STATEMENT OF

LINTON WELLS II

ACTING ASSISTANT SECRETARY OF DEFENSE

FOR NETWORKS AND INFORMATION INTEGRATION

AND

DOD CHIEF INFORMATION OFFICER

BEFORE

THE HOUSE ARMED SERVICES COMMITTEE

TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIIES

SUBCOMMITTEE

MARCH 3, 2005

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

"Tactical C4 Systems: Why Does the DoD Have So Many Different Systems Performing the Same Functionality?"

Introduction

Good afternoon Mr. Chairman, Representative Meehan, and members of the Subcommittee on Terrorism, Unconventional Threats and Capabilities. Thank you for the opportunity to testify before you about an important element in the war against terror and ongoing campaigns in Afghanistan, Iraq and other countries around the world – tactical command, control, communications and computer (C4) systems.

As you review the Department's fiscal year 2006 budget submission and assess the daily news reports from overseas, you may ask, "what are we getting for the money we are investing in C4 systems?" "Is anyone in the Department of Defense ensuring that we're getting something for the dollars spent – is there a hammer to ensure results in this area?" "Who has the authority to force discipline and change in this area?" And, as you have asked in the title of this hearing, "it appears there are numerous duplicative C4 systems in use by the Services, has anyone terminated any of these?" Let me try and answer these now, and tell you why our C4 systems are so critical to our warfighters and winning the war against terror.

DoD's Information Vision

The information revolution is changing our society and the way we live, generating fundamental societal change, and creating a global environment in which communications technology is expanding the ability to create, use, access and share knowledge. The Department's network-centric transformation has been, and will be, critical for national defense,

as global, non-traditional threats compel DoD to engage in unfamiliar regions, work with a changing array of coalition partners and face challenging demographic, religious and environmental dimensions of security. The Department needs to be able to operate across the full spectrum of threats and environments, from general war to present circumstances where our adversaries use asymmetric approaches that allow them to avoid confronting superior U.S. forces head on, while exploiting social, political, and economic seams that have the potential to produce catastrophic consequences. We see adversaries who use terrorist weapons such as improvised explosive devices (IEDs) against their own people, their own infrastructure and against deployed multinational forces. These adversaries have easy access to the same global commercial base that we do, and can exploit the same communication and information resources as the American public. They have proven that they are an intelligent, thinking and adaptable enemy, able to keep the playing field level even as U.S. capabilities evolve.

Policy and resource planning must be integrated to realize the Department's commitment to accelerating the transformation to net-centric capabilities. The Office of the Assistant Secretary of Defense for Networks and Information Integration (OASD(NII)) works closely with other elements of the Office of the Secretary of Defense, the Joint Staff, the Services, Agencies, Joint Forces Command and other combatant commanders to eliminate technical and organizational impediments. In particular we have partnered with the Joint Staff, the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Joint Forces Command, and the Services to update the Joint Battle Management Command and Control (JBMC2) Roadmap, which provides a comprehensive, executable plan for improving how we organize, train and equip to achieve Joint battle management command and control capabilities. We seek to leverage existing processes to ensure that net-centric capabilities are taken into

account when formulating requirements through the Joint Capabilities Integration and Development System (JCIDS) and when developing and deploying system capabilities through the acquisition process and the Planning, Programming, Budgeting and Execution (PPBE) process.

The Department's vision of Network-Centric Operations is to foster an agile, robust, interoperable and collaborative DoD, where warfighters, business and intelligence users all share knowledge on a secure, dependable and global network that enables excellent decision-making, effective operations and network-centric transformation. We want to deliver "Power to the Edge." We see soldiers, sailors, marines, airmen and civilians of DoD all connected by a network they trust and that facilitates the building of trusted relationships. Empowered by access to quality information and unconstrained by artificial boundaries, there is no limit to what American servicemen and servicewomen will be able to accomplish.

As part of DoD's information age transformation, the network is emerging as the single most important contributor to combat power and protection. Network-Centric Operations provide an unprecedented potential to attain critical advantage over adversaries within available resources in the long-term. Increased information sharing capabilities also have had positive repercussions in the Global War on Terror.

Network-Centric Operations allow the Department to leverage both commercial trends and new DoD thinking about missions and operations. OASD (NII) has supported an accelerated military transformation to expand access to information and eliminate unnecessary duplication of systems. As the pace of this change accelerates, we are both developing advanced DoD systems and addressing how to respond to commercial product life cycles that may be measured in months or weeks instead of the years over which the government budget process is developed.

The Global Information Grid Foundation

To respond to this increased pace of technological change and evolving operational demands, the Department needs to converge multiple programs into one seamless capability and rapidly transition to there from legacy systems. To this end, the Global Information Grid (GIG) is one of the key enablers that form the foundation of the DoD's Network-Centric Transformation. The GIG represents a globally interconnected, end-to-end set of information capabilities and processes for collecting, processing, and managing information on demand to warfighters, policymakers, and support personnel. The GIG fulfills a fundamental principle of Network-Centric Operations by securely connecting people and systems regardless of time or place, providing vastly superior situational awareness and better access to information for accelerated decision-making.

To enable the transformation needed to meet the challenges posed by today's new threat environment, the Department needs a single, secure grid providing seamless end-to-end capabilities to all warfighting, policy-makers and support personnel. The objective is to support defense and national security requirements through all levels of conflict and contingency support. The network-centric operations bring together joint, high-capacity, networked sensors, weapons systems and decision tools, merging key tactical, operational and global functional capabilities. The GIG supports all Department missions with information technology, including joint operations, joint task force and combined-task force commands, with the most effective and assured information-handling capabilities.

Perhaps the single most transformational and operationally significant attribute presented by the GIG vision will be that U.S. servicemen and women 'at the edge' will no longer be at the mercy of someone remote from the fight determining what information they need. Specifically,

information posted to the GIG becomes available to all relevant users from the grid, allowing them to "pull" information according to their need or have it "pushed" to them based on pre-defined criteria. The GIG provides a critical foundation for the Department's Network-Centric vision by: (1) supporting the posting of data to shared spaces as early as possible; (2) providing users with an enhanced capability to pull required data from wherever they are, whenever they need it; and (3) ensuring information assurance measures are applied effectively and across the enterprise. The network-centric data strategy links together disparate systems and also provides the basis for coalition interoperability in a time of rapid transformation. Radio frequency spectrum issues become exceptionally important in this increasingly wireless environment.

To ensure that these families of programs are developed in a seamless and fully interoperable fashion, NII has established a new Senior Systems Engineering position reporting directly to the ASD(NII)/DoD Chief Information Officer. The Systems Engineer examines key initiatives associated with implementing the Department's network-centric vision; serves as a principal advisor on the end-to-end systems engineering and integration; is responsible for the development and oversight of the DoD GIG Systems Engineering Oversight Process; and provides input to the JCIDS, acquisitions and PPBE processes.

The basic premise of the GIG is to leverage technologies successfully used by most commercial data communications in the world today – an Internet Protocol (IP)-based infrastructure. Key to the success of the GIG are six major DoD programs that are the bedrock of network-centric transformation: four deal with transportation of information, one with enterprise services, and one with information assurance. The four transport components include terrestrial networks (GIG-BE, which is discussed more below), mobile networks using IP (Joint Tactical Radio System (JTRS)), space-based laser communications (Transformational Satellite

(TSAT) Communication Program), and teleports (which link the ground and space segments together). JTRS, the wireless radio segment, is based on the software programmable components, and ultimately will replace numerous Service-unique radios with common software radios that can be used in hand-held, mobile, vehicular, airborne, and maritime settings. This family of radios will bring much needed interoperability to tactical users who today have different radios that don't communicate with one another, and will bring joint wireless communications to U.S., allied and coalition forces. TSAT, the space-based segment of the transport layer, is critical because many users are deployed in areas where terrestrial fiber is unavailable, and many of our information sources, particularly intelligence, surveillance and reconnaissance capabilities, are airborne – making connecting to them difficult. This satellite communications capability provides high speed, secure, protected, dynamically allocated and efficiently utilized bandwidth to satisfy the warfighter's demands. The result is protected bandwidth on demand and communications on the move, which empowers our mobile forces and reduces last tactical mile bottlenecks.

The enterprise services component of the GIG consists of a suite of reusable core enterprise services such as (1) discovery of potential new users or data sources, (2) mediation between various data formats, (3) discovery of data and applications to solve problems, and (4) provisioning of the appropriate security services and keys to allow access to the data required. Prior approaches were built on point-to-point interfaces between systems. Hence, duplication of efforts occurred as each new point-to-point interface to share data was defined or upgraded. This network-centric, service-oriented environment enables the data from any system to be available to all users at all times, subject to security and access controls. In this environment new systems only need to be developed when new information is required. Capabilities can easily be offered

as value added services that provide tailored answers to problems, such as target tracking, blue force tracking, or current weather information by exploiting the information made available from existing systems. Users will pull the information they need, when they need it.

Finally, for the GIG to enable and empower people at the edge of the network, it must be secure and dependable. We cannot allow vulnerabilities to be the Achilles' heel. Therefore, the GIG security solutions must move away from the common approach of perimeter defenses to one that allow us to maintain real-time situational awareness in our networks. These information security features must be designed into the network from the beginning and not be an afterthought.

There are three concepts that complement individual programs and help shape the implementation of the GIG. (1) network operations and network management, especially at the tactical edges of the network, (2) spectrum management, which involves intensive planning, especially for tactical, mobile, ad-hoc networks; and (3) the net-centric data strategy, which enables different systems to access the same data but manipulate, process, format, or otherwise translate that data in accordance with the needs of individual users. It also provides the basis for coalition interoperability in a time of rapid transformation. Data will be posted to the network and applications will use the best data available on the network, no matter what system provides it, to enable end-user decision-making. Every sensor, platform, and user communicates directly with the network. Sensors not directly connected to the core network use feeder systems, such as the space-based TSAT and JTRS. The goal is to get the data from the sensor posted on the network for use by everybody at the first point where it become "consumable." Likewise, users can reach back to the network to get the data they need, processed by the applications they choose.

I'd like to point out two major success stories which clearly demonstrate the Department's unequivocal commitment to reaching its dual goals of achieving network-centric operations and ensuring the greatest return on our investment in information superiority initiatives: the Global Information Grid – Bandwidth Expansion (GIG-BE) and the Joint Command and Control (JC2) program.

GIG-BE

The GIG-BE is one of several programs that have been cited in testimony to this Subcommittee, and it is key to realizing the Department's enterprise information environment. It is providing a worldwide, ground-based fiber-optic network that will expand Internet-Protocol (IP)-based connectivity and at the same time effectively and efficiently accommodate older, legacy command, control and communications (C3) systems. This enables an exponential leap in ground-based voice, video and data exchange capabilities for the Department of Defense and the Intelligence Community. In less than three years, the GIG-BE program has moved from its original planning phase through its initial operational capability, and it will reach full operational capability at the end of this year. It represents a model for the close collaborative working relationships among all levels of Defense and Intelligence Community management that drive our corporate pursuit of network-centric operations. Under Defense Information Systems Agency (DISA) leadership, this program meets stringent COCOM, Service, Agency and national intelligence requirements, and it provides the ground-based foundation on which the Services and the Intelligence Community are basing complementary programs to deliver both superior combat effectiveness and effective and efficient peacetime operations in the future.

With an initial investment of $877 million, DISA is delivering a secure and redundant, state-of-the-art, ground-based optical IP network that will connect over eighty intelligence,

command and control and operational locations throughout the continental U.S. and the Pacific, European and Southwest Asian theaters. Twelve of these sites are fully implemented, and remaining installations are progressing on schedule. As a global, high capacity, optical communications system, the GIG-BE program reduces bandwidth-constraints for data exchange and instead provides sufficiently increased bandwidth to support combat operations. Moreover, it provides physically diverse routing services for DoD and the Intelligence Community by expanding the Department's core telecommunications backbone. This greatly enhances the reliability and the survivability of the entire network. Because the government now effectively owns the fiber and the optics of this network, it greatly facilitates our ability to upgrade its security and performance. Additionally, GIG-BE is critical to exploiting our reach back capability, which will maximize our continuing investments in critical airborne Intelligence, Surveillance and Reconnaissance and future combat support assets. With expanded bandwidth, the elimination of single points of failure and a high degree of network security and integrity, the GIG-BE program contributes significantly to meeting ground transport needs for voice, video and data.

The GIG-BE program is the first of its kind to bring high-speed, high assurance IP encryption (HAIPE) to DoD networks. The introduction of HAIPE devices, as a result of the National Security Agency's anticipatory development, will greatly increase our ability to bring secure net-centric capabilities to Intelligence Community and DoD operations.

The GIG-BE program is delivering much needed capabilities to decision-makers and warfighters alike. It represents a clear and continuing commitment among Defense and Intelligence Community leaders to achieving net-centric capabilities, and it demonstrates an exceptional return on our investment in information superiority assets.

Joint Command and Control (JC2)

Another network-centric initiative is the Joint Command and Control capability (JC2) which will replace the current family of Global Command and Control Systems (GCCS). It is a Pathfinder Program in the JBMC2 Roadmap. GCCS limitations stem from the fact that each military Service found it necessary to produce a tailored version of GCCS to support individual Service missions. This has led to limitations on a Task Force Commander's ability to use common applications, share data and coordinate planning activities, drawbacks that are most obvious when joint operations are being planned and executed. For instance, the commander may want to plan a combined Army and Marine Corps land maneuver with Air Force close air support and supporting naval fire. Given the limitations of today's legacy systems, the three component commanders would use their own readiness data bases to assign the necessary forces, their own planning systems to develop routing and support logistics, and their own report-back systems to determine progress during execution. This arrangement forces the planning process into a series of coordinating iterations to ensure resources are at the right place and at the right time. This planning process consumes time and effort that could be better spent in maneuvering and attacking the enemy.

JC2 will provide an integrated, seamless, network-centric means to accomplish this task. It is being designed for the Joint Force Commander to address mission areas in complete packages, for example, situation awareness and force protection instead of Service-centric tasks such as field artillery support or air tasking order development. It has been fully vetted within the Joint Staff's JCIDS process and the Department's acquisition and program and budget processes to best ensure the most judicious use of C2 resources. Indeed, funding for the family of GCCS programs is the primary source for funding JC2. Moreover, the current block of GCCS programs

is the last block and is being postured for the net-centric environment which will allow re-use of some of the GCCS applications in JC2.

The JC2 program demonstrates the Department's commitment to terminating legacy, Service-centric systems and reapplying their resources to joint systems that will operate in a network-centric environment.

Contingency Support and Migration Planning

One of the most critical areas for which OASD NII provides policy, oversight and guidance in this era of asymmetric warfare is in the area of communications and information management support for stabilization and reconstruction (S&R) operations. Experience in operations from the Balkans to Afghanistan and Iraq has shown us that warfighting, security and force-protection in post-conflict situations are inextricably tied to efforts to empower friendly governments and restore civil society. At the same time, we must ensure that solutions provided for those situations are consistent with the long-term vision for the GIG. To this end, we have established a new directorate within NII – Contingency Support and Migration Planning (CSMP). The goal is three-fold: (1) to provide NII-related support to contingency operations as appropriate, (2) to ensure the solutions implemented in contingencies move the Department towards the net-centric vision, and (3) to take potentially useful commercial solutions that may be discovered during contingency operations and convert them into programs of record, if appropriate. In this role, CSMP is building a close partnership with JFCOM's newly formed Joint Systems Integration Command.

Even as we support the normal processes of the Department through the GIG architecture, and network-centric operations, there are times when DoD communications and information management must be able to reach out beyond the boundaries of the military to

engage with non-traditional associates, such as international organizations, non-governmental organizations, and even commercial partners. In civil-military operations, information and communications technologies can be important contributors to the effectiveness of indigenous security services, magnets to attract the foreign investment needed for reconstruction, and critical enablers of the information flows that are the lifeblood of democratic societies. In these roles, CSMP is partnering with Joint Forces Command in the development of operational concepts and joint experimentation, with the regional combatant commanders to understand their contingency issues, with the Joint Staff to coordinate with the operating forces, and with other parts of OSD and the Services to understand the available technologies and acquisition opportunities.

In the process, we are helping to develop a doctrine for integrated operations, called by some "Joint operations with a capital J." These operations should be developed, practiced and responsive across, and among, joint U.S. military, combined coalition, US interagency, international organizations, Non-Governmental Organizations (NGOs) and, in some cases, commercial partners. The basic premise is that today's environment demands that DoD take a holistic approach to integrated, distributed, global operations, from combat, to S&R operations, to the sort of disaster relief and humanitarian assistance efforts we saw in the wake of the tsunami of December 26, 2004. The combination of rapidly deployable communications and collaboration capabilities, a group of people experienced in operating in such diverse environments, and a doctrinal underpinning will stand us in good stead in the future.

Conclusion

The imperative is to provide the tactical C4 needed by our men and women to succeed in the tasks they face around the world. The risk of failure is so dire – and conversely, the rewards for success are so high – in fighting the Global War on Terror, that we must give priority to C4

in our acquisition, program development and funding processes. In a fragmented world of non-state enemies and developing-nation allies, we must provide C4 capabilities to win the Global War on Terror and enable necessary redevelopment and democracy. We are continuing, then, to identify the best systems, and to study and engineer the human systems and processes needed to maximize them – in partnership with other parts of OSD, the Services and Defense Agencies, the Joint Staff, Joint Forces Command and other combatant commanders. This work must continue, and your help is essential if we are to succeed. Thank you.