in this hearing.

Transformation

This transformation is a key element of the Department's Defense Strategy that has been established by the Secretary to meet the challenges of the dangerous and uncertain security environment of the 21st Century. This transformation is intended to make dramatic changes in how the military fights and how the Department does business.

The military effectiveness of a network-centric capable force is significantly enhanced because of major improvements in situational awareness, interoperability, combat operations cycle time, agility, collaboration and the ability to self-coordinate. Furthermore and equally important, lives will be saved.

A recent report on Operation Iraqi Freedom highlights the importance of up-to-date, accessible information. In General Franks' words, "the *power of information has been key throughout this operation, and it is truly having the effect of saving lives*".

Today, I will provide a brief description of our vision, describe our GIG architecture and tell you how we are using this architecture to drive the three primary Departmental processes – 1) requirements, 2) budget, and 3) acquisition – to deliver an environment that supports our 21st Century mission.

The Vision

The Department's information vision is to empower users through easy access to information anytime and anyplace, with attendant security. To do this, we must provide a comprehensive information capability that is global, robust, survivable, interoperable, secure, reliable, and user driven. This is the enabling foundation for the Department's Defense Strategy.

The ultimate achievement of this vision is critically dependent on the development, deployment and integration of an effective Global Information Grid.

The Global Information Grid Architecture

The Global Information Grid or GIG is ***the organizing construct for achieving net-centric operations and warfare*** in the Department of Defense (DoD). We define the GIG as "a globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to the warfighters, policy makers, and support personnel." The GIG is a vision, an entity and an architecture.

As a vision, the GIG establishes the conceptual framework for a "to be" information environment for the DoD. This environment will provide information and

communication services vital to the effective conduct of DoD activities, be they warfighting or business in nature. It also will be the foundation for allowing the DoD to achieve its net-centric operations and warfare goals.

As an entity, the GIG comprises many systems that interoperate to provide the right information to the right places when needed. Thus the GIG will be like a private World Wide Web (WWW): many systems distributed worldwide that interoperate to allow vast amounts of information to be readily pulled by anyone or anything; anywhere, anytime; if appropriately authorized. In the same manner that the WWW is transforming industries and societies on a global scale, the GIG will support the transformation of our warfighting and business practices.

The GIG is also a well-established and documented architecture that ***is the "Department's Enterprise Architecture" that defines the*** enterprise level information environment 'blueprint'. The GIG Architecture comprises three perspectives or "views" -- operational, systems and technical. As such, the architecture represents the structure of GIG components, their relationships, and the principles and guidelines governing their design, operation and evolution over time. The responsibility for GIG development and maintenance belongs to the Assistant Secretary of Defense for Networks and Information Integration (ASD (NII)) in the Office of the Secretary of Defense.

The GIG Architecture is used to determine interoperability and capability requirements, advance the use of commercial standards, accommodate accessibility and usability requirements, and implement security requirements across the Department. The currently approved version, GIG Architecture v2.0, represents a Joint Force and Coalition Force net-centric perspective on information support to warfighting

and related operations illustrated through a set of use cases that represent the post 9-11 world in which we live; to include supporting Homeland Defense, Special Operations and Continuity of Operations. This year, the GIG Architecture and its development process were very favorably reviewed by the Government Accounting Office as part of its 2003 review of Executive Branch Enterprise Architectures, and it is being worked to align with the Federal Enterprise Architecture.

Each of the Service's major transformation initiatives; the Army's Future Combat Systems (FCS), Air Force's C2 Constellation and the Department of the Navy's ForceNet initiative are currently developing architectures that are required by the Department to be in conformance with the GIG Architecture. In addition, critical core enabling programs such as the Air Force's Transformational Communications System, and DISA's Net-Centric Enterprise Services programs must also conform to the GIG Architecture.

As a result of the work done on the GIG Architecture, the Department defined and is making progress on five programs/efforts key to the enterprise information environment: GIG-Bandwidth Expansion (GIG-BE); Transformation Satellite (TSAT); Joint Tactical Radio System (JTRS); Network Centric Enterprise Services (NCES); and Information Assurance (IA). The first three programs provide an integrated communications layer within the GIG that increases connectivity and eliminates bandwidth as a constraint while the latter two efforts provide the basic infrastructure and protection services required to effectively operate the GIG.

As a result of this work and in concert with the core DoD enterprise-wide programs, the Services are planning and implementing a number of complementary

programs required to realize the superior combat effectiveness of a net-centric environment. These programs will, in effect, provide interoperable subnets of the GIG and will, when completed, become integral parts of the GIG. You will be hearing more about these programs later.

We must extend these transformations to our allies, initially using legacy systems, but including them in our transformation as quickly as we can.

The primary means for verifying conformance is via the Department's Joint Technical Architecture (JTA) and the GIG Architecture's Net Centric Operations and Warfare Reference Model (NCOW RM).

The JTA is a minimal set of primarily commercial Information-Technology standards. These standards are used as the building codes for all systems being procured in DoD. Use of this building code facilitates interoperability between these systems and their integration into the GIG.

The NCOW RM defines in detail, the specific operational attributes, systems interfaces and technical standards profile. All Service transformational efforts and programs must demonstrate conformance with the NCOW RM and JTA in order to meet oversight requirements of the Defense Acquisition Board and the Joint Requirements Oversight Board.

The ***Business Enterprise Architecture (BEA) for the business domains was developed as an extension of the GIG Architecture*** under the direction of the DoD Comptroller, in conformance with the overall GIG Architecture. Version 2 of the GIG architecture and its BEA extension are both "to-be" architectures, that is, they describe

the DoD Enterprise of the future, and when taken together, represent a framework of requirements for transforming warfighting capabilities and business processes.

In DoD, the effective integration of architectures is enabled through the use of supporting elements such as the DoD Architecture Framework, Net-Centric Operations and Warfare Reference Model, DoD Architecture Repository System, DoD Data Strategy, Joint Technical Architecture. Several policies have been established recently requiring adherence with these GIG-Architecture supporting elements. The common approaches required by these elements will enhance our ability to integrate architectures and avoid unnecessary duplication of effort. We are incorporating these support elements across all Component architectural development efforts to ensure that the resulting products are supportive of and extensions to the GIG Architecture. Considerable progress has been made and the Department is now institutionalizing this progress through new policies and redefined processes. For example, from a policy standpoint the recently approved version of the DoD Architecture Framework is mandatory across the entire Department, and together with its companion data model, represents the integrating standard for all architecture data. From a process standpoint, the Flag and Senior Executive Service GIG Architecture Integration Panel or GAIP, led by ASD(NII), provides the primary cross component governance and integration of architectures in the DoD and among the intelligence community agencies.

The GIG Architecture Drives Departmental Processes

As previously stated, architecture is playing an increasing role in three of the Department's primary business processes: requirements, budget and acquisition. In

fact, the requirements and acquisition processes have recently been reengineered to make better use of architectures for decisional purposes.

The new requirements process, Joint Capabilities Integration and Development System (JCIDS), uses the GIG Architecture description of information technology as the authoritative view of interoperability and information assurance for use in defining Joint capabilities. The recently approved mandatory Net-Ready Key Performance Parameter (NR-KPP) increases the Department's emphasis on information assurance and data interoperability through NCOW RM in formulating specific NR-KPPs for new programs.

In the recently revised DoD Acquisition Process, the GIG Architecture is recognized as the underpinning for all mission and capabilities architectures developed by the Services and DoD Agencies. The Department also requires the development of GIG-conformant C4I Support Plans that detail information interoperability and content needs and dependencies of individual programs.

With the soon-to-be approved IT portfolio management policy, the GIG Architecture will now be used to support the Department's budget process, directly guiding the resourcing of IT investments. ***The GIG Architecture,*** along with other criteria; such as the relevance of an IT proposal to the Department's core mission, priorities, and strategic planning goals; support to functional area goals and objectives; return on investment for business initiatives; and the soundness of plans for managing, mitigating or diversifying risks will be used to define critical interrelationships among portfolios and to determine which IT investments within and across portfolios should be

supported. An intent of all architectures is to eliminate stovepiped development and redundant services and systems, thus attaining best use of taxpayer dollars.

We are particularly grateful for your support of our Horizontal Fusion portfolio and programs. These precursors to real net-centric capabilities have allowed us to test the results available when we use net-centric concepts, and the results have been so successful that we are now including in the Strategic Guidance of the Department that we will accelerate our move towards net-centric capability.

Finally, the Department is implementing a systems engineering function to ensure that programs technically comply with the GIG Architecture and its supporting elements noted above. This systems engineering activity is being complemented with a GIG end-to-end evaluation (testbed) facility. This facility will be used to ensure that systems being developed by DoD components meet GIG Architectural requirements and its associated building codes listed in the JTA.

Summary

As in all transformations, there are debates over the speed of changes and points of emphasis, but the integration of the present approaches is encouraging and producing exceptional results.

I have briefly described how a unifying set of documents is the basis for the JCS requirements process, the OSD acquisition process, and the department's budgeting process.

In the testimony that follows, you will hear how Service visions and architectures are being developed in consonance with, and as extensions to. the GIG Architecture.

The Department's vision, architecture and supporting elements and policies are providing the unifying thread for each Service. Building from a common architectural foundation, the systems that the Services are acquiring will become part of the GIG as they are developed and delivered.

This IT work is greatly increasing our nation's ability to conduct effective, responsive operations. Our capabilities are being strongly enhanced because of major improvements in situational awareness, Joint Force interoperability, reductions in operational cycle times, ability to dynamically and continuously plan operations, ability to perform effects-based operations and ability to rapidly adapt to battlefield conditions. And, perhaps most importantly, as we've learned again in Iraq, better access to information means fewer casualties.

I would like the thank the Chairman and members of the Committee for their past support, and I am sure my successor looks forward to working with you and other members of Congress in the coming year as we strive to meet the challenges of achieving net-centric operations. Thank you for this opportunity to share our progress with you.

NOT FOR PUBLICATION UNTIL RELEASED BY THE
SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND
CAPABILITIES, HOUSE ARMED SERVICES COMMITTEE
U.S. HOUSE OF REPRESENTATIVES

WRITTEN STATEMENT OF

MAJOR GENERAL MARILYN QUAGLIOTTI, U.S. ARMY
VICE DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

BEFORE THE
SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND
CAPABILITIES
HOUSE ARMED SERVICES COMMITTEE

Wednesday
11 February 2004

NOT FOR PUBLICATION UNTIL RELEASED BY THE
SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND
CAPABILITIES, HOUSE ARMED SERVICES COMMITTEE
U.S. HOUSE OF REPRESENTATIVES

2/10/04 12:54 PM

STATEMENT FOR THE RECORD
MAJOR GENERAL MARILYN A. QUAGLIOTTI
DEFENSE INFORMATION SYSTEMS AGENCY
BEFORE
THE HOUSE ARMED SERVICES COMMITTEE
TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES
SUBCOMMITTEE

Prepared Statement of Major General Marilyn A. Quagliotti, United States Army, Vice Director, Defense Information Systems Agency, before the House Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, Washington, D.C., February 11, 2004.

Thank you, Mr. Chairman and members of the Subcommittee, for this opportunity to testify before your Subcommittee on Terrorism, Unconventional Threats and Capabilities. I am Major General Marilyn A. Quagliotti, United States Army. I am the Vice Director of the Defense Information Systems Agency.

The Defense Information Systems Agency (DISA) is responsible for building, operating and protecting joint command, control, communications and computer (C4) capabilities to help catalyze and sustain the Department of Defense's (DoD) transformation from platform-centric to network-centric operations. We are the preferred provider of Global Net-Centric Solutions for the Nation's warfighters and all those who support them in the defense of the Nation. In effect, we are one of the principal executers and integrators of the DoD Global Information Grid Architecture, based on guidance from the Assistant Secretary of Defense, Networks and Information Integration (ASD NII). DISA directly supports three of Secretary Rumsfeld's critical operational goals expressed in the Quadrennial Defense Review. Those goals – assuring information systems; providing persistent surveillance, tracking and rapid-engagement with high-volume precision

strikes; and leveraging information technology and innovative concepts to develop an interoperable joint C4ISR architecture and capability – will be made possible by the underlying support of a Global Information Grid (GIG).

It is our strong belief that in order to reach the Quadrennial Defense Review goals, net-centric transformation is central to our success. The DoD Chief Information Officer (CIO) has established a DoD Global Information Grid architecture; it is the blueprint that we are using to define key DISA-provided transformation components. DISA is deploying an innovative communications infrastructure – the Global Information Grid-Bandwidth Expansion (GIG-BE) – that will begin to reduce bandwidth as a constraint in future wars. We plan to deliver this high bandwidth capability to 10 sites this year. DISA continues to deliver the DoD Teleport, which extends significant multi-band and multimedia connectivity to deployed forces. The Department's joint command and control (C2) system of record, Global Command and Control System-Joint (GCCS-J), and the Global Combat Support System, Combatant Command/Joint Task Force (GCSS [CC/JTF]) provide end-to-end information interoperability across and between C2 and Combat Support (CS) functions. Finally, another important transformation initiative, Net-Centric Enterprise Services, will provide a common set of information capabilities across the Global Information Grid, allowing DoD, the intelligence community, and coalition partners to pull information they want, whenever they need, from wherever they are – within appropriate constraints.

Operations Enduring Freedom and Iraqi Freedom were opportunities to put new warfighting capabilities into action, and allowed DISA to demonstrate wonderful success with our

initiatives. It is important to continue to maintain net-centric capabilities for our warfighters, today and in the future. For that reason, I stand before you today.

In 1999 and 2000, the Department's NII (formerly C3I) and J-6 Joint Staff conducted a mission analysis. The analysis was sent to Congress as a report in 2001. The results of the analysis defined what would be necessary for the Department to conduct network-centric warfare. Net-centric warfare requires an end-to-end coherent network. We don't have that network today, but we do have a vision and that vision is a key part of the Global Information Grid (GIG). The vision and attributes of the this network are as follows: A single, secure grid that provides seamless, end-to-end capabilities to all warfighting, national security and support users; support to the Department and intelligence community's requirements from peacetime business support through all levels of conflict; joint, high-capacity netted operations; coherent cross-service command and control integrated with weapons systems; support to strategic, operational. tactical and base/post/camp/station levels; "plug and play" interoperability guaranteed for the United States and its allies; mediated connectivity for coalition users; and information on demand and "Defense in Depth" against all threats. Since that time, the Department has worked to achieve protected, assured and interoperable communications.

If we are to create a Global Information Grid that provides net-centric operations, DISA must address two major strategic challenges. First, we need to operationalize our networks –that is, organize the force to support and view the networks as warfighting resources, such that this becomes an integrated part of our warfighting command structure. Second, we need to solve interoperability problems that prohibit successful joint mission execution. By only addressing

technical issues, we will not achieve the end state of network-centric warfare. The framework for change includes: doctrine, organization, training, materiel, leaders, personnel, facilities, culture, resources and processes (DOTMLPF & CRP). Actions must be accomplished in each of these areas for network-centric warfare to become a reality.

DISA has now been given new opportunities to take on large acquisition activities in the joint arena for the Department. To facilitate these new opportunities, we have created a full-time Component Acquisition Executive (CAE) responsible for not only the content or the technical reviews of all of our programs, big and small, but also all of the program review materials. This function deals with large-scale acquisition activities we have underway -- GIG-Bandwidth Expansion and Net-Centric Enterprise Services. This function will provide DoD a joint acquisition organization dedicated to meet Joint Forces Command and Joint Staff requirements for joint programs.

With the Congress' help, we have achieved significant materiel advances. This year, the GIG Architecture and its development process were very favorably reviewed by the General Accounting Office as part of its 2003 review of the Executive Branch Enterprise Architectures, and it is being worked to align with the Federal Enterprise Architecture. Following ASD NII's lead with their architectural standards, DISA is working hard to achieve network-centric solutions.

Global Information Grid-Bandwidth Expansion

Given that the architecture is based on the exploitation of the benefits of net-centricity, it is envisioned that Global Information Grid-Bandwidth Expansion (GIG-BE) is the first step towards

creating a ubiquitous "bandwidth-available, anyone-to-anyone" environment to improve national security intelligence, surveillance, reconnaissance, command and control information sharing. The program will provide increased bandwidth and diverse physical access to between 90 and 100 critical sites in the Continental United States (CONUS), Pacific, European and Southwest Asian Theaters.

GIG-BE will provide a secure, robust, optically switched terrestrial network delivering very high speed classified and unclassified Internet Protocol (IP) services. In addition, the GIG-BE will be configured with equipment necessary to facilitate optimization around the GIG-BE high-speed infrastructure of DoD's existing communications infrastructure, the Defense Information Systems Network (DISN).

The GIG-BE program has progressed from concept to Milestone C in little over one year. The program is on schedule to reach Initial Operational Capability in September 2004 and Full Operational Capability in September 2005.

Teleport

The DoD Teleport System is the upgrade of telecommunications capabilities at selected Standardized Tactical Entry Point (STEP) sites. The system provides deployed forces with sufficient interfaces for multi-band and multimedia connectivity from forward-deployed tactical locations, enabling direct reachback to multiple command, control, communications, computer and intelligence (C4I) systems. The Teleport system facilitates operational flexibility and interoperability between multiple deployed combat elements, providing a direct access link from

small unit teams to a Combined Task Force (CTF), Battle Group (BG), or Air Expeditionary Force (AEF). It allows the commander to conduct split-based operations when necessary, pushing combat units forward to remote areas, and leaving databases and higher headquarters behind. For example, CENTCOM Headquarters commanded and controlled Special Operations units operating in Afghanistan during Operation Enduring Freedom. Based on a technical, flexible approach, the DoD Teleport system continues to rapidly evolve in response to warfighter needs.

Global Command and Control System-Joint (GCCS-J)

GCCS-J is DoD's joint C2 system of record. Operational at over 650 sites worldwide, GCCS-J is an essential component for achieving the full spectrum dominance articulated in Joint Vision 2020 by enhancing information superiority, and supporting the operational concepts of full-dimensional protection and precision engagement. Built upon the Common Operating Environment (COE) infrastructure, GCCS-J integrates C2 mission applications, databases, Web technology and office automation tools. It provides an open system architecture that allows a diverse group of mission applications/systems and commercial-off-the-shelf software packages to operate at any GCCS-J location. GCCS-J offers "plug and play" access to the joint and service systems that joint warfighters use to plan, execute and manage military operations, and it eliminates the need for inflexible. duplicative, stovepipe C2 systems.

GCCS-J allows the Commander-in-Chief, Secretary of Defense, National Military Command Center, Combatant Commanders, Joint Force Commanders, and Service Component Commanders to maintain dominant battlefield awareness through a fused, integrated, near real-time picture of the battlespace by synchronizing the actions of air, land, sea, space and special

operations forces. GCCS-J provided USCENTCOM critical capability that was key to the successful execution of the Global War on Terrorism. The use of GCCS-J during these military operations supported our ability to track blue and red forces, shortened decision cycles, increased operational flexibility, provided near-time common shared views across services at all echelon, supported in-air targeting based on shared intelligence information, and reduced fratricide.

Global Combat Support System, Combatant Command/Joint Task Force (GCSS (CC/JTF)

GCSS (CC/JTF) provides end-to-end information interoperability across and between Combat Support (CS) and C2 functions. This system integrates CS information into overall situational awareness, encouraging collaboration of logisticians with operators, and resulting maintenance of high tempo battle rhythms. In addition, GCSS (CC/JTF) significantly increases access to critical personnel and medical information, providing direct support to field operations. It is fielded both as a GCCS-J mission application, and as a stand-alone capability directly accessible to combat support operators.

Net-Centric Enterprise Services (NCES)

As I already mentioned, our networks are constantly being modified, upgraded and improved to better support the warfighter. This presents a unique challenge, not only to our research and development organizations, but also to our system's operators and users. This constant change requires a networked capability that is not only flexible and expandable, but designed to meet current and future threats. Part of our new organizational structure is an end-to-end engineering organization and several specific major program offices that are responsible for engineering, developing, acquiring and fielding portions of the GIG.

Net-Centric Enterprise Services (NCES) will provide enterprise level information technology (IT) services and infrastructure components for the Global Information Grid. It will provide a common set of interoperable information capabilities to the warfighter which will (1) support posting of data to shared spaces; (2) provide users with the capability to pull whatever data they need, whenever they need it, from wherever they are; and (3) provide information assurance. NCES will increase warfighter flexibility, improve the quality and timeliness of DoD decision cycles, and enhance business operations. Stove-piped department and/or service-specific enterprise level legacy programs will be replaced by or migrated to the consolidated infrastructure built upon NCES capabilities. The end result will be the enterprise-level integration of IT systems, in both warfighting and business domains, in an interoperable, net-centric operating environment. NCES supports DoD's transformation goals to achieve rapid decision superiority, streamline business processes, conduct effective and discriminating information operations, and provide the joint force shared situational awareness.

NCES transforms legacy planning and execution capabilities into protected, Web-based, real-time collaborative business processes, including Joint and Coalition information exchanges across organizational boundaries. It supports real-time battle management and operations by providing a user-defined operational view of the battle space. NCES meets the military requirement to provide dramatically improved situational awareness, robust alerting, shortened decision cycles and shared understanding.

The integration of NCES capabilities will provide a consolidated, services-based IT infrastructure. The NCES acquisition strategy seeks to reduce overall costs and time to deploy IT systems supporting day-to-day business and warfighter operations through consolidation, centralization/regionalization, and retirement of legacy systems. The NCES services-based architecture approach eliminates costly legacy interfaces between disjointed, disparate and stove-piped systems by providing a comprehensive set of core enterprise services.

Information Assurance (IA)

In this era of asymmetric network warfare, we clearly need to understand the threat to our networks, how our networks can be attacked, and how we will respond to an attack. DISA's information assurance (IA) work is focused on assuring DoD mission execution by providing essential computer operational, procedural, and technical services and standards to DoD. All of these IA services are vital to DoD reliance on "the net" for warfighting and warfighting support.

Over time, we have learned that we must be proactive in our defense and operationalize our networks. We must balance the risk of attack against the needs of the mission. We have to integrate network defense and network management with the operational use of the network. To this end, we have developed equipment, configurations, processes and procedures that make up our IA initiatives.

DISA is patrolling the gateways between DoD and the Internet by designing and operating perimeter protections and attack detection at these gateways. DISA ensures that each network component is remotely managed in a secure way, and that signaling among components is

secured. DoD follows DISA-provided standards for the proper use of infrastructure mechanisms like the domain name system (DNS) and the Border Gateway Protocol (BGP). DISA is also pursuing DoD-wide efforts to further harden the DoD DNS by developing and pursuing a joint plan for a DoD-wide DNS security standard. These protections and standards apply to the current Defense Information Systems Network (DISN) as well as to the emerging GIG-Bandwidth Expansion network. DISA and DoD's contributions to hardening the DNS have also benefited the robustness of the Internet itself.

IA will be included in an integrated concept called Network Operations (NetOps). Under the NetOps concept, DoD is professionalizing and normalizing the operation, management and control of the GIG under the leadership of United States Strategic Command (USSTRATCOM). DoD, DISA and industry partners have all teamed together to acquire and provide enterprise-wide solutions to the threats and vulnerabilities we face, now and in the future.

IA is a team effort that stretches across government and industry. Major General J. David Bryan, former Vice Director of DISA and current Commander of Joint Task Force-Computer Network Operations (JTF-CNO), works closely with USSTRATCOM, which runs the JTF-CNO – located in DISA's headquarters building. The DISA operational infrastructure, as well as those of the military services and the JTF-CNO, work closely together to ensure disciplined DoD network operations and computer network defense.

In order to support this new NetOps structure, we have transformed the way we do end-to-end operations. DISA will oversee the NetOps mission through our new GIG Operations element.

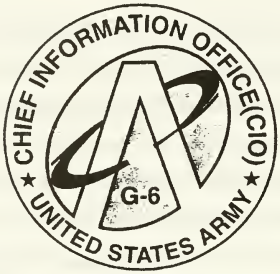
As such, the USSTRATCOM staff portions of the JTF will be fully integrated with the DISA network operations and defense staff, so that the GIG can be monitored 24-hours a day, and that operations and defense decisions can be made and implemented quickly and effectively.

The Department, as a whole, has come a long way towards solving the interoperability problem, and we continue in those efforts. DISA plays a key role. The Joint Capabilities Integration and Development System (JCIDS) analysis is a process developed by the Joint Staff, Office of the Secretary of Defense and the Joint Forces Command, focused on achieving joint operational capabilities rather than on individual systems. It is composed of a structured, four-step methodology that defines capability gaps, capability needs, and approaches to provide those capabilities within a specified functional or operational area. Based on national defense policy and centered on a common joint warfighting construct, the analyses initiate the development of integrated, joint capabilities from a common understanding of existing joint force operations and doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF) capabilities and deficiencies.

DISA's role in this process is to ensure that the Joint Interoperability Testing Command (JITC) is resourced, and has the requisite talent to run interoperability testing so that service systems are compliant with joint standards. JITC ensures that the products acquired and built by DISA and the services meet appropriate DoD security standards through C4 and security certifications.

Summary

I believe we are on the right path to achieving net-centricity. However, we face cultural, organizational and leadership challenges of a complexity we have never seen before. With the materiel solutions identified and funded, we expect information on demand to help us achieve our end-state goal of net-centric warfare. DISA exists to provide the net-centric capabilities to our Nation's warfighters and defense professionals who are regularly called on to execute any type of operation, from full-scale conflict such as Operation Iraqi Freedom to small scale contingencies anywhere in the world. We are one of the principal executors and integrators of DoD's GIG Architecture. Results of these efforts have proven their efficacy through Operations Enduring Freedom and Iraqi Freedom. The DoD IT challenges are considerable, but we continue to move forward on our leadership's vision. We are committed to providing cost-effective, worldwide, robust, secure, joint and interoperable C4 architecture and capabilities that are essential to our national security. Mr. Chairman, members of the Subcommittee, again, thank-you for the opportunity to appear before your subcommittee.



STATEMENT BY

LTG STEVEN W. BOUTELLE
CHIEF INFORMATION OFFICER/G-6
UNITED STATES ARMY

BEFORE THE
SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL
THREATS AND CAPABILITIES
COMMITTEE ON ARMED SERVICES
UNITED STATES HOUSE OF REPRESENTATIVES
SECOND SESSION, 108TH CONGRESS

ON DEPARTMENT OF DEFENSE INFORMATION SYSTEMS
ARCHITECTURE AND INTEROPERABILTY

FEBRUARY 11, 2004

NOT FOR PUBLICATION UNTIL RELEASED BY
THE COMMITTEE ON ARMED SERVICES
UNITED STATES HOUSE OF REPRESENTATIVES

STATEMENT BY
LTG STEVEN W. BOUTELLE

ON DEPARTMENT OF DEFENSE INFORMATION SYSTEMS ARCHITECTURE AND INTEROPERABILITY

Mr. Chairman and members of the subcommittee, thank you for the opportunity to provide testimony on Department of Defense information systems architecture and interoperability.

Today, we are an expeditionary Army supporting our Nation in the Global War On Terrorism. Our Army is in the midst of a massive reorganization creating modular fighting units that can be rapidly deployed around the world. Our forward deployed forces must have capability to reach back from anywhere on the globe through global networks to tap intelligence resources and collaboration tools on a real-time basis. Our forces will continue to deploy as an integral part of a Joint force and often as a part of a coalition team as we continue the fight against a global terrorist network.

As a Joint or Coalition expeditionary force, interoperability is not an option. Existing systems must be interoperable or made interoperable. All new systems must be developed with Joint interoperability and interdependencies as Key Performance Parameters. The good news is that our services have achieved much interoperability today. Many of our communications systems and networks are based on the same commercial Internet Protocol (IP) that served as the foundation for the World Wide Web. This is a mandated standard of the Department of Defense's Joint Technical Architecture. This, and other commercial based information technology protocols and standards are a foundation for achieving Joint, interagency, and multi-National (JIM) interoperability. The Army has nearly completed the migration to an IP-based network as part of the larger Joint Network. In accordance with the Joint Technical Architecture and current DoD guidance, we are moving to IP version 6.0 for a more efficient and effective network. In practical terms, interoperability exists today at the network level and extends through space-based and terrestrial transmission systems. These transmission systems serve as part of the Global Information Grid (GIG) supporting users around the world. The DoD GIG Data

Strategy directs a more complete migration to commercial web-based technologies, which will further strengthen interoperability across the Joint, interagency, and multi-national environment.

Network level interoperability is vital to all organizations within the DoD. An example of this type of interoperability is a user with an Apple computer sending email to a user with an IBM computer. Both computers have different operating systems and probably different email programs, and the network is comprised of piece parts from many manufacturers such as Sun, Cisco, IBM, and Microsoft. However, common and enforced standards, such as those that reside in the Joint Technical Architecture, ensure your email transits the mix of equipment and is successfully delivered. An example of the military application of network interoperability is the Joint Blue Force Situational Awareness, or Blue Force Tracking, implemented in Operation Enduring Freedom and Operation Iraqi Freedom. While each service used different platforms and computers to track Blue (friendly) Forces, the Network interoperability standards enabled commanders on the ground to enjoy near-real-time visibility of friendly forces on dissimilar systems from individual trucks, tanks, helicopters, command centers and even here in the Washington area.

Our Army and DoD continue to expand the network interoperability of all of our programs. We continue upgrading individual platform interoperability based on the standards of the JTA. The bottom line is that while we have interoperability between the services now, it will be even more pervasive and richer in the future. Additionally, we are committed to working with OSD to ensure the GIG aligns with the Federal Enterprise Architecture (FEA).

As the Army transforms to the Future Force, we are developing lighter, highly mobile, more modular, and strategically responsive organizations fully enabled by a more robust network of satellites, fiber optic cables, radios, and tactical communication system. Battle Command capabilities, tied together by these enhanced networks will be the bridge from Current to Future Forces and enable the Expeditionary Joint Forces Commander to fully conduct interdependent, globally dispersed, network-centric warfare. Battle Command is the essential operational capability that fundamentally enables the global conduct of future Joint operations. Our Chief of Staff has seventeen focus areas; one of these is networks. As we realign into modular units, we are adjusting the architecture of these units to exploit the success we saw in Operation Enduring Freedom

and Operation Iraqi Freedom and to align with the Joint Technical Architecture. We are now in fact restructuring the Third Infantry Division at Ft. Stewart, GA, which has recently returned from Iraq. We are redesigning this unit to be flexible, adaptive, and Joint.

Systems such as the Joint Tactical Radio System, Warfighter Information Network – Tactical, Strategic Tactical Entry Point, Teleport, and Global Information Grid – Bandwidth Expansion are essential to support warfighters with secure, simultaneous real-time voice, data, imagery, and video globally.

The Joint Tactical Radio System (JTRS) is the next generation radio. This system changes the construct for radio hardware by relying on software to change frequencies and waveforms. In addition to increased ease of interoperability, a common family of radio systems across the Department allows for savings in development and procurement costs. JTRS represents Joint communications at its purest form. It is a fully integrated and fully interoperable system combining the best of multi-service programmatic, technology, and operational experience and leadership while taking advantage of economies of scope and scale for development. This high-capacity,

software-programmable family of radios is multi-band/multi-mode capable and will provide simultaneous voice, data, and video communications enabling it to support the worldwide Joint mission tasks. It also lays the foundation for achieving network connectivity across the frequency spectrum and provides the means for digital information exchanges, both vertically and horizontally, between Joint warfighting elements. It represents a key part of success for our future warfighter and Joint teams.

The Warfighter Information Network – Tactical (WIN-T) is absolutely essential in our expeditionary Army. WIN-T will serve as the Army's communications network for the future warfight, replacing the Army's twenty-five year old tactical communications system, Mobile Subscriber Equipment (MSE). WIN-T leverages the rapid growth of commercial communications technologies we all enjoy, and brings those technologies on to the modern battlefield. This will allow the Army to fully use enhanced services such as high-resolution imagery, operations on the move, and collaborative tools across the battlefield. WIN-T represents the Army's requirement to be born Joint, is a mission critical system, and is an integrating communications network that brings next generation communications to the Joint Warfighter.

Based on DoD's Joint Technical Architecture, it is optimized for offensive and Joint operations, while providing the Theater Combatant Commander the capability to perform multiple missions simultaneously and still maintain campaign quality.

The Army's flagship transformation program, the Future Combat Systems (FCS), is a networked "system of systems" that uses advanced communications and technologies to integrate the soldier with "families" of manned and unmanned platforms and sensors. The FCS network is composed of various communications nodes supported by UAVs (Unmanned Aerial Vehicles) and UGVs (Unmanned Ground Vehicles). The FCS is a distributed network centric system leveraging WIN-T to allow reach back through STEP sites, Teleport, and the GIG-BE to critical war fighting resources. This highly agile and lethal force will provide the tactical formations required to fulfill the Army's vision for its future force.

The Satellite/Teleport/STEP are currently, and will remain, a linchpin for the war on terrorism. Our Nation's military relies on this information projection capability to link intelligence sources with commanders allowing collaborative planning and execution worldwide

on a real-time and virtually instantaneous basis. We actively participate in the Joint Satellite Communications Acquisition Council with our sister services, OSD, and Joint partners. Additionally, the Army meets with ASD(NII) Senior C4 representatives to discuss emerging satellite communications architecture and technology insertions to gain synergy and ensure the Army architecture is thoroughly aligned with the other services and Combatant Commands.

Upgrading select STEPs to Teleports is another extremely important program. Selected Strategic Tactical Entry Point (STEP) sites that currently access only military satellites are upgraded with additional satellite terminals operating in commercial Satellite Communications (SATCOM) and radio bands. This capability greatly increases our ability and flexibility to support the warfighters deployed globally. This is currently funded to take place in three generational upgrades from FY 03 through FY 08.

The Army is actively involved in synchronizing its information systems architecture. The Joint Tactical Radio System, the Warfighter Information Network – Tactical, Strategic Tactical Entry Points, and

Teleport are all being developed in conjunction with guidelines from the Joint Technical Architecture and OSD, which continues to provide adequate oversight. Our Nation is in the midst of a global fight on terror. The relevant and ready Army functions as the country's expeditionary force of power. The future success of the Army depends upon its ability to transform within a fully integrated Joint environment and we cannot afford to delay that transformation. The Army's C4 and information technology transformation is the enabler for an Army at War and transforming. With the continued support of Congress, we will achieve our goal of an integrated net-centric, knowledge-based Future Force that functions as an integral part of the Joint warfight. Our Nation requires a relevant, ready, Joint and integrated Army capable of winning the Nation's wars.

NOT FOR PUBLICATION UNTIL
RELEASED BY THE
HOUSE ARMED SERVICES COMMITTEE

STATEMENT OF

RADM THOMAS E. ZELIBOR, USN

DEPUTY FOR C4 INTEGRATION AND POLICY

DEPARTMENT OF NAVY DEPUTY CIO FOR NAVY

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS

AND CAPABILITIES

ON

11 FEBRUARY 2004

CONCERNING

DEPARTMENT OF DEFENSE INFORMATION SYSTEMS ARCHITECTURE: ARE WE ON

THE RIGHT PATH TO ACHIEVING NET- CENTRICITY AND ENSURING

INTEROPERABILITY?

US NAVY INFORMATION TECHNOLOGY (IT) ARCHITECTURE: FORCEnet

NOT FOR PUBLICATION UNTIL
RELEASED BY THE
HOUSE ARMED SERVICES COMMITTEE

Introduction

Mr. Chairman and distinguished members of the Terrorism, Unconventional Threats and Capabilities Subcommittee, thank you for this opportunity to appear before the committee to discuss the Navy's Information Technology (IT) architecture framework, called FORCEnet, and how we are interfacing with the Department's Global Information Grid (GIG) initiatives as well as the other Services' and Federal IT architectures.

Background

What is FORCEnet?

FORCEnet is the Navy and Marine Corps' means of operationalizing the concepts of network centric warfare. Within Sea Power 21, the Chief of Naval Operations defines FORCEnet as the operational construct and architectural framework for naval warfare in the Information Age that integrates warriors, sensors, networks, command and control, platforms and weapons into a networked, distributed combat force, scalable across the spectrum of conflict from seabed to space and sea to land. FORCEnet is not a program, but the forcing function for organizing, planning and investing in Navy's IT and tactical information architecture. The Department of Defense (DoD) and the other Services are working towards the same end-state. Under the leadership of Assistant Secretary of Defense for Network and Information Integration (ASD (NII)), the Services and Agencies are working together to develop a consistent set of information technology policies, strategies, architectures and standards across the DoD.

Architecture

Instead of developing our own architectures and standards from the ground up, Navy is participating fully in the DOD's architecture and standards development process to ensure Navy improves interoperability amongst joint forces. For example, at the OSD level, Navy participates in the Assistant Secretary of Defense for Network and Information Integration (ASD (NII)) Global Information Grid (GIG) Architecture development; and at the joint level, Navy participates in the Joint Forces Command (JFCOM) chartered Cross-Service Architecture Integration Working Group. Within the construct of a Joint Task Force, the JFCOM working group defines and develops the Joint Command and Control (JC2) architecture for DOD. Thus, the FORCEnet architecture is based on GIG architecture development, and is the Navy's instantiation for implementing seamless integration across multiple domains.

The GIG Architecture is "a globally interconnected end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel." The GIG has become the organizing construct for achieving net-centric operations and warfare across the DOD. The GIG includes both warfighting and business domains. Likewise, we are working to integrate our tactical and warfighter support domains in an overarching Department of Navy Enterprise Architecture, of which FORCEnet is a key component.

Navy is strongly engaged in and influencing the development of key GIG Architecture components so that we can leverage "born joint" architectures. For example, Navy fully participates in the development of (a) Transformational Communications Architecture (TCA), transforming future satellite communications; (b) the Global Information Grid – Bandwidth Expansion (GIG-BE), bringing high data rate connectivity to worldwide bases and facilities;

(c)Teleports , that connects current and future satellite communications architectures and terrestrial networks; (d)Joint Tactical Radio System (JTRS) that will provide a family of interoperable radios to enable joint tactical communications; (e) GIG Enterprise Services (GES)/Net-Centric Enterprise Services (NCES) that brings an enterprise perspective to DOD application and information handling processes; (f) Information Assurance (IA) initiatives, providing secure interoperable networks; and (g) Internet Protocol Version 6 implementation, that will provide added security and quality of service for our communications.

Challenges

Maintaining legacy architectures while defining future architectures and then investing to migrate to those future architectures is the major challenge. The Navy's challenge continues to be synchronizing the integration of our existing systems into joint architectures while ensuring we remain connected to our allies and coalition partners as well as Homeland Security Agencies, such as the Coast Guard. For example, Navy is working the migration of our legacy satellite communications (SATCOM) systems into the Transformational Communications Architecture (TCA) for satellite communications. Navy fully participates in TCA development and will leverage TCA based systems to meet our forecasted SATCOM needs. Our requirements were consolidated with other Services and intelligence agencies to ensure there is a joint perspective on future satellite communications services. The process to achieve this architecture works well and the TCA represents a DoD, Intelligence Community and NASA approved satellite communications architecture. This joint approach is a first in the satellite communications business.

We are exploring the integration of tactical and non-tactical networks as we take a holistic perspective on optimizing warfighting capabilities. Afloat and ashore IT architectures must be

seamlessly integrated and interfaced so that units transiting from East or West Coast ports to overseas locations can operate jointly. We are in the process of developing an integrated roadmap for both tactical and non-tactical networks such as our overseas Base Level Information Infrastructure (BLII), our CONUS based Navy Marine Corps Intranet (NMCI), and our afloat networks. Perhaps a simple analogy might serve to illustrate the Navy's role in GIG Architecture development. GIG initiatives like the GIG-Bandwidth Expansion could be viewed as the National Interstate Highway System. The Federal Government builds the Interstate Highway System in coordination with the States, while the States build roads that connect to the Interstate Highway System. All users of this highway system employ the same traffic signals and signs for interoperability. FORCEnet builds "Navy" roads to the "GIG" interstate, using common standards for interoperability such as the Joint Technical Architecture (JTA). Additionally, we use and enforce a FORCEnet Compliance Checklist to ensure that all Navy programs are FORCEnet and GIG-compliant.

Experimentation, demonstration and testing are also important activities for determining architecture development and Navy is conducting a series of operational demonstrations called Trident Warrior in coordination with the other Services. These operational demonstrations help in the accelerated innovation, assessment, and fielding of warfighter capability. Navy is hosting the ASD (NII)-sponsored Global Information Grid/Transformational Communications (GIG/TC) Testbed at the Navy Research Lab (NRL). The GIG/TC Testbed will connect the FORCEnet Testbed with other Service and Agency testbeds for the purpose of conducting end-to-end testing on all GIG-compliant systems as those systems are developed.

Summary

In summary, Navy remains heavily engaged with ASD (NII) and the other Services and Agencies in creating a joint, interoperable GIG Architecture. Through agreed upon standards and business processes, we are breaking down traditional stovepipe approaches and working towards achieving joint and coalition interoperability. Furthermore, we are migrating towards enterprise solutions across the Navy and the DoD to deliver information to the warfighter. With your continued strong support, our military has made significant progress improving our joint warfighting and business capabilities, and transforming our military into a 21st Century fighting force. We appreciate your efforts to help us be responsive to a changing world, and in supporting the warfighters that make the world a safer and better place. Thank you for this opportunity to address the committee on this important issue.

NOT FOR PUBLICATION
UNTIL RELEASED BY
THE HOUSE ARMED
SERVICES COMMITTEE

STATEMENT OF

BRIGADIER GENERAL JOHN R. THOMAS

DIRECTOR, COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTERS

HEADQUARTERS, UNITED STATES MARINE CORPS

AND

DEPARTMENT OF THE NAVY

DEPUTY CIO FOR USMC

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES

CONCERNING

DOD INFORMATION SYSTEMS ARCHITECTURE: ARE WE ON THE RIGHT PATH TO ACHIEVING NET-CENTRICITY & ENSURING INTEROPERABILITY?

ON

11 FEBRUARY 2004

NOT FOR PUBLICATION
UNTIL RELEASED BY
THE HOUSE ARMED
SERVICES COMMITTEE

I. INTRODUCTION

Mr. Chairman and distinguished members of the Terrorism, Unconventional Threats and Capabilities Subcommittee, thank you for this opportunity to appear before the committee to discuss the Marine Corps involvement in the Department of Defense systems architecture and how we are using enterprise architecture to obtain the information technology capabilities for our forces in the 21st Century.

Today's operating environments are defined by joint and coalition operations. Now more than ever, we must stress interoperability in all of our warfighting endeavors, and reflect integration and interoperability in every information technology program. As an integrated combined arms task force, the Marine Corps operates closely with the Army, Navy and Air Force across a variety of missions and mission areas. Synchronizing the Marine Corps architecture with naval, joint, and DoD architectures for joint interoperability is a paramount effort. As the Director, Command, Control, Communications and Computers (C4), I am committed to ensuring that the Marine Corps is equipped with jointly interoperable IT capabilities, leveraging all joint and transformational programs, to support our Marines.

I would like to address how the Marine Corps is synchronizing our IT enterprise with the Department of Defense architecture—the Global Information Grid—and our naval architecture—FORCEnet. I would also like to share with you our involvement with governance activities required to manage the dynamics of this synchronization.

II. ARCHITECTURE SYNCHRONIZATION

The maritime expeditionary nature of the Marine Corps, together with experiences from Operation Enduring Freedom (OEF) and Operation Iraqi Freedom (OIF), reinforces the principle that we must emphasize jointness in our operational mindset and in the systems we acquire. To that end, our IT enterprise must not only be internally consistent and interoperable, it must also be interoperable with the rest of the Department of Defense (DoD). My primary focus in acquiring and managing IT capabilities for the Marine Corps is approving programs conforming to DoD, joint warfighting, and naval architectures. We must ensure our enterprise is leveraging the IT capabilities contained in these architectures.

The Global Information Grid (GIG) is the Department of Defense (DoD) framework for achieving net-centric operations and warfare (NCOW). The GIG refers to the collection of processes, personnel, systems, networks, technologies, and standards needed to guide transformation to a net-centric environment. The GIG supports warfighting domains and business domains through an enterprise infrastructure consisting of common computing capabilities and IT services. DoD is developing the GIG to be in accord with the Federal Enterprise Architecture (FEA). The FEA is a collection of interrelated models to facilitate cross-agency analysis to promote collaboration within and across Federal Agencies. The GIG is DoD's enterprise architecture that establishes the standards for the Components, Services and Agencies.

FORCEnet is the Department of the Navy's component of the GIG. FORCEnet is the operational and architectural framework for transformational capabilities for naval warfare being pursued by the Naval Services. FORCEnet is at the intersection of the

Chief of Naval Operations concept for Sea Power 21—Sea Strike, Sea Shield, and Sea Basing; and the Commandant's concept for Expeditionary Maneuver Warfare (EMW)—Ship-to-Objective Maneuver and Sustained Operations Ashore. Both the Navy and Marine Corps are currently working to identify the essential C2 and IT capabilities of FORCEnet.

The Marine Corps Enterprise Network (MCEN) is the Marine Corps component of FORCEnet and the Global Information Grid (GIG). MCEN is our enterprise framework for IT. The MCEN supports all information exchange requirements for Marine warfighters and our Supporting Establishment. It is our end-to-end IT capability and infrastructure spanning both our warfighting and business domains. To be jointly interoperable, our MCEN must be able to seamlessly interface with other Services, with Combatant Command and Joint headquarters, and with the rest of the DoD. MCEN, as part of the broader FORCEnet architecture, connects the garrison, maritime, and expeditionary infrastructures vital for sharing information with all Marines.

Marine Corps transformation to a net-centric force is inextricably linked to the evolution of FORCEnet and the GIG. As both evolve, we are co-evolving our MCEN architecture and adjusting our underlying programs to leverage transformational capabilities—GIG Bandwidth Expansion (GIG-BE), Transformational Communications (TC), Joint Tactical Radio System (JTRS), Net-Centric Core Enterprise Services (NCES), and Information Assurance (IA).

A critical enabling initiative for the Marine Corps in this net-centric transformation is the Marine Corps Enterprise Information Technology Services (MCEITS). MCEITS is our framework for realigning, collapsing, and consolidating our

IT environment. MCEITS represents a new environment for integrated net-centric enterprise information services. It realigns the Marine Corps environment of applications, databases, networks, and facilities into an integrated, layered architecture for delivery of capabilities based on a common infrastructure and shared services. MCEITS will leverage capabilities from the GIG NCES program, and the Navy-Marine Corps Intranet performance-based contract. MCEITS supports IT portfolio management, and addresses technology, processes, standards, workforce, and governance satisfying the IT objectives contained in Navy-Marine Corps strategies and central to net-centric operations and warfare.

For evolving the MCEN architecture, we have a collaborative architecture team from Headquarters Marine Corps C4, the Marine Corps Combat Development Command (MCCDC) and Marine Corps Systems Command (MCSC). This team is responsible for the operational, systems, and technical architecture views. The operational views describe our processes and associated information flows, and the systems and technical views describe our systems, applications, data, and technology standards. Collectively, we are developing an integrated enterprise architecture. One visible product from this collaboration, derived from the architecture information produced by MCCDC and MCSC, has been the Marine Corps Integrated Architecture Picture (MCIAP). The MCIAP is a graphical depiction of our Marine Air Ground Task Force (MAGTF) systems overlaid against notional Marine Expeditionary Forces, Brigades, and Units. The MCIAP has been a useful management tool for our programming and interoperability activities during POM-04, PR-05, and we are taking advantage of it for POM-06. We continue to enhance the MCIAP with information from our Supporting Establishment; our naval

shipboard environment; and with information on interfaces to Components, Services, and Agencies. We adhere to a technical standards baseline that is based on the Joint Technical Architecture (JTA). These architecture products establish the means from which we assess new IT capabilities for introduction into the MCEN.

III. ARCHITECTURE AND IT GOVERNANCE

The Marine Corps is actively participating in architecture and IT governance at all levels of the DoD. We are working with the Office of the Secretary of Defense (OSD)—CIO Executive Board, Joint Chiefs of Staff (JCS), and Joint Forces Command (JFCOM) in various working groups and domain governance bodies to refine the architectures and select the IT capabilities as part of the GIG.

Within the Department of the Navy (DoN), the Marine Corps participates in an active governance framework that spans policy, architecture, and acquisition. The Information Executive Council (IEC), our Department-level IT governance board, is working with our Program Executive Offices (PEO) and Systems Commands (SYSCOM) to implement Department-wide portfolio management led by designated Functional Area Managers (FAMs). Specific roles and responsibilities are being assigned to FAMS for developing and maintaining their respective domain-level architecture(s) in order to effectively manage their portfolios.

Within the Marine Corps, I provide centralized IT leadership through policy guidance and published standards, guide the IT infrastructure, and work in partnership with the Deputy Commandants and FAMs to ensure IT objectives supporting the Marine Corps strategy are met. Our Information Technology Steering Group (ITSG) with

representatives from the Deputy Commandants and FAMs guides and supports our internal enterprise approach for selecting IT solutions. This governance framework allows us to pursue a single, centrally commanded and defended, global Marine Corps Enterprise Network.

IV. CONCLUSION

The MCEN, the Marine Corps component of FORCEnet, is evolving to better serve our enterprise and the joint community. It is our framework for enterprise IT. The MCEN, together with MCEITS—our IT transformation initiative for net-centric services, defines our information infrastructure for delivering end-to-end, secure information at the right time, to the right place, and in the right format.

The Marine Corps is rapidly becoming a net-centric force. The opportunities afforded us through new technologies, coupled with our active participation in IT governance throughout the DoD, is allowing us to leverage the GIG and FORCEnet to introduce those capabilities, and change the way we conduct operations.

Mr. Chairman and members of the Terrorism, Unconventional Threats and Capabilities Subcommittee, thank you again for your steadfast support, and for this opportunity to appear before the committee to discuss how the Marine Corps is evolving our IT architecture and capabilities for the 21st Century.

NOT FOR PUBLICATION UNTIL
RELEASED BY THE
HOUSE ARMED SERVICES COMMITTEE

STATEMENT OF
DAVID TILLOTSON III, SES
DIRECTOR FOR C4ISR ARCHITECTURE AND ASSESSMENT
DEPUTY CHIEF OF STAFF, WARFIGHTING INTEGRATION
HEADQUARTERS UNITED STATES AIR FORCE
BEFORE THE
HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES
ON
11 FEBRUARY 2004
CONCERNING
DEPARTMENT OF DEFENSE INFORMATION SYSTEMS ARCHITECTURE: ARE WE ON THE RIGHT PATH TO ACHIEVING NET-CENTRICITY AND ENSURING INTEROPERABILITY
US AIR FORCE INFORMATION TECHNOLOGY ARCHITECTURE

NOT FOR PUBLICATION UNTIL
RELEASED BY THE
HOUSE ARMED SERVICES COMMITTEE

Mr. Chairman and member of the subcommittee

I am honored to be here today to discuss the Air Force's contribution to the Global Information Grid and net-centric warfare. Let me first take this opportunity to thank you for your continued support of the men and women of our Armed Forces.

A quick after-action review for Operations Iraqi Freedom (OIF) and Enduring Freedom (OEF) found that our Soldiers, Sailors, Airmen and Marines were more powerful and effective than ever before. This effectiveness was seen in increased precision, speed and lethality. As we become more effective, our adversaries have become keenly aware of the reaction time for our operators to obtain information and disseminate it to the shooters. At times they are able to exploit any delay and adapt tactics to improve their survivability. Just a few years ago, reaction time for time-critical targets was nominally measured in hours. Although reaction time was compressed to double-digit minutes during OIF, it's clear that future operations will require reaction times in the single digits.

To reach this goal we must achieve decision superiority and full-spectrum dominance in a Joint warfighting environment. The DoD's fundamental approach toward these ends is to use the construct of the Global Information Grid (GIG) to aim at a net-centric force and operation. In addition to the overarching GIG architecture and the DoD Architecture Framework, the Department outlines a combat systems construct (the Joint Task Force core architecture), a business construct (the Business Enterprise Architecture), and guidelines for the supporting IT infrastructure (the Network Centric Operations Reference Model

and Joint Technical Architecture) which guide the development of processes and systems which the Air Force deploys. I will focus in the remainder of this statement on the warfighting construct that appears to be the focus of this committee's discussions, but also note that the Air Force business enterprise also flows from the DoD business enterprise architecture in the same manner I will describe for the warfighting systems.

The C2 Constellation as a Component of the GIG

The Air Force's contribution to the overarching concept for warfighting operations is the C2 Constellation, which are the USAF components to the GIG. The C2 Constellation is a family of C4ISR systems sharing horizontally and vertically integrated information through machine-to-machine conversations enabled by a peer-based network of sensors, command centers and shooters. It is an operational construct and architectural framework that guides our development of people, processes and technology toward network-centric operations and the achievement of decision superiority and air and space dominance in support of the Joint Forces Commander.

Key elements of this C2 Constellation include the various platforms and sensors the USAF provides to the Joint Force Commander and key programs that support command centers such as the Air Operations Center and the Distributed Common Ground Segment (DCGS). Underpinning programs within the AOC, such as the Theater Battle Management Core System (TBMCS)

already serve as the joint standard for air operations planning and execution, and we are continuing to migrate these systems to a more modern, web-enabled architecture. I will say more about the USAF effort on DCGS later, but will note here that it forms the basis for moving the entire DoD DCGS to a more modern, net-centric architecture.

In addition, the USAF provides transportation layer components of the overall DoD GIG under an effort we call ConstellationNet. The ConstellationNet is the communications network—air, space, and terrestrial—that must allow a free flow of information so that it is rapidly accessible and presented to warfighters at the right time and right place to create the commander's desired effects. GIG transport layer components delivered under this effort are included in various USAF programs. The USAF portion of GIG-BE (GIG Bandwidth Expansion) provides expanded terrestrial service at key USAF bases globally. The Joint Tactical Radio System (JTRS) is essential to our vision for an improved airborne network, which expands genuine network operations to the airborne platforms. With the installation of Family of Advanced Beyond line of sight Terminals (FAB-T) on additional aircraft, such as AWACS, JSTARS and Global Hawk, we will have the capability to vastly extend our airborne network to all reaches of the globe. Finally, the USAF is responsible for a large portion of the space segment communication evolution including deployment of the Advanced EHF, Wideband Gapfiller System and the Transformational Satellite (TSAT) program. Each of these MILSATCOM systems represents progressive improvement in quality of service to all joint warfighters. The TSAT program, in

particular, extends the network to the space segment by providing high capacity, IP routing on the space segment and providing protected, high bandwidth access to air and surface forces on the move.

Architecture, Standards and Defining the Path

In order to ensure that the goal of a DoD Global Information Grid is realized, the Air Force, like the other Services, are both contributing to and deriving planning from the architectural frameworks developed under the leadership of OSD(NII) and the Joint Staff. Starting with these joint architecture frameworks, we apply the activity models and technical standards to the components of the DoD system for which the USAF is accountable. In addition, we are engaged directly with our Sister Services in teaming together at the technical, working, policy and senior-leader levels to achieve network-centric operations. These joint efforts are directed toward our desired end-state—completely integrated C4ISR. Ongoing activities include a cross-service Architecture group led by OSD, the Joint Battle Management Command and Control (JBMC2) roadmap group, the Joint Battle Management C2 board of directors under Joint Forces Command lead, an Airborne Networking Cross-Service Senior Steering Group and multi-service groups at various levels. The discussion among all these activities is facilitated and enabled by our ability to speak to common architectural components and standards, all of which are key to realizing interoperability. All of this activity is keeping us firmly on the path to

deployment of interoperable, net-centric systems that realize the vision of empowering the users through easy access to information anytime and anyplace, with attendant security. Some examples highlight the case:

The USAF is integrating architecture products and process into its requirements reviews. Stepping beyond the requirements of the Joint Staff process, the USAF is scrubbing its efforts in terms of a number of use cases that we call CONOPS focus us on key capabilities of the force. Both the operational processes and the systems are cast in an architectural setting reflecting either an "as is" or "to be" condition as we assess how procedures, systems, and their associated investments contribute to needed capability. That architecture is key to focused analysis. A similar process is underpinning the Joint Staff and other service activities.

Services are taking the architectural and standards guidance issued by the Department and applying it to shape decisions about programs and standards even at the service level. Applying the data standards from the Department, the services developed and sent to the Joint Staff a message standard which transforms Link 16 messaging standard to Extensible Markup Language (XML). Drawing from lessons learned in Cluster 1, and recognizing the benefits of common software and hardware components from architectural and engineering analysis, the Navy and USAF acquisition executives proposed combining the JTRS Cluster 3 and 4 development effort into one program. This recommendation was endorsed by the Defense Acquisition Board (DAB) in Dec 03.

Early discussion of architecture and network-centric requirements are driving early direction and management decisions for key programs at the Department level. The USAF was faced with the need to recapitalize its aging DCGS system and crafted an approach which derived from the standards set by the GIG architecture and Network Centric Reference Model as the basis for a new requirement. Subjected to service and DoD review, the approach proved attractive to all and the USAF program was adopted as developing the backbone for the broader DoD DCGS modernization effort. The DAB directed the use of the integration backbone and multi-int fusion as the migration path for all the service DCGS elements. As a result, the USAF RFP was modified to include other Service requirements, and all Services participate in the program oversight process. The key was early development of an architectural foundation that addressed the key precepts of net-centric operations and conformance to the GIG architecture.

The USAF-led TSAT program is a key component of the GIG and its evolution. TSAT requirements were derived from two years of architecture-based studies that from the outset cast the TSAT as a component of a joint, interagency network architecture. Potential technical approaches balanced industry and commercial solutions with more specialized capability. Designed as one element of a broader transformational communication architecture (TCA), the TSAT requirements were driven by consideration of all potential users and other network providers, but those requirements represent only a portion of the need. Architecture allowed us to assess and allocate that requirement;

standards ensure that the components will connect. The TCA continues to guide the development and acquisition of TSAT and a number of other systems, and allows the Department to manage the consequences of changes across the other components of the architecture. I led the Independent Program Assessment on TSAT, and we focused throughout the review on how the program office was establishing rigorous, architecture- and standards-based processes to ensure the synchronization of the TSAT program with other components of the architecture. In addition, we explored how the other agencies and services would participate in this process. The review of an AF program immediately led to interaction with the intelligence community, all the services, the Joint Staff, STRATCOM, and OSD. The architecture and engineering forums in the Department and the GIG end-to-end testbed that have been established are key components of the development process that this program has embraced. The common language that will unite this effort with the broader GIG is the architecture and standards handed down from the Department and implemented by the programs.

Commitment to the Vision and the Basis for the Flight Ahead

The USAF fits as a component of the joint warfighting effort.

Our systems reflect the same tenet - they are a component of the broader GIG. The detailed architecture we develop flows directly from the standards set by the Department and provide a more detailed view of a component of that overall architecture.

Architecture and standards provide a common mechanism for communication among the services and agencies. We are adopting the reference model approach called out in the Federal Enterprise Architecture framework, ensuring these reflect the standards imposed by DoD, and extending the details to the USAF level. These architectures and standards are becoming a regular part of our decision processes at all levels within the service, among the services and between the services and Joint Staff and OSD. The architecture products we develop are provided back to other services, the DoD and Joint Staff and to industry to facilitate decisions and guide development.

The USAF is committed to realizing a vision of providing a comprehensive information capability that is global, robust, survivable, interoperable, secure, and reliable that allows warfighters to create the right effect, at the right time, at the right point in the battlespace. Architectures and standards ensure we maintain course on that flight path.

DOCUMENTS SUBMITTED FOR THE RECORD

FEBRUARY 11, 2004

Support of the DoD Global Information Grid (GIG) Architecture

MG Marilyn A. Quagliotti, USA
Vice Director, Defense Information Systems Agency

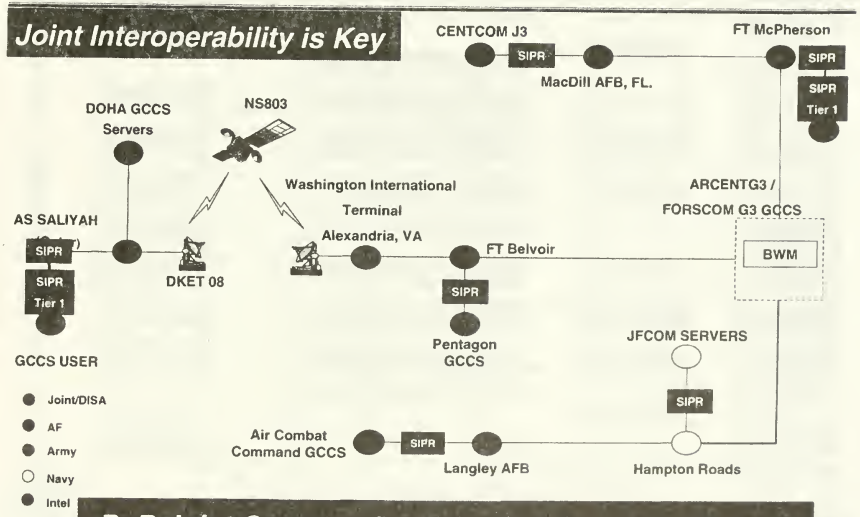
11 February 2004

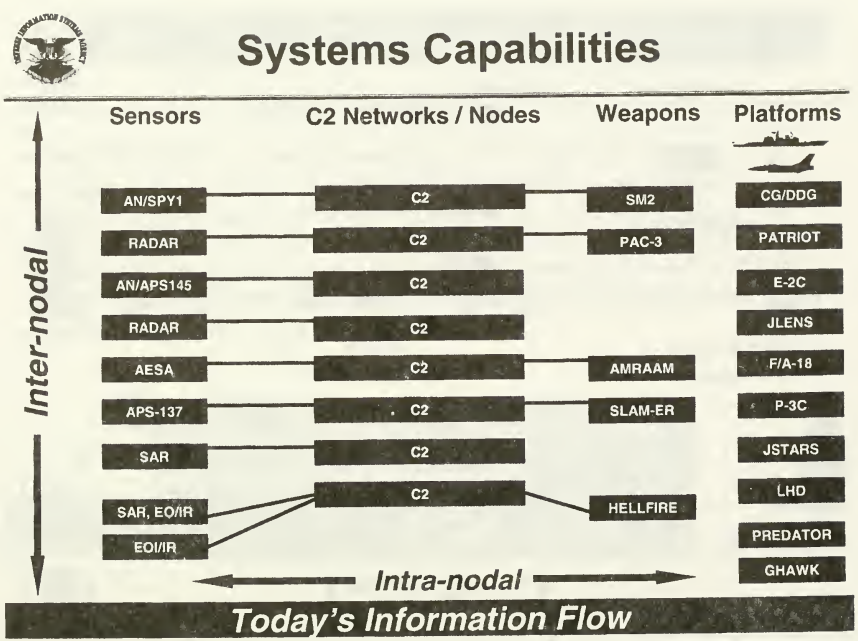
Support to The GIG Architecture

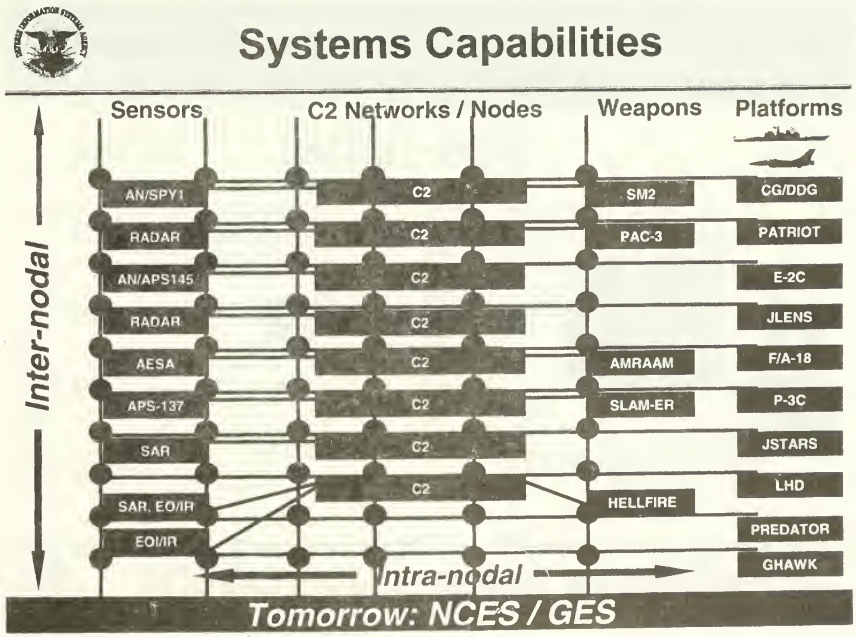
New Mission - The Defense Information Systems Agency is a combat support agency responsible for planning, engineering, acquiring, fielding, and supporting global net-centric solutions and operating the Global Information Grid to serve the needs of the President, Vice President, the Secretary of Defense, the Joint Chiefs of Staff, the Combatant Commanders, and the other DoD Components under all conditions of peace and war.

- Joint Acquisition Organization
- End-to-End Engineering
- End-to-End GIG Operations

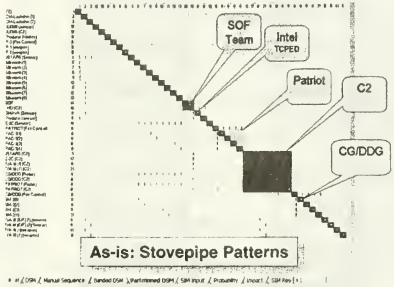
GCCS - J

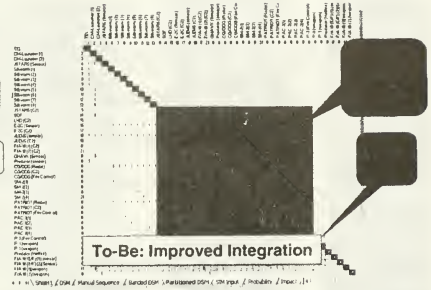

Joint Interoperability is Key
CENTCOM J3
SIPR
MacDill AFB, FL.
FT McPherson
SIPR
SIPR Tier 1
DOHA GCCS Servers
NS803
Washington International Terminal
Alexandria, VA
ARCENTG3 / FORSCOM G3 GCCS
AS SALIYAH
SIPR
SIPR Tier 1
GCCS USER
DKET 08
FT Belvoir
BWM
SIPR
Pentagon GCCS
JFCOM SERVERS
SIPR
Joint/DISA
AF
Army
Navy
Intel
Air Combat Command GCCS
SIPR
Langley AFB
Hampton Roads
DoD Joint Command and Control System of Record


Systems Capabilities
Sensors
C2 Networks / Nodes
Weapons
Platforms
AN/SPY1
RADAR
AN/APS145
RADAR
AESA
APS-137
SAR
SAR, EO/IR
EOI/IR
C2
SM2
PAC-3
AMRAAM
SLAM-ER
HELLFIRE
CG/DDG
PATRIOT
E-2C
JLENS
F/A-18
P-3C
JSTARS
LHD
PREDATOR
GHAWK
Inter-nodal
Intra-nodal
Today's Information Flow


Systems Capabilities
Sensors
C2 Networks / Nodes
Weapons
Platforms
Inter-nodal
AN/SPY1
RADAR
AN/APS145
RADAR
AESA
APS-137
SAR
SAR, EO/IR
EO/IR
C2
SM2
PAC-3
AMRAAM
SLAM-ER
HELLFIRE
CG/DDG
PATRIOT
E-2C
JLENS
F/A-18
P-3C
JSTARS
LHD
PREDATOR
GHAWK
Intra-nodal
Tomorrow: NCES / GES

Integration Pattern Emergence





(NCES – GES)

Even the smallest units can pull whatever data they need, whenever they need it, from wherever they are…

The DISA Big Six Material Solutions

- GIG-BE
- Teleport
- Net-Centric Enterprise Services (NCES)
- GCCS-J ++==➔ JC2
- GCSS
- Information Assurance

QUESTIONS AND ANSWERS SUBMITTED FOR THE RECORD

FEBRUARY 11, 2004

QUESTIONS SUBMITTED BY MR. SAXTON

Mr. SAXTON. What mechanisms do you have in place to ensure that your warfighting or tactical systems will interoperate with your sister service's systems?

General BOUTELLE. The Army has four mechanisms in place that facilitate interoperability in the DoD and Joint environment. They are: (1) the establishment of an Army Architecture Integration Cell (AAIC) with the mission of collaborating with both DoD and Joint force developmental efforts, synchronizing system engineering efforts, and integrating the Army Battle Command, Army Business Enterprise and LandWarNet architectures with DoD and Joint integrated architectures; (2) compliance with the Joint Technical Architecture that implements DoD and Joint information technology standards and protocols, (3) compliance with the Clinger-Cohen Act of 1996, and (4) compliance with the Joint Capability and Integration Development System (JCIDS) and the Joint Interoperability Test Center (JITC) to ensure that Army National Security System and Information Technology systems are interoperable with Air Force, Navy, Marine Corps and Defense Agency systems.

Admiral ZELIBOR. FORCEnet is being implemented in coordination with the Army, Air Force, Coast Guard, Joint commands and the Office of the Secretary of Defense—enhancing efficiency, joint interoperability, and warfighting effectiveness. The Joint Staff, together with OSD, continues to develop guidelines and procedures to ensure interoperability among all our programs. Navy will use the Joint Capability and Integration Development System (JCIDS) and the Joint Interoperability Test Center (JITC) to ensure that Navy-developed systems will interoperate with Air Force, Army, Marine Corps and Defense Agency-developed systems.

Mr. TILLOTSON. We have several initiatives in place to ensure interoperability:

a. All systems are required to meet an interoperability key performance parameter in system design. This requirement is being expanded across the services to address all the needs of network centric operations.

b. The Joint Interoperability Test Center (JITC) oversees service testing to ensure these interoperability requirements are in fact tested.

c. System designs are reviewed and certified by a joint DoD–NSA board to ensure compliance with network security standards.

d. Via the Air Force Communications Agency, we conduct network readiness assessments on new systems as they are fielded to ensure they will actually operate on the DoD network. Systems are not allowed to operate on the USAF portion of the GIG until a Certificate of Networthiness is issued.

e. Finally, we are working with DoD and Joint Staff to establish a virtual test facility to provide a standing DoD network against which contractors can develop and test new systems.

General THOMAS. The first mechanism the Marine Corps uses to ensure our warfighting systems will interoperate with sister Service systems is closely following DoD and Joint policy and direction, specifically the DoD 5000 series, CJCSI 3170, and CJCSI 6212. Second, the Marine Corps participate in DoD, Joint, and Component-level technical working groups that establish conditions that promote system interoperability. Further, our systems are subject to interoperability key performance parameters (KPP) and Network Centric Checklist reviews. By following DoD and joint doctrine closely and engaging actively in the joint forums, we are able to synchronize the release of system configuration baselines to our forces with their release to the other Services, we increase interoperability by following DoD and Joint acquisition strategies, and we verify joint interoperability through the use of joint test-beds through the Defense Research Engineering Network (DREN) to support federated and system-of-systems testing.

Mr. SAXTON. How does your service mitigate operations and future risk by using your respective service-based architecture?

General BOUTELLE. The Army mitigates operations and future risk by developing an Army Enterprise Architecture framework consisting of three subordinate integrated enterprise architectures, e.g., the Army Battle Command Architecture, Army Business Enterprise Architecture, and the Army LandWarNet Architecture. These subordinate architectures establish the overarching integrated architectures that provide the reference for functional gap analysis, system engineering, and invest-

ment strategies. In addition, these architectures support cost analysis, feasible scheduling, and decision support. The Army Architecture Integration Cell (AAIC) is a partner with the HQDA staff and Major Army Commands (MACOMs) to ensure integrated, synchronized, and coordinated solution sets.

Admiral ZELIBOR. The Architecture framework is one piece of the overall mitigation strategy. Another piece we have found to be key is experimentation, demonstration, and testing. Architecture is used in risk mitigation by providing a framework for modeling and simulation and experimentation. Potential operational concepts are evaluated and assessed in joint and fleet experiments. Feedback and lessons learned from the experimentation process are then reflected in the operational architecture to address shortfalls and implement improvements. The Joint Rapid Architecture Experimentation (JRAE) process is helping to consolidate the service's efforts in this area. Potential system architectures are used in modeling and simulation efforts to conduct analysis of future campaigns through probable threat scenarios, mission threads and tactical situations. By submitting potential system architectures to modeling and simulation, gaps and overlaps in systems and capabilities are discovered. Trade-off studies are done to balance risk versus cost of future systems to improve the architecture.

Mr. TILLOTSON. By developing systems using the GIG's net-ready/net-centric construct, systems will become "plug and play" within the next generation. For example, the JBMC2 effort (JFCOM-led with all service participation) will prescribe the need and means for intra-service collaboration and communications, and will use architecture to define interfaces and interactions with all ground, air, and space assets. The Network Centric Enterprise Services program will define common capabilities that all Service systems will use. Use of these common standards and services both reduces overall development time, and ensures that when systems are fielded, they are more likely to operate together. At an operational level, the use of these common standards and services reduces miscommunication or non-communication, improving overall effectiveness.

General THOMAS. Our Service view based on a single DoD architecture, the Global Information Grid (GIG), mitigates risk by providing a common enterprise environment that can be enjoyed and reused by all MAGTF elements within the Joint Task Force. The Marine Corps component view of the GIG architecture is the framework that guides our requirements analysis, experimentation and testing. Using the GIG architecture as a guide for our to-be operational systems shapes development perspectives and mitigates future operational risk. These perspectives are evaluated and assessed through testing, modeling and simulation, and engagement in joint and fleet experiments. The resulting feedback and lessons learned are used to make adjustments, to identify gaps and overlaps, address shortfalls, validate operational requirements, and ultimately to implement improvements across the spectrum of doctrine, organizations, training, materiel, leadership, personnel, and facilities (DOTMLPF).

The Marine Corps Integrated Architecture Picture (MCIAP) is another component of our mitigation approach. The MCIAP depicts a notional MAGTF systems architecture overlaid on our operational architecture. The MCIAP shows a system's interrelationship with other service systems.

Mr. SAXTON. How is your service developing its architecture? Are you collaborating with the others services? Why not develop a single DoD architecture?

General BOUTELLE. The Army has established the Army Architecture Integration Cell (AAIC) for managing the development of integrated and synchronized architectures with the DoD Enterprise Architectures. The AAIC coordinates architecture development efforts among the Army Executive Architects who are: the Army Operational Architect (Training and Doctrine Command (TRADOC)), the Army Systems Architect (Assistant Secretary of the Army for Acquisition, Logistics, and Technology (ASA (ALT)), and the Army Technical Architect (Army Chief Information Officer/G–6). These Executive Architects' mission is to ensure that the Army Enterprise Architecture is an integrated and seamless Enterprise nested within the DoD Enterprise Architectures. The use of the DoD Architecture Framework Document v1.0 provides a common framework for architecture development between the services.

The Army is definitely collaborating with the other Services through the Cross Service Architecture Working Group, synchronizing with the Joint Functional Capabilities Boards and by participating in numerous Joint integration efforts.

A single DoD architecture would require numerous subordinate architectures based on joint functional mission areas and capabilities, i.e., joint command and control, joint theater air and missile defense, global information grid, joint focused logistics, etc.

Admiral ZELIBOR. Navy and Marine Corps agencies are working together to develop the FORCEnet Architecture following the guidelines of the DoD Global Infor-

mation Grid (GIG) Architecture Framework. The GIG Architecture development process incorporates guidance and requirements from DoD, Joint and Coalition sources, the Joint Battle Management Command and Control development effort, the Joint Technical Architecture and Joint Functional Concepts. The FORCEnet development team meets regularly with the Air Force and Army agencies developing similar efforts for their services and the Joint Forces Command architecture team. The services clearly recognize that we must develop future architectures together so our operational plans and systems will be interoperable and seamless. Our jointly staffed Combatant Command Interoperability Program Offices (CIPOs), which are co-located at the three Service C4ISR System Acquisition Commands (SYSCOMs), are supporting the cross-service architecture collaborations from both the cross-systems and cross-combatant command's point of view. In FY03, the U.S. Navy funded contracts with the U.S. Army and the U.S. Air Force architecture integration offices for the development of common architecture products and design plans. We are also pursuing joint rapid architecture experimentation (JRAE) with the joint community on GIG distributed services, blue force tracking and communications on-the-move requirements in FY04. These efforts are being performed in close coordination with the USJFCOM chartered Cross-Service Architecture Integration Working Group (CSAIWG). Each service's architecture must be compatible and integrated with the DoD Global Information Grid, Network Centric Enterprise Services and other DoD initiatives. The Army, Navy and Air Force have joined in contract efforts to co-evolve some related portions of the Service architectures. However, each service has specialty areas (e.g., submarine warfare) that are not supported by the higher-level DoD architectures, but the architectures developed to support those required capabilities will be integrated with the enterprise architectures. By building the architectures together, using common standards and profiles for those standards, compatible with DoD and Joint requirements, the services are working to ensure interoperability.

Mr. TILLOTSON. 1. The C2 Constellation (to-be architecture) is based on the tenets of net-centricity as outlined in DoD's Network Centric Operations Reference Model. The C2 Constellation and the associated ConstellationNet architecture identify key interface points to link all AF platforms to the GIG. The C2 Constellation and the other Service architectures are following the same approach thus ensuring ubiquitous access to information and information sharing.

2. A variety of forums ensure Services coordinate their efforts. For example, the JBMC2 effort (JFCOM-led with all service participation) will prescribe the need and means for intra-service collaboration and communications.

A Small Sample of the Cross Service Integration Groups:

Action Officer level	Oversight (O-6)	Policy (★★★)
C4ISR Intergration Working Group	C4ISR Intergration Steering Group	Multi-Service C4ISR Intergration Talks
JBMC2 AO Working Group		JBMC2 Board of Directors
Cross-Service Architecture Group	JBMC2 Roadmap Working Group	JBMC2 Roadmap Summit

3. There will be one DoD architecture—the GIG. But it will be built from service components developed within the net-centric construct. For Joint (1) prescribes the means and (2) prescribes the ends and some aspects of the means for internal AF (1) prescribes the means and the ends.

General THOMAS. The Marine Corps develops its component architectural view within the single DoD architecture—the Global Information Grid (GIG).

Navy and Marine Corps agencies are extending the GIG Architecture into a Naval view called FORCEnet. The FORCEnet view adheres closely to DoD Architecture framework guidelines while satisfying unique Naval requirements. The FORCEnet development process incorporates guidance and requirements from DoD, Joint and Coalition sources, the Joint Battle Management Command and Control development effort, the Joint Technical Architecture and Joint Functional Concepts.

The Marine Corps is also a participant with the US Joint Forces Command chartered Cross-Service Architecture Integration Working Group (CSAIWG). The Army, Navy, Air Force, and Marine Corps are co-evolving related portions of their Component views of the GIG in support of Joint architecture objectives.

The Marine Corps is heavily involved in Joint Service activities for transformation of the Joint Technical Architecture to support Network-Centric Enterprise Services (NCES). We are also coordinating our architecture efforts with OSD on their Busi-

ness Enterprise Architecture (BEA), part of the Business Management Modernization Program (BMMP).

Mr. SAXTON. How is your service implementing net-centric warfare (NCW) concepts? Are you changing operational tactics, techniques, and procedures to accommodate the new technology environment?

General BOUTELLE. The Army recognizes that NCW concepts are many and addresses numerous perspectives. However, common in all NCW concepts is the need for an integrated enterprise and an end-to-end supported network. To achieve both, Army Transformation has focused extensively on integrating its functions, processes, organizations and its networks. The goal is to achieve superiority in land warfare, supporting business systems and associated information environment.

Achieving NCW means all domains must inherently employ net-centric operations and demonstrate required levels of net-centricity. The Army is obtaining just that. Applications are being developed with the enterprise in mind; data is being structured to be conducive for universal access and common enterprise services; and best practices are being adopted for implementing enterprise operational standards.

The Army's CIO/G–6 has mandated the combining of the all Army networks that include National Guard, Army Reserve, and all active component forces. The resulting network has been named LandWarNet. LandWarNet is the name for the Army enterprise network. It includes all Army networks—from sustaining military bases to forward-deployed forces. LandWarNet is the combination of infostructure and network services across the Army. It provides for processing, storing, and transporting information over a seamless network. LandWarNet is the Army's portion of the Department of Defense (DoD) Global Information Grid (GIG) Enterprise information environment (EIE) supporting DoD around the world. "LandWarNet" is the Army counterpart to the Air Force's Enterprise "ConstellationNet" and the Navy's "FORCENet."

Admiral ZELIBOR. Current doctrine reflects existing capabilities. The technology to enable full NCW is still under development and Navy is experimenting with how to, best incorporate and field these capabilities. As these methods are proven/fielded, they will be fully incorporated into doctrine.

As network capability is developed and fielded, it is also being documented in appropriate doctrine. Navy is incorporating emerging technology and NCW philosophy into Naval Warfare Publication "NWP 6–00, Operational Command and Control" and Naval Tactics, Training, Procedures "NTTP 6–00.1, C4I Infrastructure." Additionally, emerging technology is enabling NCW at the tactical level. Navy's Tactical Development and Evaluation program has developed several Tactics Memorandums (TACMEMO) that deal with aspects of NCW. Examples include: "TM 3–21.1–03; Network-Centric ASW Collaborative Mission Planning and Execution"; "TM 6–02.1–03; Use of the SIPRNET in Conducting Force Over the Horizon Coordinator Duties"; and "TM 3–13.1–03; Computer Network Defense for the Carrier Strike Group/Expeditionary Strike Group (FIWC)."

There is an ongoing effort to update doctrine to reflect our incorporation of NCW as it is practiced today. Taking queue from the Joint C4 doctrine, Navy is totally revising its command and control doctrine. Early drafts of NWP 6–00, Navy Operational Command and Control, and NTTP 6–02, Navy C4I Infrastructure, were released in early January of this year. These drafts have been scrutinized by the fleet and comments incorporated. Revised drafts will be released for review in late April.

Navy doctrine reflects what we have today; it is not theoretical in nature. As we develop new techniques, new tactics and systems, these publications, as well as all Navy doctrine, will be updated to reflect current, proven technology and practices.

Mr. TILLOTSON. The Air Force is implementing net-centric warfare (NCW) concepts through the development and refinement of Air Force architectures and the integration of NCW capabilities. The Air Force's Command and Control (C2) Constellation is designed to capitalize on emerging technology to network USAF capabilities, to include linkage to other components of the joint force. The C2 Constellation's open architecture provides for "plug and play" capability on a global scale. The Air Force is committed to realizing a vision of providing a comprehensive information capability that is global, robust, survivable, interoperable, secure, and reliable that allows warfighters to create the right effect, at the right time, at the right point in the battlespace.

In addition, the Air Force C4ISR Flight Plan provides a roadmap to achieve the NCW vision. This flight plan addresses: 1) IP-based routing which enables and allows self-forming, self-healing networks; 2) shared data access which improves C2 and situation awareness across platforms; and 3) assured service through robust connectivity, better security, and jamming protection.

As the network becomes more robust, Air Force operational tactics, techniques, and procedures (TTP) will certainly evolve. TTP are continually updated and refined

based on technology insertion and operator requirements. As an example, the Air Force leads the Joint Expeditionary Force Experimental (JEFX) exercise to evaluate new technologies and capabilities. Recommendations are then incorporated into new TTP. In JEFX 04, Network Centric Collaborative Targeting initiative will evaluate a self-forming network of sensors to provide an order of magnitude improvement in locating time sensitive targets. As new NCW capabilities emerge, new Air Force TTP will be formulated to meet service and joint warfighter needs at every level of warfare.

General THOMAS. Guided by the Golbal Information Grid (GIG) architecture, the Marine Corps is incorporating network centric concepts and technologies. We are committed to the concepts of shared information, common information resource components, and net-centric enterprise shared services. Functional domain managers now have an environment where they focus on developing their unique application requirements and not on replicating those common elements that are used by all applications. Further, we are developing and fielding interoperable network components to all elements and to the lowest level of the MAGTF the tools that will allow access to the vast array of data and intelligence that is available through Marine Corps, joint and DoD sources.

With the technology to conduct Network Centric Warfare (NCW) carefully being developed and fielded, the Marine Corps remains committed to implementing the concepts of NCW as they expand and improve our warfighting doctrine of expeditionary maneuver warfare and ship to objective maneuver. We approach NCW from a holistic perspective that includes doctrine, organizations, training, materiel, leadership, personnel, and facilities (DOTMLPF). Marine Corps doctrine constantly evolves to incorporate new technologies and is based on the principles of task organization, combined arms integration, and maneuver warfare. New capabilities allow us to experiment with new operating concepts while retaining our basic principles. For example, the Navy and Marine Corps through advanced concept technology demonstrations (ACTDs) and frequent naval exercises are experimenting with new naval formations and operational command structures enabled by net centric capabilities. Additionally, new technologies are providing greater access to information by lower echelons, thus giving small unit commanders better situational awareness and force application options. While new technologies provide the Marine Corps new opportunities for warfighting, we are mindful that uncertainty and the fog of war can counteract certain technological advantages. Therefore, we will exploit new capabilities while working to mitigate the potential pitfalls of over-reliance on technology.

Mr. SAXTON. How will your service test Internet Protocol version 6 (IPv6)? What kind of performance metrics will your individual service use to test the quality of service (QoS) issues we have raised? How realistic and rigorous will the testing be to determine if IPv6 will provide—at a minimum, the same quality of service that the Department's present computing network protocols provides (sic) today?

General BOUTELLE. The Army CIO/G–6 has established an IPv6 Transition Plan Working Group led by the CIO/G–6 and made up of members of the Army's acquisition community (ASA (ALT)), MACOMs, Installation Management Activity, and Network Enterprise Technology Command (NETCOM). This working group reports to the Army CIO Executive Board and oversees the efforts of the technically-oriented IPv6 Transition Task Force and several subordinate technical bodies overseeing different aspects of the Army's transition to IPv6. One of these subgroups is charged with Test and Evaluation.

The mission of the Test and Evaluation Subgroup is to develop test plans, develop scenarios for interoperability testing, coordinate test activities, and act as a liaison with the DISA distributed test bed to ensuring a successful IPv6 transition within the institution, operational, and tactical systems and networks of the Army. The subgroup will coordinate with the DoD Transition Office to develop a comprehensive plan to evaluate commercial-off-the-shelf (COTS) and Government-off-the-shelf (GOTS) IPv6 capable products, maintain a database of IPv6 capable products, and verify interoperability among IPv4 and IPv6 capable COTS and GOTS products through transition mechanisms. These activities will require coordination with DISA and other Services. Test organizations that will be represented in this subgroup include the Army Information Systems Engineering Command (ISEC) Technology Integration Center (TIC), the Central Technical Support Facility (CTSF), and the Joint Interoperability Test Center (JITC).

The Army Technology Integration Center (TIC) has already begun interoperability testing of IPv6 implementation from vendors providing Commercial Off-The-Shelf (COTS) equipment. The TIC does this for various programs and Project Managers. Mr. Stenbit's IPv6 memo caused the IT vendor community to accelerate their IPv6 efforts and provide the needed capability in their products by October of 2003. They

did this with software initially, but the IPv6 functionality of these products will eventually be designed into silicon and hardware to improve performance and throughput. In addition, the Army participated in DoD's IPv6 pilot project (Phase I of Moonv6)[1] and intends to continue such participation in future Phases of the Moonv6 testing effort. For phase 2, the Army will be leading the Moonv6 testing effort on mobility, obviously an area of great interest to the Army.

The TIC currently evaluates each device for current conformance to Internet Engineering Task Force documents, performance benchmark comparisons, network management features, and security mechanisms for both IPv4 and IPv6 protocols. The TIC also evaluates Campus Area Networks as a system for comprehensive functionality and interoperability in both IPv4 and IPv6 environments. Operating systems and application support are also evaluated for IPv4 and IPv6 performance and support.

To verify IPv6 provides the same quality of service as IPv4, the TIC evaluates each device in the system and measures throughput in bits per second, delay in microseconds, network data loss in frames lost, and validates that Internet Protocol Quality of Service parameters to include Type of Service and Differentiated Services are supported within each device. Clientserver response time is measured for operating systems and applications that incorporate IPv6.

All devices are connected in an installation network standard architecture and evaluated for functionality and interoperability using computers that parallel real user traffic profiles, as measured at several representative installations, in both IPv4 and IPv6 environments. This evaluation emulates real user scenarios such as an 8:00 am startup where all users are logging into the network and checking email concurrently. The required criteria for all IPv6 evaluations are identical to that of IPv4 for all systems. The TIC's array of test scenarios exercise the functionality, performance, stability, and throughput of COTS products as they run IPv6 protocols, and the results ultimately help to improve the products, software, hardware, and integration of these products into the Army enterprise. These IPv6 tests have been conducted at the TIC since October 2003.

As Government-developed systems are available, they will undergo intra-Army interoperability testing at the CTSF. Typically, CTSF testing will include interoperability testing of a full complement of associated systems expected to be delivered as part of the Army's software blocking process.

The Army has recently begun a modeling and simulation exercise of IPv6 in the Stryker Brigade Combat Teams (SBCT). The model simulates the IPv4 network currently found in the SBCT and then overlays both a dual-host and IPv6 native network onto the SBCT communications architecture. The IPv4 network establishes the control (baseline) parameters and metrics that can be analytically compared to the dual-host or native IPv6 network. The SBCT model is being validated by PM, TRCS to ensure it accurately reflects the network environment of an operational SBCT.

The Army is also planning to participate in joint IPv6 experimentation efforts, especially the Joint Rapid Architecture Experimentation (JRAE) Joint RAPTOR 04–4. This experiment is intended to demonstrate end-to-end testing between Navy surface vessels and Army/Air Force sites using IPv6 and dual stack techniques. Satellite and the IPv6-enabled Defense Research Engineering Network (DREN) will be used to establish an IPv6 backbone for the experiment. The following areas are being considered as part of the Joint Raptor 04–4:

IPv4/IPv6 transition techniques

Testing of prototype IPv6 High Assurance Internet Protocol Encryption (HAIPE) devices (Provided they are available by Aug/Sep)

Voice Over Internet Protocol (VoIP)

Data compatibilities between the Services

End to end Quality of Service/Class of Service (QOS/COS) issues

Multicast on red and black sides of crypto

Mr. TILLOSTON. 1. The Command and Control (C2) Constellation is the operational construct and architectural framework conforming to DoD and Joint Staff net-centric standards serving as the Air Force's contribution to the Global Information Grid (GIG) and net-centric warfare. The Constellation Net is the Air Force transportation layer of the DoD GIG and is our vision for a seamless air, space, and terrestrial-based network. The Air Force is currently defining the IPv6 transition plan using this construct to identify and focus transition efforts on high-value targets bringing operational benefits in the near term. We are leveraging existing programs, test labs and facilities, and live operational tests to rigorously test IPv6. The

[1] Moonv6 is a pilot project designed to push the envelope of IPv6; includes Government, Industry, and Academia. It is a network with approximately 20 nodes that runs IPv6 protocols. The original thought was "shoot for the moon" on IPv6, hence the name.

Combat Information Transport Systems (CITS) and Global Combat Support System (GCSS) program offices are working jointly to build a representative network to test IPv6 over our standard base networks, wide-area networks, and information systems. The Air Force Information Warfare Center is testing Information Assurance aspects of IPv6 using their MAJCOM-scalable test facility, and the Air Force Research Lab is identifying test opportunities as well. The Air Force will also continue its partnership with OSD, JS, DISA, and the other Services to identify test targets for the scale-level tests in 2004, 2005, and 2006.

2. Because of the operational importance of the GIG, it is imperative quality of service is either maintained or improved. Based on the inherent redesign of the IPv6 protocol, we anticipate improved efficiency once the transition is complete. An important aspect of future network performance is the maturity of IPv6-capable vendor products, both hardware and software, e.g., hardware-based routing providing faster network throughput.

Our IPv6-enabled test network performance will be compared to the current network baseline. The Air Force will specifically identify key performance metrics in our test plans to focus on network stability and quality of service such as routing convergence, packet latency, throughput capacity, delay, reliability, etc. Through continued participation in the DISA-led MOONv6 test and the Joint RAPTOR exercise test efforts we will continue to refine, and further define, performance metrics.

3. The Air Force will not permit operational use of IPv6 until we achieve the same quality of service provided by our networks today. Applying rigor to our test scenarios, along with identifying the right performance metrics, will ensure we achieve this aim. The Air Force is participating in the MOONv6 test with DISA, the Services, and the education community, providing an excellent opportunity to test the protocol's maturity and the supporting vendor products. The main Air Force node on this IPv6 test network is at the Air Force Communications Agency at Scott AFB, Illinois. This test is an opportunity for industry and the Military Services to experiment and learn more about IPv6 maturity in a geographically dispersed test environment. Other DoD test and research networks (the Defense Research Engineering Network and the DISA Leading Edge Services Network), and exercises such as RAPTOR, provide additional proving grounds for IPv6 implementation from which the Services can obtain lessons-learned. Analysis of testing efforts will help further define rigorous testing criteria to ensure no mission degradation and current quality of service is maintained once operational. The Air Force is currently planning operational deployment of IPv6 within the base infrastructure provided under the CITS program and the AFSN (wide-area network) that provides the interface between our base infrastructure and the DISN long-haul infrastructure.

General RADUEGE. What this means for our organization is that we are in the midst of all agencywide transformation that is enabling the agency to handle major joint and DoD wide acquisitions.

This transformation began in response to Mr. Stenbit's request that we put greater focus on our ability to acquire even larger and more complex programs than we currently have. A principal first step was that DISA stood up a separate, full time Component Acquisition Executive with a qualified staff of acquisition professionals to provide proper acquisition policy process, oversight, leadership and training. In addition, we have put in place SES level leadership guiding key joint programs, such as GIG–BE and NCES. We also stood up a separate Engineering organization dedicated to working closely with the CAE to ensure end-to-end systems engineering and horizontal integration of these joint programs that DISA manages.

Admiral ZELIBOR. The Department of Navy (DoN) C4I Chief Engineer (CHENG SPAWAR) is coordinating an Integrated Product Team (IPT) to establish an IPv6 Migration Strategy and Schedule as a deliverable to CNO by 15 April 2004. The strategy will include an End-to-End Network Testbed to ensure appropriate testing of functionality, performance, and QoS. Current Navy applications employing IPv4 have been limited. We have queried the Program Executive Offices (PEO) and System Commands (SYSCOM) for projected QoS needs. Once we establish what applications are (or will be) using QoS, the network testbed will be tailored to simulate these services. Future QoS implementations for programs such as the integrated Shipboard Network System (ISNS) and Automated Digital Network System (ADNS) will also be objectives of the testbed. The Navy's testing plans will be part of a coordinated and comprehensive IPv6 testing effort across DoD involving testing facilities as well as pilot implementations over the next several years to ensure that IPv6 can provide the performance, scalability, security and interoperability needed.

General THOMAS. The Marine Corps is working in partnership with other Components, Services, and Agencies for the development of strategies to test and migrate our IPv4 networks to IPv6. IPv6 will enhance DoD's ability to implement QoS. True end-to-end QoS does not exist over the Global Information Grid (GIG) using IPv4

today. In most cases QoS on IP networks today is artificially achieved by increasing bandwidth to prevent traffic from being blocked. However, a real need exists to build this capability into our networks to support data, voice and video convergence. The Marine Corps will participate in efforts underway at Defense Information Systems Agency (DISA) to define QoS policy for use on the GIG. Performance metrics for QoS testing include packet loss, end-to-end packet delay, and perceived as well as measured application performance across the network. Every effort will be made to ensure the rigor and validity of these tests. The Defense Research Engineering Network (DREN) will provide a native IPv6 test backbone for software application and system testing between Marine Corps sites as well as support testing with other services, industry, and academia. The Marine Corps believes that a collaborative effort with DISA, other Defense Agencies, and other Services will achieve the desired end-state of a GIG that provides QoS in support of Net-Centric Operations and Warfare.

Mr. Saxton. What is the Army's strategy to merge current information systems with Future Combat Systems (FCS) and Warfighter Information Network-Tactical (WIN–T)?

General BOUTELLE. Warfighter Information Network-Tactical will provide the FCS the integrating information network standard for information transport, network management, information integrity. Information Dissemination management (IDM), information assurance, and Quality of Service. These requirements were written into the WIN–T program to ensure synchronization with FCS. Current capabilities cannot support the FCS Concept of Operations (CONOPS) in the areas of reliability, mobility, bandwidth, information assurance, and mobile network operations. Within the FCS System of Systems Common Operating Environment (SOSCOE), Army is putting in an interoperability layer so FCS equipped Units of Action (UA) can translate the Current Force system information into the language that FCS understands (and vice versa). The WIN–T network will provide its users in the Future Force the external interoperability and connectivity with Current Force systems, as well as Joint, Stryker, Allied, Coalition, and commercial networks. This interoperability capability is one of the six Key Performance Parameters (KPPs) and will ensure that commanders at all echelons have interoperability with the full spectrum of Army Batttefield Command Systems. FCS is also baselined with a tactical tailored implementation of the Network Centric Operational Warfighter Reference Model (NCOW–RM), which will facilitate moving to the NetReady Key Performance Parameters (KPPs).

Mr. SAXTON. How will you stress and test the WIN–T network to ensure it will meet the Army's operational requirements? How and when will you test FCS and WIN–T together?

General BOUTELLE. The WIN–T network will be incrementally tested and stressed as the program evolves through its acquisition phases.

During the current System Development and Demonstration (SDD) phase, extensive modeling and simulation (M&S) of the proposed network architectures will be performed to evaluate system performance, assess and mitigate technical risks, perform cost/performance tradeoffs and refine system designs. Modeling will be based on a modified Caspian Sea scenario and will display a representative range of network topologies under which WIN–T will be expected to perform. This will be accomplished by using a TRADOC approved scenario and representative traffic scripts. This Caspian Sea model will be accredited by ATEC for use in the evaluation of the system to support the Milestone C Decision. A live Developmental Test/Operational Test (DT/OT) will be conducted at Electronic Proving Ground (EPG) Fort Huachuca, AZ, using representative soldier operators. Parallel DT/OT events will be conducted for each WIN–T contractor. All three WIN–T tiers (terrestrial, airborne, space) will be represented during this test. Plans call for each contractor to provide "one of each" representative equipment to demonstrate SDD exit criteria and achievement of Technology Readiness Level 6.

The Low Rate Initial Production (LRIP) phase will allow PM WIN–T to procure sufficient assets to support Production Verification Tests (PVT), Force Development Test and Experimentation (FDTE) and Initial Operational Test (IOT). PVT will consist of both a PVT-Contractor and PVT-Government to evaluate the systems technical capabilities. FDTE will be conducted by TRADOC to evaluate training and make recommendations on established WIN–T doctrine. IOT will be conducted in an operational environment and will consist of sufficient assets to demonstrate a UE with connections to higher and lateral echelons as well as multiple interconnected UAs. WIN–T will support split-based operations over representative distances and implement reach back for both stationary and on-the move communications, access at all security levels and provide network access to local subscribers. Static ground, airborne and space relays will be used to enhance the area of coverage. Interoper-

ability testing will be performed to evaluate the interface with Army Current Force, Defense Information System Network (DISN), Joint Networks, Allied Networks and US Commercial Networks. Modeling and Simulation will be used in this phase to provide realistic traffic stimulation. As in the SDD Phase, M&S will be used to assess all representative network topologies and mission requirements.

PM WIN–T has been coordinating testing and M&S efforts with the FCS Command, Control, Communications, Computers, Intelligence Surveillance and Reconnaissance Integrated Program Team (C4ISR IPT). The initial focus will be on obtaining a common simulation environment for the two programs. It is anticipated that M&S integration can commence in FY06 and will continue throughout the life of the two programs. PM WIN–T will be providing prototype WIN–T Points of Presence (PoP) to the FCS equipped Units of Action (UA) program for use in initial integration efforts beginning in 2006. The PoP serves as the entry point to the WIN–T network. These assets will be used by FCS in their testbed and at Integration Phase SDD 2 (IPS2) in June 2006. This event will enable FCS to demonstrate UA to UA communications. WIN–T will provide a sufficient number of PoPs to support the FCS C4 Integration Test in June 2007. WIN–T UE elements will be provided to demonstrate the preliminary UE to UA architecture in a live field environment. Beginning in January 2009, the WIN–T IOT and the FCS LUT2 will be conducted. These events will provide an opportunity to demonstrate the combined UE/UA architecture in an operational environment.

Mr. SAXTON. Is FORCEnet an enterprise architecture?

Admiral ZELIBOR. The vision of FORCEnet is a single, enterprise-wide, enterprise-deep architecture. It will reach across all programs (Weapons/IT/C4ISR/Hull, Mechanical & Electrical (HM&E)) to incorporate tactical and non-tactical/business systems to create a continuous information environment across the Naval enterprise. It will function as the Naval component of the DoD enterprise-wide GIG architecture. As the enabler for the Naval Power 21 capabilities of Sea Strike, Sea Shield, and Sea Basing, FORCEnet is required to support each pillar. This necessitates that FORCEnet architecture be an enterprise-wide unified entity, and must seamlessly integrate with the architecture of other Services and the broader DoD information infrastructure.

Mr. SAXTON. What kind of forcing mechanisms do you have to ensure that the ships, aircraft, and shore-based sites will comply with FORCEnet?

Admiral ZELIBOR. The mechanisms to enforce FORCEnet compliance by programs of record (POR) are in the process of being developed and will require close cooperation between operational, policy and acquisition organizations in the Navy and Marine Corps. The primary organization will be the Virtual SYSCOM, which includes representatives from SPAWAR, NAVFAC, NAVSEA, NAVAIR, and ASN RDA's FORCEnet EXCOMM. Compliance criteria are being formally documented and will be enforced through the technical authority of the FORCEnet CHENG. In addition, a FORCEnet Compliance Checklist and a supporting end-to-end governance process are being implemented to support adherence to FORCEnet criteria. These FORCEnet criteria—which include FORCEnet operational requirements, FORCEnet system/technical requirements (including FORCEnet architectures and standards), FORCEnet policy requirements, and FORCEnet implementation requirements—incorporate relevant Naval, Joint, DoD, and Inter-Agency requirements. As an example, FORCEnet language was included in the Capability Development Document, C4ISR Concept of Operations (CONOPS), and Contract/Request For Proposal (RFP) for the Littoral Combat Ship (LCS).

Mr. SAXTON. What kind of performance parameters do you have?

Admiral ZELIBOR. Performance parameters reside primarily with the FORCEnet individual Program of Records. These are not new or different from existing acquisition performance requirements that are developed to evaluate a system designed to satisfy a given requirement. Global FORCEnet performance parameters (Measures of Force Effectiveness [MOFE]) can be developed after FORCEnet operational concepts, CONOPS, requirements and architecture operational views are created.

Mr. SAXTON. How will FORCEnet affect Navy tactical and business information technology systems?

Admiral ZELIBOR. FORCEnet is not an acquisition program; rather, it is an enterprise alignment and integration initiative that potentially touches every Naval program, and is the Naval vehicle to make Network Centric Warfare an operational reality. FORCEnet will provide the metrics for evaluating compliance of all Naval information systems to the FORCEnet and Global Information Grid (GIG) architecture and standards. This compliance will in turn require new and existing programs to seamlessly share and exchange information regardless of the type of information processing conducted, the information format presented to the decision maker, and the media over which the information is transmitted. Not only will greater oper-

ational flexibility and agility be achieved through this enterprise alignment with the FORCEnet compliance process but information systems will be better designed to provide for and enable adaptive business and war fighting process transformation and execution. The FORCEnet alignment mechanisms will provide for evolution as new technologies are identified and injected into the FORCEnet network fabric. FORCEnet does not have a specific end-state; rather it will establish an environment, which facilitates Naval Transformation.

Mr. SAXTON. How will Navy-Marine Corps Intranet (NMCI) fit into FORCEnet?

Admiral ZELIBOR. NMCI is one of the many pieces that support FORCEnet. NMCI provides the shore network infrastructure within Continental US (CONUS) for Navy's FORCEnet Architecture. NMCI is a long-term initiative between the Department of Navy and the private sector to deliver a single, integrated, and coherent department-wide network for Navy and Marine Corps shore commands. NMCI will provide comprehensive end-to-end information services for data, video and voice communications for Department of Navy military and civilian personnel and connect to the Global Information Grid (GIG) Architecture, making our workforce more efficient, more productive, and better able to support the critical war fighting missions of the Navy and Marine Corps. The "Outside of Continental US" (OCONUS) shore infrastructure is provided by Base Level Information Infrastructure (BLII); the afloat infrastructure is IT–21. These systems, along with sensors, communications systems, weapons, and people, are all part of FORCEnet.

General THOMAS. The Marine Corps Enterprise Network MCEN is the Marine Corps component of FORCEnet and the Global Information Grid (GIG). MCEN is our enterprise framework for information technology (IT). MCEN, as part of the broader FORCEnet naval view, connects the garrison, maritime, and expeditionary infrastructures vital for sharing information with all Marines. MCEN supports all information exchange requirements for Marine warfighters and our Supporting Establishment. It is our end-to-end IT capability and infrastructure spanning both our warfighting and business domains.

Mr. SAXTON. Will the C2 Constellation allow a soldier or Marine on the ground to communicate directly with the pilots flying close-air-support? Is this a needed capability? How will the C2 Constellation interoperate with the Army and Navy's architectures?

Mr. TILLOTSON. Yes. The best example is Forward Air Support, where the Marine on the ground can directly send information to air support.

We are driving to a net centric architectural environment that will allow information exchanges from and to any node (without regard to Service). Information exchanges will no longer depend on point to point communications. Information is routed through whatever nodes make it possible for each end to connect. For example a soldier with a UHF radio needs to communicate with a coalition aircraft with an EHF radio. The request for information goes over the net on UHF nodes until it reaches a node that has an UHF and EHF link then the request travels by EHF till it reaches the other end. The response then comes back in a similar manner but not necessarily by the same path. This method is similar to internet processes today; routers send messages to the next closest router to the destination; if the next closest router is a different type, the message is translated as it is sent.

General THOMAS. The Marine Corps ensures synchronization and joint interoperability through the respective Joint Concepts and Integrated Architectures that are being developed through the Functional Capabilities Boards (FCBs), as part of the CJCSI 3170 Joint Capabilities and Integration Development System (JCIDS) process. We participate fully in the JCIDS process and regularly contribute Marine Corps-specific architectural pieces to the FCBs. These architecture artifacts are intended to plug in to the overall Joint integrated architecture at key interface points. In addition, we are also working very closely with other Services as we collectively pursue greater Joint interoperability. For example, we are working directly with both the Naval Network Warfare Command and the Space and Naval Warfare Systems Command on FORCEnet operational and systems architecture development, and we are also working with US Army G–8 and Training and Doctrine Command (TRADOC) in the development of the operational views to support Joint Blue Force Situational Awareness and Army/Marine Corps interoperability requirement efforts for our respective ground forces.

Mr. SAXTON. The Air Force has stated that the C2 Constellation and ConstellationNet are the communication "infostructure"—can you please explain what this means?

Mr. TILLOTSON. The C2 Constellation defines the people and mechanisms (systems, planes, supplies, etc.) required by the Air Force to execute a particular mission. One portion of the Constellation is the underpinning information transport mechanisms, which includes the people who operate the networks and their equip-

ment (such as switches, routers, communication fiber, data links, SATCOM, etc.) which move the information. We refer to this transport and computing layer as the "infostructure."

The part of the Infostructure used by the C2 Constellation is called ConstellationNet-networking warriors, weapons, and sensors at all levels. Within the C2 Constellation, it refers to standard services described by the Infostructure Architecture. These include connection to the GIG, storage and transportation of voice, data, and imagery information, tactical datalinks, satellite communications and future Transformational Communications.

Mr. SAXTON. Given the previous initiatives that the Department of Defense has undertaken to transform business and military operations and the lack of progress made by these initiatives, what makes the Global Information Grid different and worth an investment of least $23 billion over the next 5-years?

Secretary STENBIT. The success of the Department's transformation to the Global Information Grid paradigm results from the comprehensive and overarching nature of this seamless, common network. The GIG is not a system, and there is no single program that encompasses the entire GIG. Instead there are many programs and systems that will deliver the information capabilities and services available to GIG users. The GIG is a, vision, an entity, and an architecture. As a vision, the GIG establishes the conceptual framework for a "to be" information environment for the DoD. As an entity, the GIG comprises many systems that interoperate to provide the right information to the right places when needed, like a private worldwide web. The GIG is also a well-established, documented, and integrated architecture that defines the enterprise-level information environment blueprint from three perspectives—operational, systems, and technical.

We are putting in place improved and timely information technology investment policies, procedures and architectures that are enabling change throughout the Department in all areas from capabilities definition to planning, programming and budgeting to actual systems acquisition. This all encompassing approach will assure that we have the right capabilities to perform our mission, conduct effective information operations, and eliminate outdated ways of doing business.

True transformation can only be achieved by transforming the way we communicate, by making the network work for us, and by taking full advantage of information age technologies to ensure that our warfighters have immediate and direct access to the information they need. By exploiting technological advances that continue to shrink the costs of bandwidth, information processing, and information storage, we are making great strides toward that goal.

Details and Accomplishments

As testified by ASD(NII) and the Services before Congress on February 11, 2004, the GIG is the organizing construct for achieving net-centric operations and warfare in the DoD. Specifically, the GIG is defined as a globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG is a vision, an entity, and architecture.

As a vision, the GIG establishes the conceptual framework for a "to be" information environment for the DoD. This environment will provide information and communication services vital to the effective conduct of DoD activities, be they warfighting or business in nature. It also will be the foundation for allowing the DoD to achieve its net-centric operations and warfare goals.

As an entity, the GIG comprises many systems that interoperate to provide the right information to the right places when needed. Thus, the GIG will be like a private worldwide web (WWW): many systems distributed worldwide that interoperate to allow vast amounts of information to be readily accessed by anyone or anything; anywhere, anytime; if appropriately authorized. In the same manner that the WWW is transforming industries and societies on a global scale, the GIG will support the transformation of warfighting and business practices.

The GIG is also a well-established, documented, and integrated architecture. GIG is the Department's "Enterprise Architecture" that defines the enterprise-level information environment (EIE) blueprint. The GIG Architecture comprises three perspectives or views—operational, systems, and technical. As such, the architecture represents the structure of GIG components, their relationships, and the principles and guidelines governing their design, operation, and evolution over time. The GIG Architecture is used to determine interoperability and capability requirements, advance the use of commercial standards, accommodate accessibility and usability requirements, and implement security requirements across the Department.

There is no single program that encompasses the entire GIG. Many programs and systems will deliver the information capabilities and services available to users on the GIG. For example, there are many programs addressing the communication layer of the GIG such as GIG Bandwidth Expansion, JTRS, TCS, WIN–T, and several other Service Initiatives.

GIG Enterprise Services (GES) is a collection of networked information capabilities organized as core enterprise services and mission specific domain or community of interest services. The core enterprise services component of GES is being delivered through the Net-Centric Enterprise Services (NCES) program. Other programs will deliver additional information services. Such programs include, for example, FCS, DCGS, JC2, ForceNet, C2 Constellation and others.

To ensure that these programs all become elements of the GIG (the entity) as they are developed and delivered, the GIG vision is supported by numerous documents, policies and processes. The documents (a GIG tool set) include: the GIG Architecture v2.0 (GIGA) which provides an integrated architecture for net-centric operations and warfare; the Joint Technical Architecture (JTA v6.0) that provides a minimum set of mandatory standards that when adhered to provide the "building codes" that will facilitate the interoperability and incorporation of systems into the GIG; the net-centric checklist that provides a detailed set of guidelines that systems must adhere to in order to test if a system is net-centric capable; a DoD data strategy that sets the framework for how a system should define, tag and post it's data so that other's in the GIG can make use of and provide information access to that system; an evolving Information Assurance Architecture extension to the GIGA; and the Net-Centric Operations and Warfare Reference Model (NCOW–RM), that gives a high-level perspective of how to use the tool set. Guidance for the use of this tool set is provided through existing and evolving Department policies and directives. Brief descriptions and locations of the GIG toolset elements and associated directives include:

A) Integrated Architectures:

A DoD framework for GIG integrated architectures to achieve net-centricity and interoperability. Following is a summary of the tools supporting use of integrated architectures in the Department:

1) DoD Architecture Framework (DoDAF):

DoDAF v1.0 provides the rules, guidance, and product descriptions for developing and presenting architecture descriptions that ensure a common denominator for understanding, comparing, and integrating architectures.

2) Net-Centric Operations and Warfare Reference Model (NCOW RM):

(userid and password required)

A description of enterprise level activities, services, technologies, and concepts (e.g. data strategy) that enable a net-centric environment for warfighting, business, and management operations.

3) Core Architecture Data Model (CADM):

Provides a common approach for organizing and portraying the structure of architecture information, and is designed to capture common data requirements. The CADM facilitates the exchange, integration, and comparison of architecture information throughout DoD, improving joint C4ISR interoperability.

4) GIG Architecture v2.0 (GIGA):

(userid and password required)

GIG Architecture v2 describes the enterprise aspects of NCOW in a series of objective (future) architectures with integrated operational, systems, and technical views. The Architecture spans the enterprise by presenting strategic, operational, tactical, and combined use cases. GIG Architecture v2 is the initial architectural description of NCOW concepts and terminology, and will be a basis for developing the NCOW Reference Model. The principal focus of GIG Architecture v2 is on future NCOW concepts.

5) Joint Technical Architecture Version 6.0:

Provides mandatory standards and guidelines in Volume 1, and lists emerging standards and guidelines for net-centricity in Volume 2. The mandatory standards in Volume 1 are the minimal set of primarily commercial Information technology (IT) standards that all presently and future IT systems procured by DoD must use. By mandating such standards, these systems will be integratable in to and become part of the GIG as they are delivered to our warfighters and other DoD personnel.

6) Information Assurance (IA) Architecture for the GIG:

The GIG must be a secure, available and trusted information infrastructure if it is to facilitate and support net-centric, effects-based warfare capabilities and effi-

cient, reliable DoD e-business. To achieve these security attributes, it is imperative that Information Assurance be designed into the GIG at the beginning of its development. At OSD's direction, the National Security Agency has taken a leadership role in defining the GIG IA Architecture to meet the desired security attributes. Version 1 of this GIG–IAA will be delivered July of 2004 for review and comment by all DoD stakeholders and Version 1 will be formally released in October of 2004.

B) DoD Data Strategy:

A published plan for making the Department's data visible through the use of tagging and advertising data assets with discovery metadata

See DoD Metadata Registry and Clearinghouse at
http://diides.ncr.disa.mil/mdregHomePage/mdregHome.portal
(userid and password required).

C) Net-Centric Checklist:

A detailed set of criteria program managers and domain owners must use to gauge how well a program meets requirements of net-centricity. This checklist will be used in technical working to ensure that a system that is moving through the DoD acquisition process meets, from a systems engineering perspective, the GIG guidelines and toolset criteria.

D) Policies and Directives:

DoD's adoption of net-centric operations and warfare in formal directives and policy memoranda:

1) DoD Directives. and Instructions

a) DoD Directive 4630.5 (DRAFT), Interoperability and Supportability of Information Technology (IT) and National Security Systems, Section 4.4

Establishes the requirement to use a Net-Ready Key Performance Parameter (NR–KPP) "to assess information needs, information timeliness, information assurance and netready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange."

b) DoD Instruction 4630.8 (DRAFT), Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)

Implements a capability-related, outcome-based process whereby IT and NSS interoperability and supportability needs for new, modified, and fielded systems are documented, coordinated, approved, implemented, and verified to achieve an integrated, and secure IT and NSS infrastructure supporting global operations across the peace conflict spectrum.

c) DoD Directive 5000.1, The Defense Acquisition System

Section 5: Establishes the requirement for the Under Secretary of Defense (Comptroller) (USD(C)) to certify all financial management and mixed (financial and nonfinancial) information systems as being compliant with the Financial Management Enterprise Architecture (now referred to as the Business Enterprise Architecture). Enclosure 1, Section E1.9: Requires Acquisition Managers to "address information assurance requirements for all weapon systems; Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance systems; and information technology programs that depend on external information sources or provide information to other DoD systems." Enclosure 1, Section E1.9: Establishes requirements for interoperability and specifies use of joint concepts and integrated architectures to characterize interrelationships.

d) DoD Instruction 5000.2, Operation of the Defense Acquisition System, Section 3.2: Requirements and Acquisition Integration

Establishes the requirement to develop joint integrated architectures for capability areas and assigns responsibility to the Under Secretary of Defense (Comptroller) (USD(C)) for the development of the Financial Management Enterprise Architecture (now referred to as the Business Enterprise Architecture). It further states that the "DoD Chief Information Officer (CIO) shall lead the development and facilitate the implementation of the Global Information Grid Integrated Architecture, which shall underpin all mission area and capability architectures."

e) DoD Instruction 5000.2, Enclosure 4, Table E4.T1, CCA Compliance Table

Requires DoD Acquisition programs to demonstrate consistency with GIG policies and architectures, to include relevant standards, at Milestones A, B and Full Rate Production Decision Review (FRPDR) (or their equivalent).

f) DoD Directive 8100.1, Global Information Grid Overarching Policy, Section 4.3

States, "GIG assets shall be interoperable, in accordance with approved requirements documents, and compliant with the operational, system, and technical views. . .of the GIG architecture."

2) DoD Policy Memoranda:

a) ASD(NII) memorandum, Department of Defense Architecture Framework (DoDAF), Feb 9, 2004

Approves DoDAF Version 1.0 for use. Defines a common approach for DoD architecture description, development, presentation, and integration for both warfighting operations and business processes.

b) USD(AT&L) & ASD(NII) memorandum, Department of Defense (DoD) Joint Technical Architecture (JTA) Version 6.0, Nov 24, 2003

Approves the latest version of the JTA for use. States that Systems in development that are prior to Milestone C and that are regulated by DoDI 5000.2 and DoDI 4630.8 must have a technical view and standards profile derived from the standards and guidelines contained in the JTA Volume 1. Approval of the standards profile and migration plan (if a plan is necessary) is required for the program to proceed through the acquisition process. The DoD CIO will determine the adequacy of the profile and plan in consultation with the appropriate Milestone Decision Authority (MDA).

c) ASD(NII) memorandum, Department of Defense (DoD) Internet Protocol Version 6 (Ipv6), June 6, 2003

Provides DoD policy for Enterprise-wide deployment of IPv6.

d) Deputy Secretary of Defense Memorandum, Global Information Grid Enterprise Services (GIG ES): Core Enterprise Services (CES), November 10, 2003, U–18556/03

Provides guidance for existing and future acquisition programs to implement the plans for Global Information Grid Enterprise Services (GIG ES).

e) ASD(NII) memorandum, DoD Net-Centric Data Strategy, May 9, 2003

Provides a key enabler of the Department's Transformation by establishing the foundation for managing the Department's data in a net-centric environment.

f) ASD(NII) memorandum, Department of Defense (DoD) Net-Centric Data Strategy: Visibility-Tagging and Advertising Data Assets with Discovery Metadata, Oct 24, 2003

Provides guidance on planning for and implementing data asset "visibility" as described in the "DoD Net-centric Data Strategy" dated May 9, 2003.

g) CJCS Instruction 6212.01C, Interoperability and supportability of Information Technology (IT) and National Security Systems

Provides detailed instructions for the implementation of information technology (IT) and National Security Systems (NSS) interoperability and supportability certifications, including format and architecture guidance for information support plans (ISPs), and details the Net-Ready Key Performance Parameter (NR–KPP). The NR–KPP establishes the information needs, information timeliness, information assurance, and net-ready attributes required for both the technical exchange of information and the end-to-end.

Operational effectiveness of that exchange. The NR–KPP consists of verifiable performance measures and associated metrics required to evaluate the timely, accurate, and complete exchange and use of information to satisfy information needs for a given capability. In accordance with DoDD/I 4630 Series, the NR–KPP, documented in CDDs and CPDs, shall be used in analyzing, identifying and describing IT and NSS interoperability needs in the ISP; and test strategies in the TEMP. The NR–KPP is comprised of the following four elements:

- Compliance with the NCOW RM
- Compliance with KIPs
- Compliance with DoD IA requirements.
- Supporting architecture documents

h) Deputy Secretary of Defense memorandum, "Information Technology Portfolio Management," March 22, 2004

Establishes DoD policies and assigns responsibilities for managing information technology investments as portfolios where decisions on what IT investments to make, modify or terminate are based on architectures, risk tolerance levels, potential returns, outcome goals and performance.

E) OSD Oversight-Process Enhancements:

1) Net-Centric Program Reviews

A review process for assessing a program's transition to a net-centric environment to support the formulation of the President's Budget FY 2006–2011. These reviews focus on helping Components and program managers comply with net-centric attributes, implement the DoD Data and Information Assurance Strategies, align programs with the Joint Technical Architecture (JTA) and the Net-Centric Operations Warfare Reference Model, establish priorities and design transition plans in line with GIG Enterprise Services. Details on website at *https://pais.osd.mil/documents.nsf*

2) Systems Engineering (SE) Oversight and End-to-End evaluation facility

An ASD(NII) GIG end-to-end Systems Engineering (SE) oversight activity has been created to work with the DoD community to identify and facilitate the resolution of interoperability, interface and standards issues between and among all programs that are critical to the incremental development and deployment of the GIG (the entity). This ASD(NII) GIG Systems Engineering (SE) activity is being complemented with the use of GIG end-to-end evaluation (test bed) facilities. These facilities will be used to ensure that systems being developed by DoD components meet GIG architectural requirements and its associated building codes listed in the JTA.

Many of the GIG tools, related policies and OSD oversight process improvements have come about within the last two years. These tools support and facilitate the implementation of the GIG. In the past such, tools did not exist making system integration into a common framework impossible. Using these new tools and processes, the ability to provide appropriate governance over DoD component-program development activities is greatly improved. Our components now have a clear set of guidelines that they are following to ensure that as they deliver system/capabilities, these capabilities will be integrated into an overall DoD Global Information Grid.

The effectiveness of these policies, toolset and processes noted above are starting to be felt across the Department. As the testimony of the Services highlighted, the GIG has become the foundation vision and architecture for each of the Service's respective visions and tools such as the JTA, NCOW–RM and others noted above are being used by the Services in development of the systems they are developing as part of the GIG.

Mr. SAXTON. Does DoD have an overarching investment plan to guide implementation of the architecture—if so, what are the key milestones in managing this investment strategy? What key organizations are responsible for these milestones?

Secretary STENBIT. Yes, the Department does have a solid investment strategy for implementing the GIG architecture. The Department is committed to implementing the GIG in the earliest possible time frame at the lowest acceptable cost so that decision makers and warfighters use the most accurate, up-to-date, and comprehensive information possible. This commitment is demonstrated by the tens of billions of dollars the Department is investing over its Future Year's Defense Program, and, when complete, it will have revolutionized our means of conducting operations throughout the spectrum of conflict. To ensure that we get the greatest return on our investment, the ASD(NII)/DoD Chief Information Officer (CIO) is guiding an investment strategy across the Department's corporate processes which link requirements, architectures, plans, program acquisition and budgets.

In the area of requirements, ASD(NII)/DoD CIO works closely with the Joint Staff (J–6) on its Net Centric Functional Capabilities Board (NC FCB). This Board maintains a prioritized list of net-centric capabilities required by operational warfighters and adjudicates warfighting capabilities proposals, gaps and needs to ensure that integrated architectures accurately represent the net centric functional capabilities required by mission areas. In addition, the ASD(NII)/DoD CIO participated last year in a Joint Staff study to evaluate its requirements generation process, and this study led to the re-design of this Joint Staff process for identifying and validating requirements. Now called the Joint Capabilities Integration and Development System (JCIDS), it ensures that requirements reflect actual capabilities needs and-that IT solutions to these needs comply with GIG architecture specifications.

To further ensure the fidelity of our GIG investments, the ASD(NII)/DoD CIO is the Milestone Decision Authority for Major Automated Information Systems (MAIS) and selected Major Defense Acquisition Programs (MDAPs), and he and his staff engage fully in management oversight of remaining MDAPs via such forums as Overarching Integrated Product Teams, Defense Acquisition Boards, and Defense Space Acquisition Boards. Because these forums consist of senior officials representing comptroller, acquisition, policy and program equities, the ASD(NII)/DoD CIO is able to use their deliberations to link GIG-related investments with program development and acquisition milestones.

Likewise, we work daily within the Planning, Programming, Budget and Execution (PPBE) processes. For example, we collaborated closely with USD/Policy in the development of the Department's FY06-11 Strategic Planning Guidance, an overarching document that highlights DoD priorities and provides strategic direction for Component resource allocation. Recently signed by the DEPSECDEF, this SPG enunciates the Department's goal of accelerating the transition to a network-centric force and dictates a discrete set of transformation investments to ensure that our GIG-related transformation initiatives are accorded the highest priority and that the delivery of their capabilities is synchronized throughout the Department. We are also involved in the Enhanced Planning Process which will dictate in several months a more refined Joint Programming Guidance for Components' investment. And, in addition to our standard budget reviews for GIG-related activities, we have begun a series of Net Centric Program Reviews aimed at determining a program's net centric qualities both from a management and systems engineering perspective. These reviews will help Components and program managers comply with net-centric attributes, implement the DoD Data and Information Assurance Strategies, align programs with both the Joint Technical Architecture (JTA) and the Net-Centric Operations Warfare Reference Model (NCOW RM), establish priorities and design transition plans in line with GIG Enterprise Services.

Finally, a GIG End-to-End (E2E) Systems Engineering (SE) Oversight activity has been stood up to work with the DoD community to resolve interoperability, interface and standards issues between and among all programs critical to the incremental development and deployment of the GIG. This effort addresses the challenges associated with making many independently funded, managed and executed programs operate in an integrated fashion in implementing the GIG vision. This activity is essential to ensure that the design decisions made by component programs will result in a true DoD enterprisewide information grid. In order to provide the conceptual integrity and unity of command necessary to deliver seamless, net-centric capabilities to warfighters and users, the GIG E2E SE oversight process is the single SE oversight process for the GIG, and it is the integrating SE oversight activity for the GIG. All other SE activities on GIG programs or GIG mission areas are subject to E2E SE oversight by this group. The objective is to translate legacy and emerging/planned GIG systems into a ubiquitous, secure and robust network.

Within these processes, the ASD(NII)/DoD CIO is actively working to ensure the most judicious use of resources that are required to implement the GIG architecture and its related activities.

There are five programs/efforts key to the enterprise information environment defined by the GIG Architecture: As a result of the work done on the GIG Architecture, the Department defined and is making progress on five programs/efforts key to the enterprise information environment: GIG-Bandwidth Expansion; Transformational Satellite Communications; Joint Tactical Radio System; Net-Centric Enterprise Services; and Information Assurance. The first three programs provide an integrated communications layer within the GIG that increases connectivity and eliminates bandwidth as a constraint while the latter two efforts provide the basic infrastructure and protection services required to effectively operate the GIG. These enterprise-level programs and efforts, as well as our Horizontal Fusion Portfolio, are part of our GIG Implementation Roadmap. Key milestones and organizations are noted below:

Program: **GIG Bandwith Expansion**

Program Oversight:	ASD(NII)	
Program Management:	Defense Information Systems Agency	
Key Milestones:	Initial Operational Capability	1QFY05
	Full Operational Capability	1QFY06

Program: **Transformational Satellite Communications System (TSAT)**

Program Oversight:	ASD(NII)	
Program Management:	Air Force	
Key Milestones:	Critical Design Review	FY08
	Initial Operational Capability	FY13
	Full Operational Capability	FY16

Program: **Joint Tactical Radio System**

Program Oversight:	ASD(NII)
Key Milestones/Org:	Cluster 1—IOC FY07 (Provides for development and production of the Ground Vehicular and Rotary Wing configurations) Program Management: Army Cluster 2—IOC FY05 (Provides for development and production of a single channel JTRS handheld radio) Program Management: SOCOM Cluster 3/4—IOC FY09 (Provides for development and production of the airborne, maritime and fixed station configurations) Program Management: Air Force ESC; Navy SPAWAR and NAVAIR Cluster 5—IOC FY07 (Provides for development and production of the handheld, man-pack and small form factor (embedded) configurations) Program Management: Army PM WIN–T

Program: **Net-centric Enterprise Services**

Program Oversight:	ASD(NII)	
Program Management:	Defense Information Systems Agency (DISA)	
Key Milestones:	New Program Start	Oct 03
	Milestone A	Apr 04 (Technology Development)
	IOC will be determined at Milestone B	

Program: **Global Information Grid Information Assurance Program**

Program Oversight:	ASD(NII)
Program Management:	National Security Agency
Key Milestones:	Increment 1 July 04 (Initial IA architecture views and capabilities description) Increment 2 Dec 05 (Identification of new start programs) Increment 3 Sep 06 (End state vision)

Additional information on these programs may be found at these unclassified web sites.

- GIG-Bandwidth Expansion (GIG–BE)
- Transformation Satellite (TSAT)

http://www.losangeles.af.mil/SMC/MC/

- Joint Tactical Radio System (JTRS)
- NetworkCentric Enterprise Services (NCES)
- Information Assurance (IA) (a Department-wide effort, not a program)

Mr. SAXTON. We have raised concerns with Internet Protocol version 6 (IPv6) and whether it will provide the same quality of service that the Department's computing network protocols presently provides. Why did you make the IPv6 decision without conducting tests at scale (i.e. Division Level Simulation) to prove this architecture will at the very least reproduce existing quality of service?

Secretary STENBIT. We have every confidence that IPv6 will not only reproduce but exceed the existing quality of service available using the older technologies. Furthermore, we have in place the test plans and associated funding to demonstrate transition readiness. IPv6 is a key commercial standard that is a part of the GIG strategy and will be the convergence protocol throughout the Department for interoperability. Achievement of IPv6 attributes is important to our warfighters because they will provide us the ability to support many highly mobile tactical users on the integrated GIG. IPv6 packet switching will allow networks to dynamically form, support the information exchange from many users to many information sites, allow for the automatic and dynamic management of information flows and facilitate and support our concepts of light, agile early entry joint forces.

Policy regarding this transition has been established to ensure that DoD's major investments in transforming the GIG to support net-centric operations are built to operate in this IPv6 world that is our objective. Services and Agencies are actively

participating in transition planning to implement this policy in a way that addresses and mitigates risks and leverages ongoing commercial work.

DoD's transition direction ensures that systems continue to operate with IPv4 until the necessary IPv6 performance, scalability, security, and interoperability criteria (developed by the Joint Staff) are successfully demonstrated. A set of pilot IPv6 implementations in selected DoD operational systems will begin in FY05. These pilot IPv6 implementations will be critical to identifying and addressing enterprise transition issues as well as demonstrating the readiness to complete the enterprise transition. In addition, to support these pilots as well as the overall transition, a comprehensive and coordinated IPv6 focused distributed testing effort across DoD's test labs and facilities is being planned. A DoD IPv6 Transition Office is also being established to provide the technical leadership and coordination across DoD's Services and Agencies and provide common engineering analyses and solutions.

Even today we have started towards our goal of demonstrating transition readiness by testing IPv6 capabilities through initiatives such as implementing IPv6 in the Defense Research and Engineering Network and our participation through existing Service and DISA testbeds/labs with industry, academic and the North American IPv6 Task Force in the large scale, ongoing Moonv6 testbed/demonstration.

In addition to the IPv6 activities discussed above, thorough developmental and operational testing remain fundamental to the acquisition process for all new systems. Therefore, as each system goes through the acquisition process, we will perform detailed test for system performance, to include IPv6 functionality and quality of service. These tests will ensure that systems are operationally suitable and effective, as tested against validated system requirements. Furthermore, the Joint Staff is developing details, including quality of service, for a Net Ready Key Performance Parameter (KPP) that will be applicable to all components of the GIG.

Mr. SAXTON. What is Horizontal Fusion? What is the purpose of it? Is there another mechanism or tool(s) the Department can use to ensure interoperability without spending more money?

Secretary STENBIT The Horizontal Fusion (HF) Portfolio Initiative was created early in 2003 as part of the strategic investment plan of the DoD CIO which contains NCES, GIG BE, JTRS, TCS, and IA. This strategic investment plan is in response to the Secretary of Defense's vision of Force Transformation and to achieve "Power to the Edge" in the new battle space. HF is the catalyst that accelerates the implementation of a net-centric operations and warfighting capability utilizing the infrastructure and services provided by the strategic plan activities, concentrating on the "interconnection" or interoperability of data applications users and services which will result in substantially improved situational awareness and decision support to the warfighter. The warfighter will have total awareness of and access to all the data on the net but will pull only what is relevant to him based on his tasks or missions.

HF has many objectives but only one purpose: to support the vision of force transformation for the Department of Defense by making net-centric warfare an operational reality. By providing the seed money to existing programs of record and emerging technologies as appropriate, HF has begun the movement of Command and Control and Intelligence domain high priority data stores, applications, users and systems onto the internet-like enterprise infrastructure detailed within the Global Information Grid Architecture and provided by the initiatives within the DoD CIO investment portfolio. Programs of record that are capable of modifying their existing operational baselines to meet the standards and requirements of a net-centric environment as well as provide significant value to services/agencies/organizations other than their own are considered for participation in each fiscal year portfolio. Selection criteria used to determine the final make-up of the portfolio each year include, but are not limited to:

(1) The extent to which Net-centric Enterprise Services will by utilized by the program

(2) The ability for the program to meta-tag their data and expose that catalog/index to the larger enterprise audience for consumption

(3) The extent to which the programs' participation will assist the DoD in addressing net-centric technology/policy/cultural "speed-bumps" (i.e., security policy, the use of smart software agents, the ability to implement cross-domain information exchange, TTP and concepts of operation)

(4) The length of time the modifications will take

(5) The cost of the modifications

(6) The programs' ability to move the modifications into its operational base and maintain the changes

Additional considerations are given for service and COCOM priorities as well as for those proposals that specifically target gap areas identified by the activities and demonstration of the previous year's participants.

In addition to accelerating operational net-centric warfare, HF provides critical feedback to the DoD CIO investment portfolio members pertaining to implementation issues associated with the specifications and guidance of each area. This feedback helps to refine these products as they are developed so that they are more definitive and easier to implement by Program Managers.

In FY03, the Horizontal Fusion Portfolio proved the concept of net-centric warfare as achievable across the DoD enterprise during the Quantum Leap–1 demonstration in August 2003. Several capabilities are now available on the operational SIPRNet. In FY04, HF has concentrated on adding high priority data (both conventional data stores and non-traditional sources of data) in meta-tagged format consistent with the DoD Data Management Strategy, net-enabling additional user support sense-making tools while refining the tools from the FY03 effort, and implementing version 1 of a net-centric web-enabled security service that supports both Cross-domain information exchange and secure wireless devices.

There is no other mechanism or tool (i.e., governance body, service, agency, organization, or effort) responsible for the execution of this evolution toward an enterprise net-centric capability. The DoD CIO is responsible for the development and the implementation of the Global Information Grid Integrated Architecture, which underpins all mission area and capabilities. HF was designed to leap-frog Programs of Record into that net-centric infrastructure; preserving legacy investment while providing additional capability and information availability. The Department is at the beginning of GIG implementation. Over the course of the current Future Year's Defense Program, the objectives of the GIG architecture will be proven out, a large portion of the DoD IT inventory will have migrated to net-centricity, the standards and implementation guidance will be mature and understood, new start acquisitions will be coming on-line already net-centric, and there will no longer be a need for the Horizontal Fusion "jump start"

Mr. SAXTON. Can you please help us to understand the Transformational Communications Network (TCA) with respect to the Global Information Grid (GIG). Is TCA a subset of GIG or visa-versa or are the two entities managed separately? What organization is responsible for the interoperability of the TCA and the GIG?

Secretary STENBIT. The Transformation Communications Architecture (TCA) is the element of the GIG Integrated Architecture that provides the details for and expansion of the GIG's space segment. OASD(NII) has responsibility to ensure that DoD programs that make up the TCA (including the Transformational Satellite Communications System (TSAT)) are interoperable with others programs comprising the GIG. OASD(NII) performs this function by working with the other OSD staffs, the Joint Staff, the Services, Combatant Commands, Agencies and the Transformational Communications Office function on the HQ Air Force staff.

OASD(NII) has established a GIG end-to-end systems engineering oversight activity that works with existing DoD decision-making processes. These processes include the acquisition process; the planning, programming, budgeting and execution process; the capabilities development process; and the DoD Chief Information Office Information Technology standards and policy process. Altogether, the GIG systems engineering oversight activity, working in conjunction with these corporate decision making processes, will ensure the GIG and TCA are interoperable.

Mr. SAXTON. Is DoD planning to follow a knowledge-based approach toward key Global Information Grid (GIG)-transport layer acquisitions. For example, will it have assurance that technologies are sufficiently mature before committing to Tactical Satellite (TSAT) product development?

Secretary STENBIT. A knowledge-based approach outlines a specific approach advocated by the General Accounting Office (GAO). The example you give is for a DoD space program, Transformational Satellite Communications System (TSAT). DoD acquires space systems using DoD National Security Space (NSS) Acquisition Policy 03–01. DoD acquires non-space systems using DoDI 5000.2, Operation of the Defense Acquisition System. To address the TSAT space program example you give, we would note that the application of the GAO's "Commercial Best Practices Model for the Acquisition Process," is principally based on a study of acquisitions with much larger production runs, and therefore applies more to non-space programs—not as well to space programs. The DoD NSS 03–01 is tailorable to meet the DoD space community acquisition development needs. NSS 03–01 provides a focused independent review process to address significant problems, and it allows the Milestone Decision Authority (MDA) authority and flexibility to manage risk. This has been done for the TSAT program. The DoD has detailed technology maturation plans consistent with commercial and government best practices for space systems

that will ensure TSAT technology is sufficiently mature to meet our planned TSAT first launch in 2011. For each key technology associated with TSAT, a milestone chart has been developed that includes metrics by which the technology maturation will be assessed. The intent is to ensure that all technologies are matured to technology readiness level 6 (TRL–6) before the technology is considered for integration into TSAT. Should any technology not meet TRL–6 in a time frame commensurate with the milestone schedule, a technology off ramp has been defined that identifies an alternative solution using mature technologies. If these more mature technologies need to be used in the first increment of TSAT, a significant increase in space communications for our warfighters will have been achieved (compared to what would be delivered with AEHF). Under this scenario, subsequent increments of TSAT would incorporate the more sophisticated technologies, as they mature, in order to more fully meet our warfighter's needs.

For example, in the critical area of lasercom, significant risk reduction efforts are in place. Over the next 27 months, the single access lasercom, currently at TRL 5, will go through extensive breadboard/brassboard design and test activities that culminate in a performance characterization in the government Optical System Verification Suite. The lasercom terminal will achieve TRL 6 and enter the build, test, launch phase after the successful completion of the risk reduction and design development activities. While we continue on our path to achieve TRL 6 by PDR, it is critical that the technology work be done in the context of design development so that TSAT technology development is synchronized with the overall design. This acquisition approach is consistent with best commercial and government practices for space systems.

Mr. SAXTON. What measures have been taken to ensure that traditional challenges to large scale, joint DoD initiatives—such as funding constraints and competition among the services and defense and intelligence agencies—are addressed when developing and implementing critical GIG components and over the near- and long-term?

Secretary STENBIT. The GIG is the infrastructure foundation for Net-Centric Operations across the Department, and as such it will provide information services critical to all Services and defense and intelligence agencies. OASD(NII) is addressing traditional challenges to large-scale, joint initiatives by: (1) developing and communicating a netcentric vision; (2) providing a framework for developments leading to the vision in the form of architectures, standards, and design tenets; (3) facilitating a community-wide forum for identifying and resolving technical, programmatic, and funding issues; (4) funding demonstrations of key net-centric capabilities that clearly show the tangible benefits of the GIG vision to the stake-holders; and (5) reducing funding competition between the Services by centrally funding the GIG-BE capabilities which were previously funded within the Services' operations and maintenance budgets.

The GIG has become the unifying and underlying vision, architecture and approach to meeting the companion visions and concepts being evolved within each of the Services. Without the five key programs comprising the GIG, Service concepts such as C2 Constellation, ForceNet, LandWarNet, and C2 on the move can not be realized. Furthermore, programs such as FCS and WIN–T are dependent on the successful completion and delivery of these five key GIG programs. To ensure that these programs meet the Services' needs and that they are protected in the PPBE process, the DoD has established the GIG end to end systems engineering activity. This activity ensures that the needs of all stakeholders are accounted for in the GIG key programs, to include programs schedule synchronization, funding prioritization, and technical interoperability of the systems being delivered into the GIG.

Mr. SAXTON. What measures has DoD taken to ensure that the GIG architecture is applied as required and that complementary architectures for new and existing systems are in compliance with the GIG architecture?

Secretary STENBIT. The GIG Architecture (GIGA) is the foundation for the Department's warfighting and business processes. As a result, several processes within the Department have been modified to ensure new and updated acquisitions are compliant with the GIG. The Joint Staff has restructured the DoD's requirements identification and validation process to focus more on top-down capability-based needs and on acquiring integrated capabilities that show through their complementary architectures how proposed systems resolve capabilities shortfalls and how systems support and depend on each other. This new process differs from its predecessor which primarily examined the justification for an acquisition as opposed to how it fit within the joint warfighting strategy and concepts. The new process is described in a Chairman, Joint Chief of Staff Instruction (CJCSI) 3170.01C, titled the Joint Capabilities Integration and Development System (JCIDS). In the JCIDS process, the GIG architecture is the foundation on which the utility and adequacy of a proposed

system and its associated architecture are compared. Consequently, for a new or enhanced acquisition to proceed through the development process, the program manager is required to explain how his acquisition and architecture fits into the GIG.

The JCIDS process requires a program manager to describe performance parameters that the acquired system must attain before a production decision is reached. Many of these parameters describe unique performance for the system being acquired (ships, planes, or guns), but there are selected parameters that must be addressed for every acquisition. These are called key performance parameters, and net-readiness is one of them. The Net-Readiness Key Performance Parameter (NR KPP) directs the program manager to ensure the new system provides needed data in a timely fashion and to ensure that the system is properly connected to the GIG with information assurance protections. To satisfactorily address this key performance parameter, the program manager uses the Net-centric Operations and Warfare Reference Model which provides standards for compliance. For example, the newly acquired system must be connected to the GIG by using internet protocols. It must provide information assurance protection, post data on the GIG for all users to access, and use available enterprise services. The use of the NR KPP is mandated by an updated DoDD 4630.5 and DoDI 4630.8, "Interoperability and Supportability of Information Technology and National Security Systems." Both of these are currently being promulgated.

Ensuring the newly acquired or updated system and its associated architecture are compliant with the reference model and that they satisfy the net-ready key performance parameter is the function of the acquisition process. There are multiple checks in the process to test for compliance. There are milestone decisions in the development process that ensure appropriate tests are established for checking compliance. There are checks to ensure funding for tests is available, and there are checks performed by independent agencies to check the results against established pass/fail criteria. The acquisition and the resourcing processes are the means to ensure that new and updated systems will be compliant with the GIG. Furthermore, the GIG systems engineering activity will be used to asses key programs compliance with the GIG toolset, to include the GIG architecture, standards, guidelines and policies. Before a key program progresses through the acquisition process, it must meet these defined criteria. Finally, as a system is delivered, it will be evaluated for GIG compliance and integration in the GIG End-to-End Evaluation Facilities recently established by DoD.

QUESTIONS SUBMITTED BY MR. MEEHAN

Mr. MEEHAN. With "transformation" the watch-word in the Pentagon and the "information age" well upon us, IT investment decisions will provide the foundation for all future military capability. The disciplines of intelligence, command and control, and targeting all require accurate and timely information, and American industry is making "information dominance" a reality for the U.S. military. It won't be easy to ensure the availability of information in a secure fashion—anytime and anywhere. Some challenges are technological, others are organizational. The coordination of the requirements and budgeting process should be a paramount concern. In the past, joint weapon systems planning and budgeting has not always succeeded. There is no denying it: redundancies continued; and joint programs have failed. I understand the issuance of an "IT portfolio management policy" is soon expected from the Department. I am told this policy will guide investment decisions to ensure the compatibility, interoperability, and efficiency of DoD IT systems. But let's be honest: policies come and go. And without focused attention to execution, even the best policy will fail. Perhaps our witnesses can provide us with some additional insight in this regard.

Secretary STENBIT. The Department's recently released IT Portfolio Management policy has several features to provide assurance that IT systems are compatible, interoperable, efficient, and effectively support DoD missions and functions. Specifically, the policy requires that IT system investments be:

- Architectural- and capabilities-based;
- Inextricably linked to the mission and functions being supported;
- Considered, evaluated and governed within the framework of DoD longstanding decision-making processes (i.e. JCIDS, Acquisition Process, PPBE processes);
- Performance-and results-based

In addition, portfolios will be managed by senior leaders in specific business and war fighting functional areas that we refer to as domains. These individuals will

take an active role in implementing the policy. The leadership they provide and the requirements of the Department's Portfolio Management policy will combine to provide a sound foundation for providing greater focus, accountability, discipline and structure during the analysis, selection, management control, and evaluation of IT investments.

General BOUTELLE. The Army has indeed recognized the necessity for and value provided by a coherent, rationalized funding strategy for our IT investments. In previous years, we analyzed our IT investment decisions to determine where there was a capability gap between our operational requirements and funding strategy, and then worked at adjustments in funding decisions. While this strategy helped from the perspective of identifying capability gaps, there was room for improvement to ensure interdependency issues were resolved, full interoperability (within the Army and Joint community) was guaranteed, and to confirm we were providing the best across the-Army solution in meeting capability requirements.

Over the past six months an improved process has been initiated within the Army CIO/G–6, specifically the construct of a Capital Planning and Investment Management process for use within the Army, fully meeting the Clinger-Cohen requirements with regard to IT investment management and oversight. This process will take full advantage of the earlier lessons learned regarding capabilities-based analysis, while taking a future focus to guarantee the IT Investment Strategy provides fully interoperable, efficient systems which are fielded taking into account any interdependencies and system migration plans. We will prepare our strategy for planned IT expenditures ensuring it is fully in line with the future direction and strategy for DoD and the Army, while providing the required resources needed for our Soldiers who are deployed or preparing to deploy.

The Army CIO/G–6 Capital Planning and Investment Management Process is beginning to demonstrate true benefits as we make difficult funding choices. From the technical perspective, we have the expertise to make the sound investment decisions to best benefit the Army. From the organizational view, this process provides the coordinated, constructive, rigid review across the Army staff required to ensure we are using our resources wisely. Interoperability is a requirement that the Army has endorsed, and I am committed to making it work; our Capital Planning and Investment Management process is the vehicle we will use to get there.

General RADUEGE. We are engaged at very senior levels in supporting Departmental efforts associated with improved coordination of the requirements and budgeting process.

General THOMAS. The Marine Corps complies with Department of Defense and Department of Navy (DoN) guidance and directives. Within the DoN, the Marine Corps IT portfolio management is governed by a framework that spans policy, architecture, and acquisition. In conjunction with the DoN, the Marine Corps is implementing Department-wide portfolio management led by designated Functional Area Managers (FAMs). Mirroring the Global Information Grid (GIG) functional domains, specific roles and responsibilities are being carried out by the FAMs for developing and maintaining their respective domain-level portfolios of systems that support their functional areas of responsibility. Furthermore, the Marine Corps Information Technology Steering Group (ITSG), with representatives from the Deputy Commandants of the Marine Corps and the FAMs, guides and supports our internal enterprise approach for selecting IT solutions. In addition, our FAMs, or their designated representatives, are working with the Joint Staff Functional Capabilities Boards (FCBs) and the DoD Principal Staff Assistants (PSAs) to address IT considerations across the DoD.

Mr. MEEHAN. The Department says it wants better coordination among IT requirements, budgeting, and acquisition. But since passage of the Goldwater-Nichols Act of 1986 and the creation of the Joint Requirements Oversight Council, jointness has been an institutionalized goal with formal mechanisms to achieve it—even as the Department identified the development of information technologies as a priority. How is the current effort to better coordinate joint initiatives an improvement over what has been tried in the past, and why should we have confidence that it will prove more successful?

Secretary STENBIT. In 2002, the Joint Staff initiated a study in which OASD/NII and service representatives participated to evaluate problems associated with the existing requirements generation process. The study included OASD/NII and Service representatives, and it looked at all requirements, not solely those for IT. It found that the requirements process was a bottom up process, that it was Service-centric, and that it did not fully consider the needs of the joint warfighter. Together, this resulted in continued stove-piped solutions. Furthermore, the study determined that the analysis supporting requirements definition was limited in scope. IT systems were not necessarily integrated, and this created interoperability problems in the

field. Duplication existed, evolutionary acquisition of capabilities was not institutionalized, and the needs of the joint warfighter were not well prioritized or effectively considered.

Last summer, the Joint Staff instituted the change from its Requirements Generation System to the Joint Capabilities Integration and Development System. This capability-based approach is a top down process for identifying capability needs based on National Military Strategy, Department of Defense Strategic Planning Guidance, the priorities of the Combatant Commanders, and joint warfighting needs. The new system institutes an analytic process for identifying capability gaps, and it mandates a broader joint review of capability proposals. It engages the acquisition community earlier in the capability definition process and improves coordination throughout the Department and the agencies. One key change to the process was to establish a Net Centric Functional Capabilities Board (FCB) which is co-chaired by OASD (NII). This FCB will ensure that joint net centric capabilities are identified and clearly defined as an input to the acquisition process, and it will make recommendations to the Joint Requirements Oversight Council (JROC) so that top priority requirements are addressed at the highest levels. As a result of these changes, the JROC will have more comprehensive information upon which to base its decisions for validating joint warfighting capabilities and ensure it provides more informed advice and recommendations to the Secretary of Defense for acquisition, programming, and budgeting decisions.

Mr. MEEHAN. Over the course of the next few months the DoD will establish the criteria for the next round of base closings. Several DoD installations-such as Hanscom Air Force Base-play a critical role in the development and support of IT programs. What level of involvement has your office had-or will it have-in drafting such criteria? What steps to you plan to take to make sure that the unique needs of the IT related mission and existing IT infrastructure sites warrant are given appropriate weight in the base closure process?

Secretary STENBIT. The Department published its proposed final selection criteria in the Federal Register on February 12, 2004 (69 F.R. 6948). By operation of law these criteria became final on March 15, 2004. The Department's execution of the BRAC process and application of the selection criteria will treat all installations equally and fairly. Military value is the primary consideration for a closure or realignment recommendations. Information technology capabilities are elements of military value and as such, captured within criteria one through four. The Department will consider military value in a way that incorporates these information technology elements.

Mr. MEEHAN. Your testimony says the GIG (gig) architecture is recognized as the underpinning for all mission and capabilities architectures developed by the Services and DoD agencies. How is this assured? Is this a formalized process?

Secretary STENBIT. Each of the Services has demonstrated its commitment to the GIG Architecture and to the Net-Centric Operations and Warfare (NCOW) Reference Model, and each is developing its architectures and information technology acquisition plans in accordance with the enterprise-wide view defined by the GIG Architecture and NCOW Reference Model. The central role of the GIG Architecture, the NCOW Reference Model and the related GIG toolset and revised oversight processes are formalized in DoD and Joint Staff policy relating to architecture development, requirements definition, resource allocation, and acquisition. Each of those processes requires conformance, compliance, or alignment to the GIG Architecture, the NCOW Reference Model, the JTA and other tools noted in our earlier response. In practice, the conformance, compliance, or alignment is assured through the work of the Joint Requirements Oversight Council, the Defense Acquisition Board, the Information Technology Acquisition Board, as well as the recently established Net-Centric Assessment process. A specific example of formalizing the process is the direction that all systems that go through the JROC must have a Net Ready KPP. The policies that govern the requirements definition and acquisition processes, for example, include specific net centric reviews and interoperability assessments.

Mr. MEEHAN. Provide additional insight into "IT portfolio management policy." What is Navy's perspective on adherence to the policy?

Admiral ZELIBOR. The Navy will comply with the Department of Defense and Department of Navy compliance guidance and directions. Navy is ensuring system C4ISR compliance through "The FORCEnet Compliance Checklist" and the "Joint Technical Architecture" (JTA) for interoperability standards. Navy's intent is to ensure joint interoperability to enable maritime forces in joint and coalition operations.

Mr. MEEHAN. With the advent of FORCEnet, what has changed in the Navy process for coordinating requirements, budgeting and acquisition? How is the process

under the FORCEnet concept any different than the one existing prior to its inception? What has changed?

Admiral ZELIBOR. FORCEnet has substantially transformed the Navy and Marine Corps in both process, product, and organization: Navy and Marine Corps offices were realigned to support FORCEnet implementation, providing increased organizational efficiency and effectiveness; the budget development process was significantly enhanced, better connecting warfighter needs and experimentation results to investment planning; an improved process to transition technology capabilities to the warfighter was developed and implemented; FORCEnet capabilities-based requirements, architectures, and standards were initiated, significantly improving the previous stove-piped, platform-based approach to requirements. Spiral 1 development of FORCEnet operational requirements, system/technical requirements, support/policy requirements, and implementation requirements have been completed; a FORCEnet Compliance Checklist and a supporting end-to-end governance process was implemented to support adherence to FORCEnet requirements; increased connectivity was established between the requirements process and the acquisition process, with enhanced involvement by the warfighter in each; the first FORCEnet at-sea event, "Giant Shadow," was successfully conducted with air, surface, and subsurface units—demonstrating and assessing Network Centric Warfare technology and tactics; the first FORCEnet joint operational event, "Trident Warrior 03" (TW–03), was successfully completed with Forward Deployed Naval Forces in coordination with Commander, U.S. Pacific Fleet and U.S. Pacific Command—delivering the first FORCEnet capability to the warfighter in substantially reduced time.

QUESTIONS SUBMITTED BY MR. BARTLETT

Mr. BARTLETT. What are your thoughts on the advantages and disadvantages of a government run, dedicated network versus a shared and managed services network for government-only use?

General BOUTELLE. Advantages of a government run dedicated network has a government managed network operations center with the flexibility to reconfigure itself to meet warfighter's unanticipated requirements with internal management lines to effect immediate changes. It can immediately deny access or block cyber-terrorism attacks with indifference to secondary network customers. Network features are tailored to the primary user, the warfighter, i.e. four levels of precedence capability on a voice network. Levels of security can be designed to meet the threat anticipated to the specific department's networks.

Disadvantages are: Long provisioning time for unique network requirements, network features being required on a group of switches that possibly could only need the feature on a few switches, and dedicated network management costs could be higher than shared network management costs.

On a Managed-services network, the advantages are: management and network operations overhead costs could be equitably shared by all using departments; all using departments could equitably share network features, personnel expertise could be shared with other like networks, products and services could be developed for multiple departments lowering their developmental and operational costs. Disadvantages are: Service Level Agreements (SLA) would have to meet varying departmental mission statements.

Mr. BARTLETT. Do our current networks provide the security, reliability and interoperability that a nationwide, dedicated fiber optic network would provide?

General BOUTELLE. The Army is transforming information assurance (IA) for its portion of the Defense Information Systems Network (DISN) in accordance with DoD directives and instructions and DoD guidance for implementation of the Global Information Grid (GIG) Architecture. Army IA is being addressed in a holistic manner and is viewed as an integral part of the GIG architecture, not as an add-on or overlay. The GIG is fundamental to DoD's transformation efforts and Army participates fully in DoD's End-to-End IA for the GIG and GIG Core Enterprise Services (CES), IA/Security efforts. The Army is building and fielding operational capabilities such as Future Combat Systems that are fully reliant on the assured capabilities of the GIG. This includes a future that will rely less and less on wired networks of any type and more on secure mobile/wireless computing capabilities, particularly for deployed forces. As current DoD communications capabilities transform into the GIG, these capabilities, wired and wireless, are becoming a robust, integrated, fully distributed, scaleable, flexible, and reliable communications and computing infrastructure that fully interconnects the armed forces by a trusted network.

Mr. BARTLETT. Today's security environment requires rapid, coordinated responses to national defense and homeland security requirements, do you feel a gov-

ernment-run dedicated network would enhance our government's response to these matters?

General BOUTELLE. Yes, a government-run dedicated network would enhance our response to national defense and homeland security matters. Events such as 9-11's telecommunications overload, daily Internet virus attacks on data networks, and natural disasters such as hurricane-destroyed communications infrastructures all demand a robust command and control (C2) system that is logically built to be available even in the event of disasters. The Defense Department's Defense Information Systems Network (DISN) is intentionally built to this higher standard. The Defense Department, Joint Staff, Services, and Combatant Commanders have policies that have put into place a robust C2 infrastructure that must be available to support commanders whenever and wherever it is needed. The Defense Switched (voice) Network, the Defense RED Switched Network (secure) (DRSN), the Defense Video-teleconference System (DVS), the Non-secure Internet Protocol Router Network (NIPRNET), and the Secure Internet Protocol Router Network (SIPRNET) are just some of the closed military infrastructures with robust bandwidth, systems interoperability, Computer Network Defense (CND) capabilities to restrict data port and protocol attacks, multiple domains and security levels, and higher reliability to negate network outages. While portions of these Defense Department networks ride some commercial telecommunications infrastructures, they are contracted and provisioned to ensure they have the necessary features to keep them available in times of crisis, threats, and war.

QUESTIONS SUBMITTED BY MR. THORNBERRY

Mr. THORNBERRY. Interesting that no one from the Joint Staff or Joint Forces Command is at this hearing. What are their requirements and how do they fit into this architecture?

Secretary STENBIT. Let me first say that while no one from the Joint Staff or Joint Forces Command was asked to testify at this hearing, I was accompanied to the hearing by RDML Nancy Brown, the Joint Staff Vice Director for Command, Control Communications and Computer (C4) Systems (J6). RDML Brown did, in fact, provide a statement for the record, and provided clarification during the hearing regarding the Joint Staff requirements and, newer, capabilities processes and how these are used to ensure that new requirements and capabilities are consistent within the overall GIG architecture.

The Joint Forces Command (JFCOM) requirements reflect the Joint community. For example, JFCOM is responsible for building an integrated architecture reflecting the joint Command and Control (C2) Battle Management requirements. This architecture will provide the Battle Management (Tactical Level) joint requirements for C2. These requirements will be integrated into the Service C2 Transformational Initiatives.

Joint Staff requirements are addressed by six Functional Capabilities Boards (FCBs)—Force Protection, Force Application, Battlespace Awareness, Command and Control, Focused Logistics, and Net-Centric. The FCBs organize and analyze capabilities proposals within assigned functional areas; oversee development of functional concept; develop and maintain prioritized list of capability proposals and gaps; and ensure integrated architecture accurately represent the functional area.

General BOUTELLE. Joint requirements drive Army architectures. Joint operational requirements for the Army are framed in the Joint Operations Concept (JopsC), Systems requirements supporting the Joint environment are guided and ensured by the Joint Requirements Oversight Council (JROC), and the Joint Technical Architecture aligns Information Technology standards.

Admiral ZELIBOR. Respectfully, we must defer to the Joint Staff and the Joint Forces Command on this question.

General THOMAS. The Joint Staff and JFCOM fit into the Global Information Grid and adhere to the same common architecture framework and interoperability standards and policies as do the Services.

Mr. THORNBERRY. What incentives do the services have to make sure joint information system requirements are being met?

Secretary STENBIT. If a Service program does not meet the Net Ready Key Performance Parameter (KPP) or prove their compliance with the GIG architecture and standards, they are subject to delays and funding withholds.

General BOUTELLE. Army incentives occur at multiple levels. At the leadership level, Joint associated/related concepts and systems development get favorable funding decisions. At the architecture level, Joint technical standards, Joint functional capabilities boards, and Chairman Joint Chiefs of Staff Instruction (CJSCSI)

6212.01C compliance are used to develop an acquisition business case that leads to a favorable acquisition decision.

Admiral ZELIBOR. The FORCEnet Compliance checklist and a supporting end-to-end governance process are being implemented to support adherence to NCW/FORCEnet criteria. This will ensure that warfighter needs are addresses in a network-centric environment, that new platforms and systems contribute to achieving a "full-netted" force, and that legacy assets are integrated as fully as possible into FORCEnet.

General THOMAS. Marine Corps experiences from Operation Enduring Freedom (OEF) and Operation Iraqi Freedom (OIF) reinforce the priciple that we must emphasize jointness in our operational mindset and in the systems we acquire. All Services fully understand that jointness is an exponential multiplier of combat effectiveness during operations. The expeditionary, combined arms nature of the Marine Corps further necessitates that we interoperate with Joint headquarters and the other Services. Therefore, we have an operational imperative to support other Services in their system developments through active engagement.

Mr. THORNBERRY. Has OSD or the Joint Staff recently canceled or prevented a service program from going forward because it did not fit joint operational needs?

Secretary STENBIT. As a result of effective OSD and Joint Staff oversight, there are few instances in which a service program reaches a point where cancellation or termination is necessary. However, there are isolated cases where an ill-defined Service initiative is revealed, and such action is necessary. Such a case in point is an Air Force program called the Situational Awareness Data Link (SADL) that was terminated in July 2002. This decision was made after extensive coordination among Joint Staff, USD (AT&L), ASD (NII) and the Interoperability Senior Review Panel that included JFCOM. The many serious questions raised about SADL included the lack of joint and coalition interoperability, spectrum supportability issues, invalidated operational requirements, lack of fundamental acquisition discipline, and failure to conduct operational effectiveness and suitability testing. The Air Force subsequently decided to pursue the joint and interoperable capability inherent in the Joint Tactical Radio System.

General BOUTELLE. Army canceled the Comanche program with OSD and POTUS approval. Termination of Comanche reflects the Army's recognition of a vastly changed global security context and national security challenges. The threat environment has changed and the Comanche platform was based on a threat that no longer exists. This directly influences how the Army fights and looks to the future to think about fighting.

Admiral ZELIBOR. DoD and DoN policies and processes are shaping system development to ensure joint operational needs are being met. Respectfully, we must defer to the OSD on the specifics of this question.

General THOMAS. DoD and DoN policies and processes that shape system development to ensure that joint operational needs are being met. We have no direct knowledge of OSD or Joint Staff decisions concerning other Service or Defense Agency programs that failed to adequately address joint operational needs.

Mr. THORNBERRY. It seems to me that DoD is becoming increasingly reliant on space and satellites for its communications and for information, yet almost every space program is delayed and over budget. What is causing all the risk in these programs?

Secretary STENBIT. DoD relies heavily on space assets. Recent experiences in Iraq and Afghanistan demonstrate that combat forces depend on them for information-related to intelligence, Positional, Navigation and Tracking data, and weather. Space provides the critical force multiplier to our combat troops. Space assets require that we deal with new and complex technologies, however, and cutting edge technologies present major management challenges associated with cost and performance. Additionally, unlike most DoD systems, satellites are bought in quantities of ten or less, and due to the expense of the satellites and their associated launch activities we must reduce risk through ground testing, engineering models, and modeling and simulation. Mission success is our first priority, and this requires managing a program's risks, to include cost and schedule. Satellite acquisition programs often push the limits of what can reasonably be expected in meeting requirements, but we cannot allow a system to proceed until it is ready. In many cases, the first planned launch is adjusted to reflect our best estimate of the time required to deliver the required capability. Under Secretary Teets, as the Executive Agent for Space, is working hard to address these issues.

General BOUTELLE. It is certainly true that the Army has become increasingly reliant on space and space systems for communications connectivity, as well as the sensor information that is passed using that very connectivity. One of the keys to Army transformation is the low data rate, Beyond-Line-of-Sight (BLOS) mobile

connectivity that space systems provide the warfighter now, and the expected high bandwidth, mobile BLOS capability expected of future (2008-2020) systems. We know that these programs will significantly push technology over the next few years. Our system developers are working closely with the space system engineers in order to mature technologies to enable transformational capabilities for our combat forces in synch with the advent of systems such as the Transformational Satellites, Space Based Radar, and others. Program managers work hard to minimize risk by maximizing testing that can be accomplished on the ground, as well as building in redundancy wherever possible to minimize single points of failure in the systems, but space is an unforgiving environment, and Final Operational Tests rely on successful launches, always a risk with new systems, and successful on-orbit tests. There will always be risk with launch, test and operations—no matter how reliable the systems appear to be during ground development.

Admiral ZELIBOR. It is certainly true that DoD has become increasingly reliant on space and space systems for communications connectivity, as well as the sensor information that is passed using that very connectivity. However, cost growth remains problematic due to the impact from emerging technologies, evolving operational concepts and increased system requirements. The inherent high cost of space systems, together with the global demand by DoD for maximum possible information, results in programs that must push the technological envelope in order to enable transformational capabilities for our combat forces.

Space systems are by their very nature risky. While program managerswork hard to minimize risk by maximizing testing that can be accomplished onthe ground, as well as building in redundancy wherever possible to minimizesingle points of failure on the satellite, space is an unforgiving environment. There will always be risk with launch-no matter how reliable the vehicle.

General THOMAS. USMC participation in satellite communications is primarily the acquisition of ground satellite terminals. Emerging technologies, evolving operational concepts and increased system requirements frequently drive cost growth. Programs that push the technological envelope in order to enable transformational capabilities for our combat forces are inherently risky by their nature. This makes them susceptible to schedule delays and associated cost overruns.

Mr. THORNBERRY. Should we be looking at a different way to buy and launch satellites?

Secretary STENBIT. Yes, and we are. We are moving toward a more operationally responsive space lift. This will allow us to respond more quickly to our space needs. This is a major shift in how we currently operate our space programs. There are several ongoing initiatives in the Department to decrease the size, cost, and timelines of satellite development. In the near term, we plan to demonstrate a more responsive and less expensive launch system capable of placing nearly 1,000 pound payloads into low earth orbit. The results of these operationally responsive launch initiatives could transform the way we deliver space capabilities.

General BOUTELLE. The Army does not buy satellites, however we are full partners in designing, developing, building and deploying space based systems. The DoD Executive Agent for Space has been working to improve the acquisition of space systems, collating the best attributes of both the National Reconnaissance Office and the Services processes and codifying them in a new acquisition instruction. Army, under the leadership of SMDC/ARSTRAT has also undertaken a review of the Army's management of Space System Acquisition and will be providing a report and recommendations to the Chief of Staff this summer.

Admiral ZELIBOR. The DoD Executive Agent for Space has been working to improve the acquisition of space systems, collating the best attributes of both the National Reconnaissance Office and the Services processes and codifying them in a new acquisition instruction. Mr. Teets has been the Milestone Decision Authority for Navy's Mobile User Objective System for UHF Satellite Communications, and that arrangement has worked well.

General THOMAS. The Marine Corps believes that the pursuit of new technology and better processes to improve efficiencies while at the same time maintaining our advantage in space is a worthwhile endeavor.

Mr. THORNBERRY. Are you familiar with the Office of Force Transformation, ADM Cebrowski's program to launch smaller satellites on a more regular basis that would allow us to keep pace with technology and change the mindset from a one of a kind system to more of a routine manufacturing capability?

Secretary STENBIT. Yes, and we applaud these efforts at developing this new class of capability based orbital systems. We are tracking the progress of the new low cost launch programs both in private industry and in DARPA. We will also need to look at how best to build, check out and operate these small spacecraft. We expect these new systems will require changes in our satellite operations infrastructure and may

lead to a major change in how we work with industry to produce spacecraft. We must shorten the time between requirement and orbit.

General BOUTELLE. The Army is monitoring TacSat 1 as it sees similarities to the desired Space Based Radar (SBR) capabilities and the TacSat CONOPS. TacSat 1 offers a practical test bed for improving the SBR CONOPS. The SBR program has the potential to bring a constellation of satellites that would benefit from the "routine manufacturing capability", thus benefiting from economies of scale and an established production line. Space offers a unique vantage point. SBR's dual collection modes, combining moving target indicators with the ability to quickly switch to the radar imagery mode, makes for a robust, dynamic collection system. TacSat 1 delivers theater tasking and theater downlink, where space assets are directly available to theater commanders to support operations as never before. Theater tasking, coupled with theater downlink, offers unique capabilities to dynamically re-task the system to tailor collection to the needs of the commander, allows for adjusting the collection plans in real time, and thus and ability react to unfolding events in an unprecedented manner. The contributions of TacSat 1 and SBR to force protection, economies of force, precision engagement, and lethality offer great potential. The Army is coordinating with the Office of Force Transformation to schedule adiscussion Grow the Army's views on SBR to Adm. Cebrowski in hopes of forging common ground.

Admiral ZELIBOR. The Navy is very familiar with Admiral Cebrowski's small satellite program. In 2003, the Naval Research Laboratory (NRL) signed a Memorandum of Understanding with the Office of Force Transformation that assigned the NRL to act as program manager for the implementation of tasks and experiments defined by the OSD/OFT for Operationally Responsive and Experimental Adaptability for Space Based Systems.' The OFT program's purpose is the "development of operationally responsive space based systems" where "responsiveness will be exemplified by the ability to select desired payload capabilities and tailor the coverage in response to a particular operational engagement, conflict, or opportunity, and the ability of operational forces to task, access, and disseminate correlated data via the SIPRNET". To initiate this effort at transformation, OFT funded NRL to design and build the first demonstration satellite for this program, called TacSat-1. One of the goals for TacSat-1 is to demonstrate the capability to build a satellite, with military utility, in less than one year. TacSat-I is nearly complete and will meet this goal. The Navy will continue to support OFT in its quest to reach its goals. The Office of Force Transformation provided funds to the Naval Research Laboratory for the development of a small satellite called TACSAT-1.

General THOMAS. The Marine Corps has been watching the Office of Force Transformation's (OSD/OFT) Tactical Satellite (TacSat) Initiative but has not been directly involved in any of the related experiments.

Mr. THORNBERRY. What are the services doing to support this effort?

Secretary STENBIT. The Air Force Space and Missile Systems Center, Air Force Research Laboratory, Naval Research Laboratory, National Reconnaissance Office, the Defense Advanced Research Projects Agency, and the Air Force-funded DoD Space Test Program are working with Adm. Cebrowski's office to support these new concepts. Currently, the Naval Research Laboratory is building the first of these small spacecraft, TACSAT 1. The next one will be built by the Air Force Research Laboratory. All the Services as well as the Joint Staff are supporting the effort in determining which requirements may be met by these small, responsive payloads.

General BOUTELLE. The Army is monitoring TacSat 1 as it sees similarities to the desired Space Based Radar (SBR) capabilities and the TacSat CONOPS. TacSat 1 offers a practical test bed for improving the SBR CONOPS. The SBR program has the potential to bring a constellation of satellites that would benefit from the "routine manufacturing capability", thus benefiting from economies of scale and an established production line. Space offers a unique vantage point. SBR's dual collection modes, combining moving target indicators with the ability to quickly switch to the radar imagery mode, makes for a robust, dynamic collection system. TacSat 1 delivers theater tasking and theater downlink, where space assets are directly available to theater commanders to support operations as never before. Theater tasking, coupled with theater downlink, offers unique capabilities to dynamically re-task the system to tailor collection to the needs of the commander, allows for adjusting the collection plans in real time, and thus and ability react to unfolding events in an unprecedented manner. The contributions of TacSat 1 and SBR to force protection, economies of force, precision engagement, and lethality offer great potential. The Army is coordinating with the Office of Force Transformation to schedule a discussion of the Army's views on SBR to Adm. Cebrowski in hopes of forging common ground.

Admiral ZELIBOR. The Navy is supporting OFT's effort by having NRL act as program manager for OFT's program, as well as by building the first demonstration satellite for the program, TacSat-1. In addition, NRL and AFRL have signed a Memorandum of Understanding whose purpose is to provide a framework for a strategic partnership between them to engender cooperation in space-related S&T to support the DoD and national space enterprise. Within the context of this MOU, NRL and AFRL are discussing their respective roles in future OFT efforts, and in other DoD "responsive space" programs.

General THOMAS. We support the Department's efforts regarding Admiral Cebrowski's small satellite program. The Marine Corps will continue to support the OFT in their quest to reach their goals relative to this initiative.

Mr. THORNBERRY. By DoD's own estimates, they are anywhere from 80 to 95 percent reliant on the relatively unprotected commercial backbone for their communications. Since our adversaries are watching what we are trying to accomplish with network centric warfare, it would make sense that they would be pursuing asymmetrical means to attack in this area. What is DoD's plan to improve communications survivability—both physical and cyber?

Secretary STENBIT. DoD protects its networks from both physical and cyber threats using an integrated defense-in-depth strategy. Networks are isolated from the Internet and public telephone system to the maximum extent possible. Where they do connect, the connections are aggressively monitored. Network switching and routing infrastructure components are located in secure locations and maintained by cleared government and contractor technicians. The diversity of the national and international long haul information transport infrastructure provides excellent protection of our networks from physical attack.

Vulnerability of single point local connections off the long haul network to DoD bases is often problematic. To alleviate the potential of single point failures, DoD, as part of its Global Information Grid Bandwidth Expansion program, engineered fully diverse connectivity (multiple physically separate paths) to our most critical installations. Complementing these technology based protective measures is a robust management and operations structure. Global network management and computer network defense activities are coordinated through an established command structure. The Global Network Operations and Security Center (GNOSC), and US STRATCOM's component commands led by the Joint Task Force for Computer Network Operations, provide oversight, direction and guidance in the management and defense of DoD networks and systems worldwide. This integrated structure is designed for continuity of operations across centers and allows 24x7 visibility of DoD networks and systems.

General BOUTELLE. From the cyber perspective, end-to-end protection of information transiting the unprotected commercial backbone is accomplished using multiple encryption processes. In the near term, for unclassified but sensitive data we employ Public Key Infrastructure and virtual private network (VPN) technologies to ensure the integrity, authenticity, and confidentiality of the data. So that data cannot be manipulated by asymmetric warfare attacks, we are improving identity management by testing a number of biometric applications and are identifying long-term requirements for developing Dynamic Access Control or DAC capabilities. DAC is the development of access control matrices that grant access to data based on user privileges. The DAC mechanism realizes the need-to-know paradigm and users will only be given access privileges if those privileges are required on a particular network. For classified transmissions, we employ National Security Agency communications security encryption devices to ensure end-to-end security. For mobile/wireless computing devices, we are crafting, as a minimum, a three-tier security approach to negate the cyber threat. The mobile computer will have a firewall to protect the device from asymmetric attack modalities. Data transport will be protected with a VPN and a data encryption package resident on the mobile computing device will protect data at rest in the case of theft of the device. To increase survivability in case of physical destruction, the Army has implemented continuity of operations plans by creating redundant facilities in a number of locations with multiple/diverse communications paths that will assume operations in the case of disruption or physical destruction of the primary sites and networks.

General RADUEGE. DISA has long recognized the fragility of our commercial telecommunications infrastructure to not only hostile kinetic and cyber attacks, but also to unintentional disruptions such as system misconfigurations, backhoe cuts of fiber optic cable, fires in major switching centers, etc.

To protect the DoD's networks from cyber threats, we have specifically architected our networks to provide maximum isolation from the global Internet and commercial telephone switching systems. The switches and routers that comprise the backbones of these networks are in physically secured locations, protected to the secret

level, and maintained by cleared government and contractor technicians. In cases where our networks must "touch" commercial networks for interoperability, such as connections between our sensitive but unclassified IP router network (NIPRNET) and the Internet, we have implemented a defense in depth approach to securing, filtering, and monitoring these connections against attacks. This approach has proven to be extremely successful as evidenced by our ability to work unimpeded during numerous worms and distributed denial of service attacks that have plagued the Internet in recent years.

Protecting our networks from physical attacks has proven to be more difficult. While most national and international telecommunications providers have significant diversity in the long haul infrastructure, DoD bases are generally connected into this infrastructure through a single cable bundle through a single commercial central communications office. As result, most of our most critical installations can be isolated by a single cable cut, switch failure, or car bomb attack. While we do have DoD SATCOM backup worldwide, and a DoD owned microwave system in Europe, these systems provide only a fraction of the bandwidth we receive from the commercial telecommunications providers. The Global Information Grid Bandwidth Expansion (GIG-BE) program is being implemented in a way that will address these vulnerabilities at the most critical DoD installations. GIG-BE is providing fully diverse connectivity into these installations over a DoD owned and operated infrastructure. This will effectively eliminate the commercial single point of failure and significantly increase the reliability and survivability of communications for our most critical installations.

Finally, a robust management and operations structure also helps to overcome these kinetic and cyber risks. Global network management and computer network defense activities are coordinated through an established command structure. The Global Network Operations and Security Center (GNOSC), and US STRATCOM's Joint Task Force for Computer Network Operations, both located at the Headquarters, Defense Information Systems Agency provide oversight, direction and guidance in the management and defense of DoD networks and systems through an interdependent and comprehensive structure. DISA operated regional centers in critical locations around the world, including Scott Air Force Base, Illinois, Stuttgart, Germany, Honolulu, Hawaii, and Manama, Bahrain provide direct support to the Combatant Commanders which combined with the Joint Task Force Service Components ensures a coordinated, global response to kinetic or cyber events and allows effective prioritization of restoral efforts, identification and monitoring of critical links as well as the coordination and direction of the activities of commercial service providers. This cohesive structure is designed for continuity of operations across centers and allows 24x7 visibility of DoD networks and systems. These centers working in concert provide for the on-demand rerouting of information based upon critical mission requirements.

Admiral ZELIBOR. We are reducing our dependencies on commercial satellites as military capacity is increasing while continuing to leverage commercial satellites where appropriate. We fully support DoD's Information Assurance Strategy goals, because Navy fully appreciates the increased survivability necessary for operating in the network-centric warfare environment.

General THOMAS. Commercial telecommunications backbones are typically composed of several telecommunications components, including the backbone transport media, carrier-class switching technologies, network technology management capabilities, and customer point of presence technologies. In addition to these technical assets, there are several key non-technical components that are critical in supporting telecommunications capabilities, including operations and management personnel, administrative support functions, and physical telecommunications facilities, including network operations centers, telecommunications equipment facilities, administrative support facilities, etc. Each of these assets is subject to potential attack by adversaries seeking to diminish or disrupt the capability of United States forces to communicate effectively.

As part of the Global Information Grid (GIG), the Marine Corps will enhance network survivability through the key concepts of network and network service ownership and strong physical and technical controls over those government-controlled capabilities to protect the communications capabilities within the Marine Corps Enterprise Network (MCEN). This is a layered information assurance strategy to protect the infrastructure.

It incorporates a mesh architecture that ensures redundancy to transport backbone. It includes network management capabilities and carrier switching components that are owned by the government and are operated by cleared government or government contractor personnel. Further, all switching equipment will be installed in government owned or controlled facilities with strong physical protections.

This will ensure that management and control can be maintained, and corrective action can be effectively made during an accident or malicious attack scenario.

Mr. THORNBERRY. The Global Information Grid is clearly an essential effort for realizing-networkcentric operations and achieving improved interoperability. Do you think we are at the point where we need a System's Engineer for the Global Information Grid? If so, how would you envision such an organization operating and what level of resources would be required to perform the level of systems engineering that are traditionally applied to major system acquisition programs?

Secretary STENBIT. Systems engineering continues to be an essential part of the GIG development. Systems engineers have assisted in developing a GIG Architecture, NetCentric Operation Warfare (NCOW) reference model, Data Management Strategy, guidance on overarching Information Assurance, Enterprise Services, and they have defined interfaces and standards in the Joint Technical Architecture. Now that portions of the GIG are being acquired and implemented, systems engineering is more decentralized to take advantage of the supporting infrastructure that each Service already has in place. Implementation plans are being synchronized by the Services with on-going platform (fleet) modernization and system migration initiatives. OSD has established working groups to maintain and evolve standards, protocols, and program-program interfaces. These working groups also serve as a forum for developers of the GIG to address issues and risks to the successful implementation of the GIG.

Systems engineering oversight, led by DASD (NII), focuses the systems engineering talent on GIG programs to address cross-cutting issues from a global perspective. Each program also has unique challenges, specific to the operational environment, maturity of the technology, and complexity of the products being developed. These are handled with resources within each program. Systems engineering is heavily involved in the beginning of a program, through design. As the products enter test, subsystem integration, and operational test and evaluation, the system engineering involvement increases once again. At any instant in time, each program contributing to the development of the GIG will be at a different stage of development, and it will have varying degrees of systems engineering involvement. However, OASD (NII) oversight, policy enforcement, and working group collaboration will remain omni-present.

General BOUTELLE. Yes. The Defense Acquisition Executive has recently tasked all Service Component Acquisition Executives to establish their System Engineer who will coordinate with the DoD System Engineer. Additionally, a Systems Engineering working group, comprised of all service components, is currently in nascent stages at the OSD level.

General THOMAS. Because the Global Information Grid (GIG) reflects the collection of processes, personnel, systems, networks, technologies, and standards needed to guide transformation to a net-centric environment, it is an inherently complex enterprise and environment. DoD, working in cooperation with Components, Services, and Defense Agencies, has established many of the design principles and standards to guide its evolution. Questions relating to organizational principles and resourcing at the Department wide level should be addressed to OSD.

○