Hearing before the{PRIVATE }
House Armed Services Committee

Subcommittee on Military Research and Development
and
Subcommittee on Readiness

March 8, 2000

Statement of
John S. Tritak
Director
Critical Infrastructure Assurance Office

Mr. Chairman, it is an honor to appear before you here today to talk with you about the National Plan for Information Systems Protection, Version 1.0. This Subcommittee has shown exceptional leadership on the matter of critical infrastructure assurance. I am grateful for the opportunity to discuss the Administration's efforts to achieve President Clinton's goal of establishing a full operational capability to defend the critical infrastructures of the United States by 2003 against deliberate attacks aimed at significantly disrupting the delivery of services vital to our nation's defense, economic security, and the health and safety of its people. This cannot be done without the support and participation of the Congress.

{PRIVATE }**I. Introduction**{tc \l 1 "**I. Introduction**"}

The Information Age has fundamentally altered the nature and extent of our dependency on these infrastructures. Increasingly, our Government, economy, and society are being connected into an ever expanding and interdependent digital nervous system of computers and information systems. With this interdependence comes new vulnerabilities. One person with a computer, a modem, and a telephone line anywhere in the world can potentially break into sensitive Government files, shut down an airport's air traffic control system, or disrupt 911 services for an entire community.

The threats posed to our critical infrastructures by hackers, terrorists, criminal organizations and foreign Governments are real and growing. The need to assure delivery of critical services over our infrastructures is not only a concern for the national security and federal law enforcement communities, it is also a growing concern for the business community, since the security of information infrastructure is a vital element of E-commerce. Drawing on the full breadth of expertise of the federal government and the private sector is therefore essential to addressing this matter effectively.

President Clinton has increased funding on critical infrastructure substantially during the past three years, including a 15% increase in the FY2001 budget proposal to $2.0 billion. He has also developed and funded new initiatives to defend the nation's computer systems from cyber attack.

In the 22 months since the President signed Presidential Decision Directive 63, we have made significant progress in protecting our critical infrastructures. In response to the President's call for a national plan to serve as a blueprint for establishing a critical infrastructure protection (CIP) capability, the *National Plan for Information Systems Protection* was released last month. It represents the first attempt by any national Government to design a way to protect those infrastructures essential to the delivery of electric power, oil and gas, communications, transportation services, banking and financial services, and vital human services. Increasingly, these infrastructures are being operated and controlled through the use of computers and computer networks.

The current version of the Plan focuses mainly on the domestic efforts being undertaken by the Federal Government to protect the Nation's critical cyber-based infrastructures. Later versions will focus on the efforts of the infrastructure owners and operators, as well as the risk management and broader business community. Subsequent versions will also reflect to a greater degree the interests and concerns expressed by Congress and the general public based on their feedback. That is why the Plan is designated *Version 1.0* and subtitled *An Invitation to a Dialogue* -- to indicate that it is

still a work in progress and that a broader range of perspectives must be taken into account if the Plan is truly to be "national" in scope and treatment.

~~Before I give you an overview of the plan, it is worthwhile to recognize two items that distinguish the efforts of the Defense Department's efforts from those of the rest of the Federal Government. First, because of their unique role, which this committee above all others knows very well, the Defense Department's efforts in this field are distinguished by different expectations and focus, different sources and levels of resources, and, in many cases, different laws which either help or hinder the Department's efforts (e.g. the Defense Production Act in the former and Posse Commutates in the later cases). Because of this unique role, the Defense Department's portion of the National Plan stands alone. The second distinction follows from the different expectations held for the Defense Department. The Department recognized the need to identify and address their critical infrastructure dependencies and protection issues much earlier than the rest of the Government, and is subsequently further ahead than their colleagues in the civilian agencies in addressing them. Indeed, they have been quite generous with their time and lessons learned in helping their civilian counterparts wrestle with these complex issues. My comments, therefore, will focus on the civilian side of the government's efforts with critical infrastructure protection, and I will leave it to Mr. Money to comment on the Defense Department's efforts.~~
~~{PRIVATE }{tc \l 1 ""}~~
{PRIVATE }**II. The Plan: Overview and Highlights**{tc \l 1 "**II. The Plan\: Overview and Highlights**"}

President Clinton directed the development of this Plan to chart the way toward the attainment of a national capability to defend our critical infrastructures by the end of 2003. To meet this ambitious goal, the Plan establishes 10 programs for achieving three broad objectives. They are:

Objective 1: Prepare and Prevent: Undertake those steps necessary to minimize the possibility of a significant and successful attack on our critical information networks, and build an infrastructure that remains effective in the face of such attacks.

> Program 1 calls for the Government and the private sector to identify significant assets, interdependencies, and vulnerabilities of critical information networks from attack, and to develop and implement realistic programs to remedy the vulnerabilities, while continuously updating assessment and remediation efforts.

Objective 2: Detect and Respond: Develop the means required to identify and assess attacks in a timely way, contain such attacks, recover quickly from them, and reconstitute those systems affected.

> Program 2 will install multi-layered protection on sensitive computer systems, including advanced firewalls, intrusion detection monitors, anomalous behavior identifiers, enterprise-wide management systems, and malicious code scanners. To protect critical Federal systems, computer security operations centers will receive warnings from these detection devices, as well as Computer Emergency Response Teams (CERTs) and other means, in order to analyze the attacks, and assist sites in defeating attacks.

Program 3 will develop robust intelligence and law enforcement capabilities to protect critical information systems, consistent with the law. It will assist, transform, and strengthen U.S. law enforcement and intelligence Agencies to be able to deal with a new kind of threat and a new kind of criminal -- one that acts against computer networks.

Program 4 calls for a more effective nationwide system to share attack warnings and information in a timely manner. This includes improving information sharing within the Federal Government and encouraging private industry, as well as state and local Governments, to create Information Sharing and Analysis Centers (ISACs), which would share information among corporations and state and local Governments, and could receive warning information from the Federal Government. Program 4 additionally calls for removal of existing legal barriers to information sharing.

Program 5 will create capabilities for response, reconstitution, and recovery to limit an attack while it is underway and to build into corporate and Agency continuity and recovery plans the ability to deal with information attacks. The goal for Government and the recommendation for industry is that every critical information system have a recovery plan in place that includes provisions for rapidly employing additional defensive measures (e.g., more stringent firewall instructions), cutting off or shutting down parts of the network under certain predetermined circumstances (through enterprise-wide management systems), shifting minimal essential operations to "clean" systems, and to quickly reconstitute affected systems.

Objective 3: Build Strong Foundations: Take all actions necessary to create and support the Nation's commitment to Prepare and Prevent and to Detect and Respond to attacks on our critical information networks.

Program 6 will systematically establish research requirements and priorities needed to implement the Plan, ensure funding, and create a system to ensure that our information security technology stays abreast with changes in the threat environment.

Program 7 will survey the numbers of people and the skills required for information security specialists within the Federal Government and the private sector, and takes action to train current Federal IT workers and recruit and educate additional personnel to meet shortfalls.

Program 8 will explain publicly the need to act now, before a catastrophic event, to improve our ability to defend against deliberate cyber-based attacks.

Program 9 will develop the legislative framework necessary to support initiatives proposed in other programs. This action requires intense cooperation within the Federal Government, including Congress, and between the Government and private industry.

Program 10 builds mechanisms to highlight and address privacy issues in the development of each and every program. Infrastructure assurance goals must be accomplished in a manner that maintains, and even strengthens, American's privacy and civil liberties. The

Plan outlines nine specific solutions, which include consulting with various communities; focusing on and highlighting the impact of programs on personal information; committing to fair information practices and other solutions developed by various working groups in multiple industries; and working closely with Congress to ensure that each program meets standards established in existing Congressional protections.

I would like to highlight a few of the programs in the remainder of my testimony. In these programs, the Administration seeks to accomplish two broad aims of the Plan – the establishment of the U.S. Government as a model of infrastructure protection, and the development of a public-private partnership to defend our national infrastructures.

A. The Federal Government as a Model of Information Security

We often say that more than 90% of our critical infrastructures are neither owned nor operated by the Federal Government. Partnerships with the private sector and state and local governments are therefore not just needed, but are the fundamental aspect of critical infrastructure protection. Yet, the President rightly challenged the Federal Government in PDD-63 to serve as a model for critical infrastructure protection – to put our own house in order first. Given the complexity of this issue, we need to take advantage of the breadth of expertise within the Federal Government to ensure that we enlist those Agencies with special capabilities and relationships with private industry to the fullest measure in pursuit of our common goal.

The Federal component of the National Plan is presented in two sections, one describing the efforts of civilian Federal Departments and Agencies to protect their critical systems, the other describing the efforts of the Department of Defense. Given its mission to defend the Nation, the Defense Department has been among the first to respond to the challenge of protecting its own infrastructure. It serves as a model for other Departments and Agencies; its programs merit separate and detailed attention.

Accordingly, I will limit my remarks to CIP efforts being undertaken by civilian Federal Departments and Agencies, deferring to Assistant Secretary of Defense Money on matters relating to Defense Department's programs.

~~To this end, t~~The President has developed and provided full or pilot funding for the following key initiatives designed to protect the federal Government's computer systems:

Federal Computer Security Requirements and Government Infrastructure Dependencies. One component of this effort supports aggressive, Government-wide implementation of federal computer security requirements and analysis of vulnerabilities. Thus, in support of the release of the National Plan, the President announced his intent to create a permanent Expert Review Team (ERT) at the Department of Commerce's National Institute of Standards and Technology (NIST). The ERT will be responsible for helping Agencies identify vulnerabilities, plan secure systems, and implement Critical Infrastructure Protection Plans. Pursuant to existing Congressional authorities and administrative requirements, the Director of the team would consult with the Office of Management and Budget and the National Security Council on the team's plan to protect and enhance computer security for Federal Agencies. The President's Budget for FY2001 will propose

$5 million for the ERT.

Under PDD-63, the President directed the CIAO to coordinate analyses of the U.S. Government's own dependencies on critical infrastructures. Many of the critical infrastructures that support our nation's defense and security are shared by a number of Agencies. Even within Government, critical infrastructure outages may cascade and unduly impair delivery of critical services. The CIAO is coordinating an interagency effort to develop a more sophisticated identification of critical nodes and systems, and to understand their impact on national security, national economic security, and public health and safety Government-wide. These efforts support the work of the ERT in identifying vulnerabilities of the Government's information infrastructures, and provide valuable input to Agencies for planning secure computer systems and implementing computer security plans. This research, when complete, will permit the Federal Government to identify and redress its most significant critical infrastructure vulnerabilities first, and provide the necessary framework for well informed critical infrastructure protection policy making and budget decisions.

Federal Intrusion Detection Network (FIDNet). PDD-63 marshals Federal Government resources to improve interagency cooperation in detecting and responding to significant computer intrusions into civilian Government critical infrastructure nodes. The program – much like a centralized burglar alarm system – would operate within long-standing, well-established legal requirements and Government policies covering privacy and civil liberties. FIDNet is intended to protect information on critical, civilian Government computer systems, including that provided by private citizens. It will not monitor or be wired into private sector computers. All aspects of the FIDNet will be fully consistent with all laws protecting the civil liberties and privacy rights of Americans.

To support this effort, the Administration will propose funding in the President's FY2001 Budget ($10 million) to create a centralized intrusion detection and response capability at the General Services Administration (GSA). This capability will function in consort with GSA's Federal Computer Incident Response Capability, and assist Federal Agencies to:

- detect and analyze computer attacks and unauthorized intrusions;
- share attack warnings and related information across Agencies; and
- respond to attacks in accordance with existing procedures and mechanisms.

FIDNet is intended to promote confidence in users of Federal civilian computer systems. It is important to recognize that FIDNet has a graduated system for response and reporting attack and intrusion information would be gathered and analyzed by home-Agency experts. Only data on system anomalies would be forwarded to GSA for further analysis. Thus, intrusion detection would not become a pass-through for all information to the Federal Bureau of Investigation or other law enforcement entities. Law enforcement would receive information about computer attacks and intrusions only under long-standing legal rules – no new authorities are implied or envisioned by the FIDNet program.

One additional benefit of Government-wide intrusion detection is to improve computer intrusion reporting and the sharing of incident information consistent with existing government computer security policy. Various authorities require Agencies to report criminal intrusions to appropriate law enforcement personnel, which include the National Infrastructure Protection Center.

FIDNet will support law enforcement's responsibilities where cyber-attacks are of a criminal nature or threaten national security.

In short, FIDNet will:

- be run by the GSA, not the FBI;
- not monitor any private network traffic;
- confer no new authorities on any Government Agency; and
- be fully consistent with privacy law and practice.

Federal Cyber Services (FCS). One of the nation's strategic shortcomings in protecting our critical infrastructures is a shortage of skilled information technology (IT) personnel. Within IT, the shortage of information systems security personnel is acute. The Federal Government's shortfall of skilled information systems security personnel amounts to a crisis. This shortfall reflects a scarcity of university graduate and undergraduate information security programs and the inability of the Government to provide the salary and benefit packages necessary to compete with the private sector for these highly skilled workers. In attacking this problem through the Federal Cyber Services initiative described below, we are leveraging the initial efforts made by the Defense Department, National Security Agency, and some other Federal Agencies. The President's Budget for FY2001 will propose $25 million for this effort.

The Federal Cyber Services training and education initiative, highlighted by the President at the Plan's release, introduces five programs to help solve the Federal IT security personnel problem.

a study by the Office of Personnel Management to identify and develop competencies for federal information technology (IT) security positions, and the associated training and certification requirements.

the development of Centers of IT Excellence to establish competencies and certify current Federal IT workers and maintain their information security skill levels throughout their careers.

The creation of a Scholarship for Service (SFS) program to recruit and educate the next generation of Federal IT managers by awarding scholarships for the study of information security, in return for a commitment to work for a specified time for the Federal Government. This program will also support the development of information security faculty.

The development of a high school outreach and awareness program that will provide a curriculum for computer security awareness classes and encourage careers in IT fields.

The development and implementation of a Federal Information Security awareness curriculum aimed at ensuring computer security literacy throughout the entire Federal workforce.

Research and Development. A key component to our ability to protect our critical infrastructures now and in the future is a robust research and development plan. As part of the

structure established by PDD-63, the interagency Critical Infrastructure Coordination Group (CICG) created a process to identify technology requirements in support of the Plan. Chaired by the Office of Science and Technology Policy (OSTP), the Research and Development Sub-Group works with Agencies and the private sector to:

gain agreement on requirements and priorities for information security research and development;

coordinate among Federal Departments and Agencies to ensure the requirements are met within departmental research budgets and to prevent waste or duplication among departmental efforts;

communicate with private sector and academic researchers to prevent Federally funded R&D from duplicating prior, ongoing, or planned programs in the private sector or academia; and

identify areas where market forces are not creating sufficient or adequate research efforts in information security technology.

That process, begun in 1998, has helped focus efforts on coordinated cross-government critical infrastructure protection research. Among the priorities identified by the process are:

technology to support large-scale networks of intrusion detection monitors;

artificial intelligence and other methods to identify malicious code (trap doors) in operating system code;

methodologies to contain, stop, or eject intruders, and to mitigate damage or restore information-processing services in the event of an attack or disaster;

technologies to increase network reliability, system survivability, and the robustness of critical infrastructure components and systems, as well as the critical infrastructures themselves; and

technologies to model infrastructure responses to attacks or failures; identify interdependencies and their implications; and locate key vulnerable nodes, components, or systems.

The President's Budget for FY2001 will propose $606 million across all Agencies for critical infrastructure related R&D investment.

The need exists, however, to coordinate R&D efforts not just across the federal Government, but between the public and private sectors as well. A fundamentally important initiative that has the ability to pull disparate pieces of the national R&D community into closer relationships is the Institute for Information Infrastructure Protection (I^3P), an organization created to identify and fund research and technology development to protect America's cyberspace from attack or other failures. I will discuss this in detail when I address Public-Private Partnership issues.

Public Key Infrastructure. Protecting critical infrastructures in the Federal Government and private sectors requires development of an interoperable public key infrastructure (PKI). A PKI enables data integrity, user identification and authentication, user non-repudiation, and data confidentiality through public key cryptography by distributing digital certificates (essentially electronic credentials) containing public keys, in a secure, scalable, and reliable manner. The potential of PKI has inspired numerous projects and pilots throughout the Federal Government and private sectors. The Federal Government has actively promoted the development of PKI technology and has developed a strategy to integrate these efforts into a fully functional Federal PKI. The President's Budget for FY2001 will propose $7 million to ensure development of an interoperable Federal PKI.

To achieve the goal of an integrated Federal PKI, and protect our critical infrastructures, the Federal Government is working with industry to implement the following program of activities:

- *Connect Agency-wide PKIs into a Federal PKI*: DoD, NASA, and other Government Agencies, are actively implementing Agency-wide PKIs to protect their internal critical infrastructures. While a positive step, these isolated PKIs do not protect infrastructures that cross Agency boundaries. Full protection requires an integrated, fully functional PKI.

- *Connect the Federal PKI with Private Sector PKIs*: Private sector groups are actively developing their own PKIs as well. While a positive step, these isolated PKIs do not protect infrastructures that cross Government or industry sector boundaries.

- *Encouraging development of interoperable Commercial Off-the-Shelf (COTS) PKI Products*: Limitation to a single vendor's solution can be a serious impediment, as most organizations have a heterogeneous computing environment. Consumers must be able to choose COTS PKI components that suit their needs.

- *Validating the Security of Critical PKI Components*: Protecting critical infrastructures require sound implementation. The strength of the security services provided to the critical infrastructures depends upon the security of the PKI components. Validation of the security of PKI components is needed to ensure that critical infrastructures are adequately protected. NIST is pursuing a validation program for PKI components.

- *Encouraging Development of PKI-Aware Applications*: To encourage development of PKI-aware applications, the Government is working with vendors in key application areas. One example is the secure electronic mail projects that have been performed jointly with industry.

B. Public-Private Partnership

Inter-dependent computer networks are an integral part of doing business in the Information Age. America is increasingly dependent upon computer networks for essential services, such as banking and finance, emergency services, delivery of water, electricity and gas, transportation, and voice and data communications. New ways of doing business in the 21st century are rapidly evolving. Business is increasingly relying on E-commerce for its commercial transactions as well as for its

critical operations. At the same time, recent hacking attempts at some of the most popular commercial Web sites underscore that America's information infrastructure is an attractive target for deliberate attack or sabotage. These attacks can originate from a host of sources, such as terrorists, criminals, hostile nations, or the equivalent of car thief "joyriders." Regardless of the source, however, the potential for cyber damage to our national security and economy is evident.

The infrastructures at risk are owned and operated by the private sector. The use of information technology is so embedded in the core operations and customer service delivery systems of industry that inevitably, it will be they who must work together to take the steps necessary to protect themselves. We can help. The first major step is the elevation of awareness across industry of the "business case for action" for leaders within industry. They have a commercial interest in maintaining a secure business environment that assures public confidence in their institutions. We can also help identify problems, good practices in management policies and strategies, and publicize them, encourage planning, promote research and development, convene meetings. In short, we can act as a catalyst for industry to mobilize.

~~The security of information flowing over the information highway is a critical element of E-commerce, as well as to our national security. It is a necessary part of building trust in the accuracy and integrity of transactions made over the information infrastructure. There is a growing awareness that America's information infrastructure -- the basis of E-Commerce -- is becoming an increasingly attractive target for deliberate attack or sabotage.~~ A strategy of cooperation and partnership between the private sector and the U.S. Government to protect the Nation's infrastructure is the linchpin of this effort. The President is committed to building partnerships with the private sector to protect our computer networks through the following initiatives:

Institute for Information Infrastructure Protection (I^3P). The Institute would identify and address serious R&D gaps that neither the private sector nor the Government's national security community would otherwise address, but that are necessary to ensure the robust, reliable operation of the national information infrastructure. The President announced he would propose initial funding of $50 million for the Institute in his FY2001 Budget. Funding would be provided through the Commerce Department's National Institute of Standards and Technology (NIST) to this organization. The Institute was first proposed by the scientists and corporate officials who served on the President's Committee of Advisors on Science and Technology, and supported by leading corporate Chief Technology Officers.

The Institute will work directly with private sector information technology suppliers and consumers to define research priorities and engage the country's finest technical experts to address the priorities identified. Research work will be performed at existing institutions including private corporations, universities, and non-profit research institutes. The Institute will also make provisions to accept private sector support for some research activities.

Partnership for Critical Infrastructure Security. Last month, Commerce Secretary Daley met with senior representatives from over 120 major corporations, many Fortune 500, representing owners and operators of critical infrastructures, their suppliers, and their customers, to organize a Partnership for Critical Infrastructure Security. Industry has taken the lead on this effort, and is actively pursuing ways to assure their ability to deliver critical services.

The Partnership will explore ways in which industry and Government can work together to address the risks to the nation's critical infrastructures. Federal Lead Agencies are currently building partnerships with individual infrastructure sectors in private industry, including communications, banking and finance, transportation, and energy. The Partnership will serve as a forum in which to draw these individual efforts together to facilitate a dialogue on cross-sector interdependencies, explore common approaches and experiences, and engage other key professional and business communities that have an interest in infrastructure assurance. By doing so, the Partnership hopes to raise awareness and understanding of, and to serve, when appropriate, as a catalyst for action among, the owners and operators of critical infrastructures, the risk management and investment communities, other members of the business community, and state and local Governments.

National Infrastructure Assurance Council (NIAC). President Clinton established the NIAC by Executive Order 13130 on July 14, 1999. When fully constituted, it will consist of up to 30 leaders in industry, academia, the privacy community, and state and local Government. The NIAC will provide advise and counsel to the President on a range of policy matters relating to critical infrastructure assurance, including the enhancement of public-private partnerships, generally.

{PRIVATE }III. Conclusion{tc \l 4 "III. Conclusion"}

In conclusion, the National Plan is an important step forward. My staff and I are committed to building on this promising beginning, coordinating the Government's efforts into an integrated program for critical infrastructure protection in support of the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism, and the Federal Government, generally. We have much work left to do, and I hope to work with the members of this committee, indeed with the Congress as a whole, as we wrestle with this developing field. I look forward to your questions.

Statement by

The Honorable Arthur L. Money

Assistant Secretary of Defense for

Command, Control, Communications and Intelligence

and

DoD Chief Information Officer

Before The

House Armed Services Committee

Subcommittees on

Research & Development and Readiness

Hearing on

Information Superiority & Information Assurance: Meeting the Challenges of the 21st Century

March 8, 2000

For Official Use Only

Until Release by the

Committee on Armed Services

U.S. House of Representatives

Opening

Thank you Mr. Chairmen and members of the Subcommittees. I am honored to be here, and pleased to have the opportunity to update your committee on many of the issues we discussed roughly one year ago. I believe the United States Government and the Department is making significant progress in its quest to achieve information superiority, providing information assurance and protecting our critical infrastructures are absolute necessities if we are to truly achieve information superiority. Other testimony that you will receive today from the Joint Staff and Services will highlight the progress we've made over the past year in achieving both information superiority and information assurance.

DoD is in the process of a transformation that will better enable it to meet the mission challenges of the 21st century by taking full advantage of Information Age concepts and technologies. Information Superiority is a key enabler of this transformation and central to emerging warfighting concepts. Today I hope to articulate DoD's Information Superiority vision, goals, and strategy; delineate current initiatives and recent accomplishments; and set the stage for the future.

In essence, Information Superiority is about ensuring that the right information gets to the right people at the right time and in the right format, empowering them by a vastly improved shared understanding of the situation. As defined in Joint Pub 3-13, Information Superiority requires "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting and/or denying an adversary's ability to do the same." Information Superiority creates an advantage in the information domain that has been shown to result in a significant advantage in the operational domain.

The synergy resulting from the consolidation of Information Superiority and CIO responsibilities the Secretary of Defense has assigned me as the ASD(C3I) and the Department's Chief Information Officer, continues to yield significant technical, operational, and financial benefits. The consolidation of policy development and oversight of the Department's space

force structure and close coordination with the intelligence community has served to create synergies and better integrate all elements of Information Superiority into a coherent whole.

DoD is currently without peer in its ability to collect, process, and use information in support of traditional combat operations. DoD is currently acquiring and deploying information-related capabilities that will maintain, if not widen, its edge in this area. However, this information advantage is incomplete and fragile. It is fragile because the systems that collect, process, and disseminate the high-quality information that powers our organization and empowers our people are vulnerable. It is therefore imperative that DoD information and information processes are adequately protected lest adversaries are able to even the playing field by exploiting vulnerabilities in DoD C3ISR and space systems. The rapid proliferation of these technologies requires that DoD work to assure its information capabilities on a continuing basis. This makes the pursuit of Information Superiority a constant quest.

Our information edge is also incomplete because DoD does not yet possess "full spectrum" Information Superiority. The current edge the U.S. holds in traditional combat does not extend to asymmetrical conflicts or operations other than war.

In addition to the need to keep abreast of evolving mission challenges and adversary capabilities, continued investment in Information Superiority also makes sense purely from a return on investment (ROI) point of view. There is a growing body of evidence that shows the enormity of the impact that increased shared awareness and network-centric operations have on mission outcomes and efficiencies. DoD has only just begun to harvest the low-hanging fruit in this area and the best is yet to come.

In light of all this, Information Superiority priorities need to be continuously reevaluated in light of changing circumstances. Therefore, DoD has established the following set of Information Superiority goals to focus efforts, form the basis for measuring progress, and setting priorities:

(1) Implement effective programming for establishing information assurance (IA) and critical infrastructure protection (CIP).

(2) Build a coherent Global Information Grid (GIG).

(3) Plan and implement joint and combined end-to-end C3ISR and space integration.
(4) Promote the development of knowledge management and a skill-based workforce.
(5) Develop policies and procedures that will reinvent intelligence for the 21st century.
(6) Strengthen information operations, security, and counterintelligence.
(7) Promote electronic commerce and business process change.
(8) Foster the development of an advanced technology plan for Information Superiority.

DoD has assembled an ambitious set of initiatives in support of these goals, which are highlighted below. However, despite these efforts, weak links in the Information Superiority value chain exist. An examination of these weak links points to the necessity to increase investments in: information assurance; efforts such as the Global Information Grid designed to establish the connectivity and interoperability needed; collection and analysis capabilities and end-to-end integration of C3ISR and space capabilities; education and training and retention of a cadre of IT professionals; removal of legal impediments to protecting information and information processes; and electronic commerce and electronic business to make the business side of DoD more effective and efficient.

Impact of the Information Age

In less than one generation, the information revolution, characterized by the introduction of networked computers into virtually every dimension of our society, has changed how our economies work, how we structure our everyday lives, and even how we provide for national and international security. With the dawning of the information age, we have entered a new era – one of increasing interconnectivity and interdependency – an era that is not reversible. Although this interdependence brings both opportunities and risks, the benefits of the information revolution in the commercial world have been proven to far outweigh the risks.

Given the implications of this interdependency in the military arena, we must take steps to understand and manage these risks so their potential negative impact is negligible in terms of our overall military mission success. It is essential we do this because to achieve revolutions in both military affairs and business affairs –- the cornerstones of our new DoD and Joint Vision 2010 -- we must actively accept and embrace this new interconnected world. We have seen this need demonstrated in both our warfighting and peacekeeping mission areas, in Kosovo and East

Timor, as well as in our business operations where our acquisition cycle time has been reduced to 15 months for key information technology systems and even less for commercial-off-the-shelf technologies.

It is the capabilities offered by this new age that are at the heart of how the U.S. military intends to win future conflicts -- by massing the effects of our highly mobile, widely distributed, self-synchronizing military forces when and where desired – what we call Information Superiority and it is the heart of Joint Vision 2010. To be successful in Joint Vision 2010, we must have information superiority, built on such advances as enhanced battlespace awareness through a common operational picture.

INFORMATION SUPERIORITY EFFORTS.

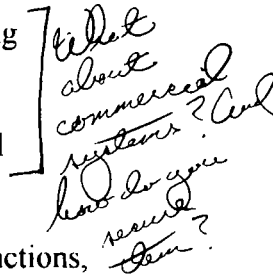
Global Information Grid (GIG).

The DoD and U.S. Intelligence Community (IC) share a vision of a secure, seamless, and collaborative information environment enabling full situational awareness during military operations and in other environments that will enable complete information dominance over any adversary. Today, numerous challenges hinder the visions contained in the DoD Joint Vision 2010 and the Strategic Intent of the Director of Central Intelligence. These challenges are so fundamental and pervasive that they raise serious doubts as to whether the DoD and IC can achieve their mutually supportive visions by 2010. Efforts initiated earlier this year, under the auspices of the DoD CIO , the National Research Council's Committee to Review DoD C3I Plans and Programs, and the Mission Information Management (MIM) Study, reinforce such doubts.

These efforts have shown the Defense Department's current information capabilities need modernization to provide value-added services, enhance efficiencies in information sharing, and promote interoperability (internally and with the IC) in support of military operations. In the past, initiatives pursued by the DoD and IC to attain information superiority have been decentralized and, most importantly, uncoordinated. While decentralized execution is necessary,

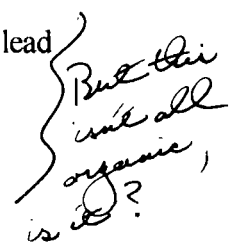
it can only be effective if the disparate entities act in concert toward a cogent, common goal of designing a seamless, collaborative and operationally effective "Information Enterprise."

Creation of a secure and assured global information enterprise (i.e., GIG) represents a key goal for the DoD CIO and Department of Defense. The is the 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 includes all owned and leased communications and computing systems and services, software (including applications), data, security services and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all DoD, National Security, and related Intelligence Community missions and functions, in war and in peace.



As the "front end" initiative for achieving this global information enterprise, the GIG will place emphasis on both the importance of information as a strategic resource and the need for greater compatibility of information technology with CINC, Service, and Agency mission critical operational processes. GIG development activities will provide the needed focus and management for the global information enterprise required to achieve information superiority by the year 2010. The GIG will provide capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms and deployed sites), and provide interfaces to coalition, allied, and non-DoD users and systems

The GIG will address the "enterprise view" with respect to communications, networking (i.e., local campus, operational, metropolitan, and wide-area), computing (i.e., local, regional and global), and interoperability as well as providing information management and distribution services, information assurance services and computing and network management services. This effort will lead to several new initiatives to manage the Department's worldwide information infrastructure as a coherent global networked information enterprise, providing forces with affordable information dominance, anywhere and any time.



Portfolio Management and Oversight.

At the same time, these interoperable information capabilities must be structured to accommodate the unique aspects of each community's operational portfolio. The operational portfolio will be linked to IT portfolios through the Portfolio Management and Oversight (PM&O) process. This process will replace the system-focused oversight with a process that will require each IT investment to be placed into a mission or functional thread (i.e., portfolio). Under this new process, the DoD CIO will evaluate IT investments based on their value to the mission or functional thread of which they are a part. The PM&O will:

- ensure IT investment decisions are directly linked to DoD mission, warfighter, and functional goals and outcomes;
- ensure IT investments result in high quality IT that enables measurable improvements to DoD mission-related and administrative processes; and
- ensure processes and systems are compliant with the Clinger-Cohen Act and related reform legislation and implementing guidance.

Y2K Lessons Learned.

The Department is continuing the process of collecting, analyzing, and synthesizing lessons learned from Y2K. Among the lessons that have been distilled from the DoD Y2K experience are that centralized guidance with decentralized execution works well, timely and accurate performance measurement is essential to management, and an accurate inventory of IT assets is fundamental to acquisition and configuration management.

We are taking steps on several fronts to institutionalize the Y2K lessons learned, particularly as we address the requirements of Section 8121. In addition to implementing the system registration and certification requirements discussed above, the Department will continue to improve configuration management procedures to enable information assurance across DoD and its partners.

Improvements to IT Education/Training and Retention of IT Professionals.

IT training is critical for the Department of Defense if it is to achieve information superiority. A strong incentive program is required to enable, acquire and retain a cadre of highly skilled IT professionals, both uniformed and civilian. The Department's IT specialists represent a world class force of IT warriors who have proven themselves the master of every IT challenge. But these specialists also possess skills that are in great demand by the private sector, so we must have a highly regarded incentive package. The incentives should include proficiency pay, enlistment and retention bonuses, training in advanced technology, opportunities to work with industry, academia, and government laboratories on high technology, and the opportunity to work on modern state-of-the-art systems supporting national security. We should not compete for people on the basis of dollars alone. We must give the soldiers and civilians who perform these functions a high quality work environment, career advancement opportunities, exciting challenges, and the means to perform important missions for our National Defense using modern technologies. In short, we need a total package to attract and retain these critical skills, a package that also addresses Quality of Life concerns.

The available pool of information technology civilian careerists is of great concern. DoD's ability to create and leverage Information Superiority depends on a skilled workforce prepared to tackle information-age problems with information technologies. A corps of appropriately trained and experienced IT professionals is the most critical component in protecting the Department's information resources against modern day cyber attacks. Individuals using, administering, and maintaining these systems must follow proscribed protective procedures, and know how to operate the equipment designed to mitigate these threats. Everyone, from the user in the foxhole to the weapon system developer to the professional network managers and system maintainer, must have some IT training. This not only provides the common knowledge base needed to leverage interoperable systems and networks, it also provides the more knowledgeable workforce needed to enable DoD to transition more efficiently as the IT environment changes. Additionally, DoD's IT training programs must keep pace with the rapidly evolving technology.

The challenge before us is to plan and implement initiatives that will create and sustain the cadre of civilian and military IT professionals needed to achieve information superiority in the 21st century.

An Integrated Process Team (IPT) was recently convened in the Department to examine the issues surrounding the training and retention of IT professionals. That IPT concluded that the DoD must create certain career management mechanisms to carry out its training and retention goals. Career management mechanisms with attractive career paths must be created and institutionalized to acquire and retain IT professionals to meet the technological demands of the Department. In other words, the problem is deeper than simply providing training courses and financial incentives to IT professionals. However, before that can be done with true efficiency and effectiveness, the Department must determine the size of its IT population and know precisely what IT activities it is performing. Today, the Department is unable to expediently determine this information. This problem not only exists within DoD, but government-wide.

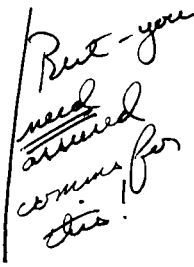
The Office of Personnel Management (OPM) is currently working with the Department and other Federal Agencies to rectify issues relative to IT classification, compensation and recruitment practices. To date efforts with OPM have resulted in *new parenthetical specialty titles* that more accurately describes IT functions, and a *competency-based job profile* to replace the current qualification standards for the Computer Specialist and Telecommunications series. The OPM initiative is in concert with the direction the Department is pursuing to develop *new parenthetical specialty titles* that will provide a basis to more accurately identify and track IT professionals. The use of the *new parenthetical titles* will allow monitoring of specific workforce trends and gaps to determine key occupations that require the use of pay flexibilities, that will provide a means to determine necessary career programs for the various IT professionals. Pilots of the new recruiting and classification techniques will start in March 2000 with the expected completion date of December 2000.

INFORMATION SUPERIORITY -- LESSONS LEARNED IN KOSOVO

The command, control, communications and computer (C4) systems provided for Kosovo operations were unprecedented in terms of capacity and variety of services, due to the communications infrastructure in Europe, both military and civilian, which are among the most robust and flexible available to the U.S. in any theater of operations. In addition, extraordinary

efforts were made to bring additional C4 capabilities into the theater, even though this impacted other U.S. military commitments worldwide. The widespread use of video teleconferencing and other advanced technologies for command and control and collaborative planning presented numerous limitations and challenges. These operations, however, highlighted the need for better interoperability with our allies as well as among the Services.

Operation Allied Force saw the first extensive use of sensor platforms deployed forward while their data reduction and analysis components remained at home base. This "reachback" technique was also used as part of the federated intelligence process to perform timely battle damage assessment, those reducing the number of scarce imagery analysts required in theater.



A wide variety of ISR systems installed on both manned and unmanned airborne platforms were critical to Operation Allied Force. These platforms are especially critical since they also support multi-INT collection activities in other areas of the world. Based on shortfalls in targeting capability and the stresses placed on ISR assets, initiatives are underway to optimize coordination between theater and national assets. We need to field those systems that improve precision and timeliness with which we detect, identify, track, and assess potential targets, regardless of constraints imposed by adverse weather, nighttime, concealment and deception techniques, or rapid movement. Ongoing programs such as Future Imagery Architecture, Global Hawk UAV, Predator UAV radar, synergistic sensor pairing, offer an improved sensor mix.

Operations in Kosovo saw an unprecedented use of UAVs, and as a result the **1999** Kosovo supplemental provided $37 million to replace and enhance Unmanned Aerial Vehicles (UAVs), $111M for additional EP-3 aircraft and enhancements, and $30M for other ISR-related investments. The supplemental funding is being used to replace Predator UAV losses, to repair Hunter UAVs and maintenance facilities, and to add a laser target designator capability to Predator. The FY 2001-2005 budget and program invests an additional $918M for a new JSTARS aircraft ($260M), accelerated acquisition and early deployment of the Global Hawk UAV system ($390M) and additional EP-3 and other ISR enhancements.

Overall DoD has funded more than $3.5 billion in enhancements to address the lessons learned from the Kosovo operation. Of this amount, over $1.9 billion was provided by the

Congress in the 1999 supplemental. In addition DoD devoted considerable attention to the Kosovo lessons learned during the development of the FY 2001-2005 program, with the result that an additional $1.6B was added to the program. Separately from this, DoD's program adds $1.5B to address the need for increased investment in TPED. Although plans to make TPED enhancements were well under way prior to the Kosovo conflict, this investment addresses many of the shortcomings in ISR integration that were identified during Kosovo operations.

The Intelligence Community is now in the process of overhauling current TPED systems and improving collection management processes to address the evolving threat and support the *Joint Vision 2010* environment. For example, NIMA has defined an end-to-end view of the *United States Imagery and Geospatial Information Service (USIGS).* NSA recently completed the *Unified Cryptologic Architecture Study 2010* that addressed challenges to the current U.S. SIGINT System. The MASINT community completed an end-to-end *MASINT Investment Strategy* that identified needed improvements to the current U.S. MASINT System. These efforts are steps in the right direction for integrating end-to-end capabilities within specific intelligence disciplines, but the emphasis in DoD ISR Vision 21 is on multi-disciplinary integration.

GPS and Space

In FY 1999 a number of enhancements to the Global Positioning System (GPS) satellite constellation were decided upon as part of the GPS modernization effort. These enhancements will satisfy the needs of all military and civil GPS users well into the next century. For the civil community, the Department of Defense and Department of Transportation agreed to add a second civil signal at 1227.60 megahertz. In addition, a third civil frequency has been planned in the "Aeronautical Radionavigation Service" band to meet the needs of civil aviation. Planned satellite improvements for the military include power enhancements, a new military signal, elimination of the dependence on the coarse/acquisition (C/A) signal for military signal acquisition, and modernized cryptography.

Because of the value of space systems to the U.S. economy and the military in future conflicts, the United States can expect attacks against U.S. and allied space systems. Consistent with treaty obligations, DoD must be able to ensure freedom of action in space for friendly

forces and, when directed, limit or deny an adversary's ability to use the medium for hostile purposes. To support space control objectives, DoD must sustain and improve surveillance and monitoring capabilities for all militarily significant activities in space.

Competition for Frequency Spectrum.

We appreciate that the Authorization Committees recognized the importance of the electromagnetic spectrum to DoD. The FY00 Authorization Act helps ensure that National security will be considered a critical factor when spectrum reallocations are required. The protection of DoD spectrum is essential to achieve information superiority. Our success in the information-intense, future battlespace will be dependent on assured access to the electromagnetic spectrum. We understand that the electromagnetic spectrum has both private and commercial value. However, the resolution of who should use the spectrum and how the spectrum should be used is a difficult one. We find ourselves not only competing with commercial interests but also with international entities for spectrum. A number of foreign nations are even considering charging the Department for spectrum usage. We must continue to recognize the importance of the radio frequency spectrum to our National security.

INFORMATION ASSURANCE AND CRITICAL INFRASTRUCTURE PROTECTION.

Information Superiority is essential to the United States military achieving and maintaining a decisive military advantage over our adversaries. In addition, as a result of our revolution in Business Affairs, the Defense Department has come to rely on the ready availability of information to run much of the business of Defense. As a result, much of the emphasis over the last several years has been focused on information assurance (IA). As recent critical infrastructure events and analysis have demonstrated, it is prudent to increase the emphasis on the first IA pillar (availability) within our information infrastructure. It is not enough just to protect our essential information; we must also be able to assure the critical infrastructures upon which information use, transport, and availability depend. To effectively assure the availability of key DoD information infrastructures, we must understand their vulnerabilities as well as their interdependencies on other key infrastructures (e.g., telecommunication systems and networks, electrical power, HVAC, people, etc.) and then be

able to mitigate them. Critical Infrastructure Protection is about mission assurance -- ensuring that infrastructures, whether physical or cyber or DoD-owned or commercially-owned, are available when needed to execute mission essential functions. Significantly, success in protecting these infrastructures can only be achieved through a DoD-wide enterprise solution that is beyond the means of any single defense entity to implement. The Department of Defense has laid the groundwork and developed the strategy and means to implement critical infrastructure protection within the Department. My fiscal year 2001 legislative agenda lays out the specific assistance you can provide to assist us in making critical infrastructure protection a reality within the Department of Defense and lead the way for our nation in this critical arena.

The key elements of the Department of Defense's effort are to provide a comprehensive critical infrastructure analysis and assessment, infrastructure vulnerability remediation, and consequence management capability to realistically address the emerging horizontal challenges of the 21st century. Specifically, we must:

a) Develop a comprehensive critical infrastructure analysis and assessment capability across the DoD enterprise, including the Unified Commanders-in-Chiefs, the Defense Infrastructure Sectors and the Services. We must be able to determine our most critical infrastructures and assets, identify their associated vulnerabilities and recognize and document interdependencies across several infrastructures. This analysis is essential to both warfighter and warfighter support/business operations, mission accomplishment, and lays the groundwork to accomplish integrated vulnerability assessments, perform mitigation of critical infrastructure vulnerabilities and manage the consequences of the loss of a critical infrastructure.

b) Conduct DoD Integrated Vulnerability Assessments at major domestic and overseas regional operating areas critical to the performance of DoD missions and remediate the most significant of the identified vulnerabilities. Regional assessments in support of installations, bases, and other critical infrastructure owners are essential in order to understand both physical and cyber vulnerabilities to those DoD and commercial infrastructures that are critical to military mission success. Initially focusing on identifying single and double asset vulnerability sets resulting in mission failure, the Department will then work with the asset owners -- whether military, government or commercial -- to develop effective vulnerability mitigation efforts,

focused on infrastructure protection investment strategies, operational protection enhancements and contingency plans. In a world where configuration management is essential to successful information assurance, these independent, on-site regional and local assessments are invaluable in verifying the defense posture necessary to maintain true information assurance.

c) Develop consequence management capabilities to address failures of critical infrastructures and assets and support dynamic mitigation of their impacts in support of Information Superiority and warfighter mission accomplishment. Consequence management capabilities within the CINCs, Defense Infrastructure Sectors, and Services are essential to supporting an effective DoD-wide management capability. Our Y2K experience provided us with direct and compelling evidence of the necessity to organize to deal with our increasingly interconnected and interdependent national and global critical infrastructures from an enterprise or horizontal perspective. Attempting to protect our critical infrastructures using our existing, narrowly focused organizational efforts will ensure that critical infrastructures will not be available to support our warfighters in an adversarial confrontation. Therefore, to effectively mitigate critical infrastructure failures, it is necessary to provide full spectrum consequence management across both the physical & cyber and government & commercial infrastructures.

In addition, the Department and our nation must remain at the cutting edge of assuring mission essential infrastructure availability to our warfighters. We must therefore, develop risk management and infrastructure process and technology improvements as well as develop the essential analytical methodologies for a true indication and warning capability against adversarial infrastructure attacks. RDT&E investments are essential not only to develop vulnerability mitigation technologies for our information infrastructures in the information assurance realm, but also in supporting infrastructures (e.g., telecommunications, electrical power, etc.), particularly those that rely upon computer control systems. Likewise, tool development to understand infrastructure interdependencies and integrate them into our analysis and assessment methodologies is essential.

These critical infrastructure protection investments will directly contribute to DoD mission success in three ways:

- Maximizing warfighter capabilities and effectiveness by minimizing the impact of infrastructure failures on defense capabilities;
- Shrinking the asymmetric advantage derived from the use of non-conventional or terrorist strategies; and
- Aligning the Department's infrastructure-related expenditures to maximize critical infrastructure availability essential to warfighter mission accomplishment.

This holistic, soup-to-nuts, approach will ensure the availability of those critical infrastructures that are essential to ensuring information superiority, as well as sustaining essential DoD and National operations and functions.

Protecting Our Information and Information Processes

The challenge for DoD is the same as that facing all Federal agencies. What sets DoD apart from other agencies is its size, complexity, and the criticality of its mission to the Nation. The Department of Defense is the largest organization in the nation. It has over 3 million people—active, Guard, Reserve, and civilian employees—spread all over the world at 637 military installations and many other locations. To administer to this community it takes roughly 10,000 separate computer systems involving 1.5 million individual computers. Of these, over 2,000 systems are mission-critical systems that must work for DoD to successfully execute its myriad missions. Nearly one half of all mission-critical computer systems in the Federal government are in the Department of Defense.

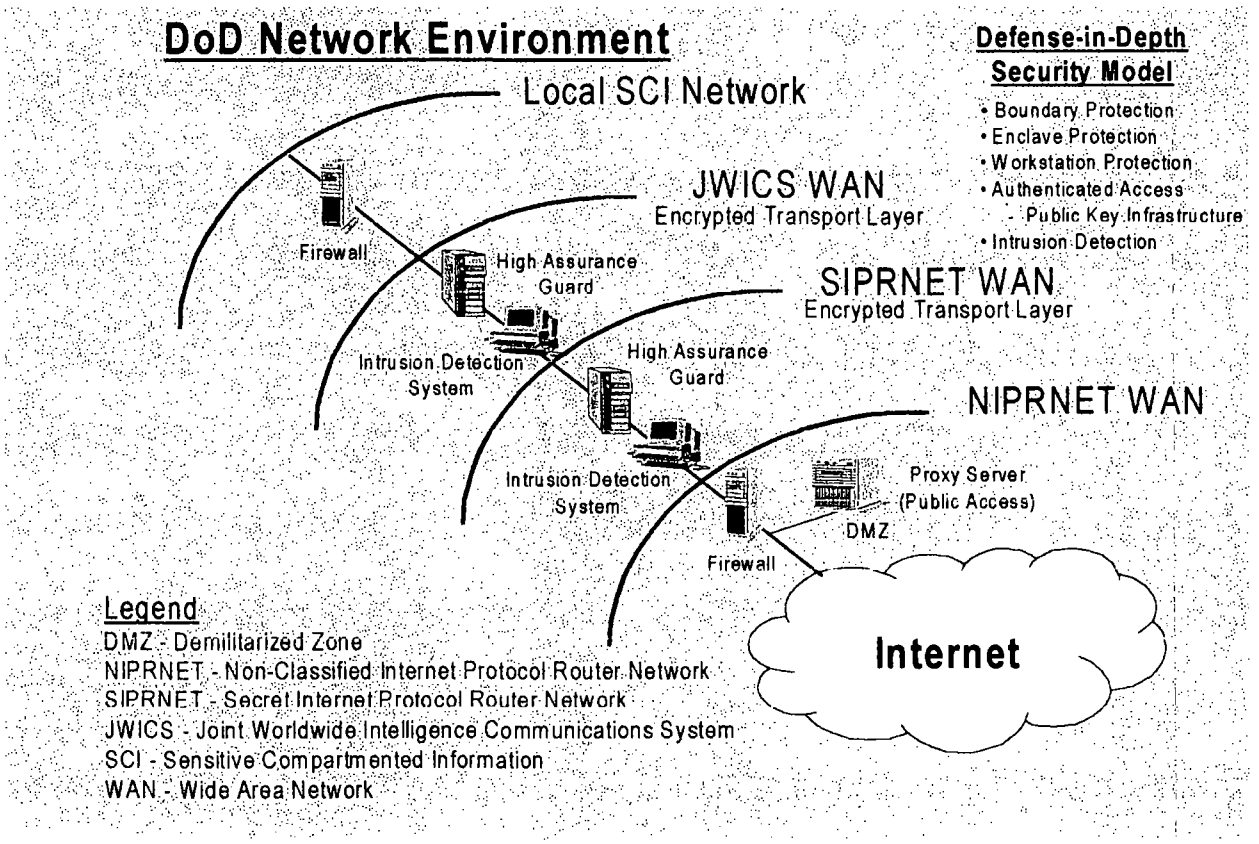
Information Assurance

The past year has been one of significantly increased activity in the Information Assurance arena. Investments and programs begun in previous years were beginning to bear fruit and progress is being made in addressing the complex issues. Also, Information Assurance awareness at all levels and in all DoD activities has risen.

The DoD treated the Year 2000 problem as if it were a cyber attack directed at the very core of its military capability—at the ability to obtain, process and control information that enables American forces to dominate the battlefield. Securing systems for the Year 2000 provided numerous lessons that will translate well to efforts in securing the critical information

infrastructure in the years ahead. Assessment efforts for Y2K led to the best ever inventory and accounting of DoD systems and their status. The information management structure now in place meets the requirements of the Clinger-Cohen Act. There is more senior level awareness and appreciation for information technology than ever before, to include an acute awareness that the government needs to keep pace with industry. The enormous effort and awareness of IT generated by the Year 2000 problem resulted in significant progress across the board in information superiority.

Given the risks and the fact that weakness in any portion of the Defense Information Infrastructure (DII) is a threat to the operational readiness of all Components, the Department is moving aggressively to ensure the continuous availability, integrity, authentication, confidentiality, and non-repudiation of its information and the protection of its information infrastructure. Achievement of Information Superiority in the highly compatible, interconnected, interdependent, shared-risk DoD environment requires that Information Assurance (IA) capabilities be based on consistent risk management decisions and a coherent strategy. The technical strategy that underlies DoD IA is Defense-in-Depth, in which layers of defense are used to achieve balanced overall IA.



The strategy recognizes that no single element or component of security can provide adequate assurance. This concept invokes the use of layered security solutions which allow us to maximize the use of commercial off the shelf (COTS) technology. The fundamental principal is that layers of protection are needed to establish an adequate security posture. For example, enclaves require a strong perimeter to guard against malicious outsiders. Within the protected enclave, protection is needed against malicious insiders and as well as malicious outsiders who have penetrated the protected enclave perimeter. This concept is relevant, whether it is used to protect against potential adversaries gaining access over the Internet or enforcing community-of-interest or need-to-know isolation within an otherwise protected intranet.

In May 1999, the Deputy Secretary of Defense issued the Defense-wide public key infrastructure (PKI) policy. This policy requires the use of a common, integrated DoD PKI to enable security services at multiple levels of assurance, providing a solid foundation for IA capabilities across the Department, and mandates an aggressive approach in acquiring and using a PKI that meets DoD requirements for all information assurance services. The DoD-wide

infrastructure will provide general purpose PKI services, e.g., issue certificates supporting digital signature and encryption, provide directory services, enable the revocation of network privileges, etc., to a broad range of applications, at the levels of assurance consistent with operational mission imperatives.

In the area of Intrusion Detection, we are greatly accelerating the development of technologies to detect and respond to cyber attacks against critical infrastructures. Current intrusion detection techniques are extremely limited in their ability to identify attacks, particularly large scale attacks against multiple points in the infrastructure, such as the recent Distributed Denial Of Service (DDOS) attacks against internet service providers and e-commerce companies. We have been conducting research into a broad variety of concepts which offer the potential to identify the most sophisticated kinds of cyber attacks, analyze the attack method and source(s), and institute protective measures in near real-time. This year we will characterize this technology and test its effectiveness in a genuine operational environment.

Wireless technology is also rapidly changing, and the Department is attempting to take advantages of 'windows of opportunity; in the wireless development cycle. Our Secure Wireless Communications initiative will provide the capability for joint forces to use whatever wireless services are available in a given region of the world. Investments by DoD today in these emerging wireless services will allow security capabilities to be built in (and reserved for future use) rather than trying to retrofit security into completed designs at substantially greater cost.

A corps of appropriately trained and experienced IT professionals is the most critical component in protecting the Department's information resources against modern day cyber attacks. Individuals using, administering, and maintaining these systems must follow proscribed protective procedures, and know how to operate the equipment designed to mitigate these threats. Although training for all employees using DoD computer systems is already mandated by statute and Department regulation, many lack a sufficient level of technical and procedural knowledge to fully protect the DoD's information resources. This problem is not unique to the Department of Defense, but certainly presents a challenge to an organization with our size, complexity, and deployment across the world.

Information Assurance and Computer Network Defense are fundamental design elements of the Global Information Grid (GIG), and thus will provide DoD a much more robust and defensible infostructure for the future. In essence, the GIG 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. Improved and timely GIG policies are the cornerstone to enabling change, eliminating outdated ways of doing business, implementing the spirit and intent of the Clinger-Cohen Act and other reform legislation, and achieving our Information Superiority goals.

Summary

The denial of service attacks witnessed in the past few weeks only prove why information assurance is so important to the processes required for businesses to operate in today's information environment. And while the DoD was not the subject of this particular attack, we are probed on a daily basis by those who are trying, or planning, to disrupt our nation's military capabilities. Constant vigilance over our networks is required, and that includes skilled people and technology working together, if we are to defend the infrastructures that allow our information processes to work effectively.

Substantial progress has been made, but we must always think of it as a journey, not a destination. As new technology is created, new attacks will be developed, and new countermeasures must be adopted. There is a lot more that has to be done in virtually every area that I've mentioned today. But only by recognizing this challenge, and facing it head on, can we realize the military potential afforded by achieving Information Superiority. I look forward to working with Congress to make Information Superiority happen.

OLA Draft 1 March 00

Brigadier General Robert M. Shea, USMC
Assistant Chief of Staff for Command, Control , Communications, Computers and Intelligence
United States Marine Corps

DRAFT TESTIMONY

INTRODUCTION

Mr. Chairman and distinguished members of the committee, I am pleased to have this opportunity to discuss how the Corps is meeting the challenge of its role in information dominance and particularly the critical challenge of Information Assurance.

Today I plan to provide you an overview of the Marine Corps approach to Information Superiority. To achieve this goal, we must ensure that our approach to information technology (IT) and command and control supports our warfighting doctrine, that we focus on interoperability, that our processes provide the infrastructure to meet information needs, that we are protecting our information resources, and that we are actively addressing every challenge.

OPERATIONAL MANEUVER FROM THE SEA OVERVIEW

I'll begin with an overview of the conceptual warfighting framework within which we expect to operate in the future. Today we have Marine Expeditionary Units (MEUs) deployed around the world. At any time they may deploy ashore to execute any one of the many capabilities for which they are specially trained. Success of those missions depends on our ability to provide the right information to the right place at the right time -- in a format they can use and understand.

If the situation warrants, the MEU becomes the base on which we build a larger operating force -- a Marine Expeditionary Brigade (MEB) or Marine Expeditionary Force (MEF) -- to conduct a classic amphibious operation with the Navy or to conduct sustained operations ashore alongside the Army. In any case, increased command and control (C2) capability is required to ensure operational success.

That is how we operate today and for the near future. But as I say these words, we are in the process of revamping our doctrine to embrace and support the concept of operational maneuver from the sea. Continued support to current operations while adapting for the future requires a holistic approach to information and command and control systems, as expressed to the committee last year by Lieutenant General Rhodes, the Commanding General of the Marine Corps Combat Development Command.

Operational Maneuver From the Sea, commonly referred to as *OMFTS*, is the Marine Corps capstone warfighting concept that, when coupled with its supporting concepts, serves as the basis for framing the capabilities the Marine Corps of the 21st century will need to achieve victory on the modern battlefield.

OMFTS envisions a future environment characterized by "crisis in the littorals." It describes a new form of littoral power projection in which the amphibious force focuses solely on the operational objective rather than building a large command and control capability ashore. It makes extensive use of maneuver at sea as a means of gaining an advantage to deliver a decisive blow at a significant enemy weakness. *OMFTS* offers the promise of extraordinary leaps in operational flexibility as the result of technological enhancements in such areas as sea based logistics, fires, and command and control systems.

When combined with a command and control system that is oriented toward rapid decision-making at all levels of command, the additional speed and flexibility offered by these new techniques produces a high tempo combat operation. This tempo will lend itself to favorable conditions for decisive victory.

With *OMFTS*, our inextricable link to the Navy grows tighter as we develop our emerging concepts of command and control afloat. In the past, we have always exercised initial command and control of amphibious operations from Landing Force Operations Centers aboard ship. Our concept called for movement of our command posts ashore as soon as we installed adequate infrastructure and were able to control combat operations.

As we look to our emerging concept of *Operational Maneuver from the Sea* and improvements in technology that are now available, we intend to exploit the advantages of keeping many elements of command and control afloat. We have always concerned ourselves with operational momentum and force protection. With *OMFTS*, supported by the technology available now or soon arriving, we can eliminate the disruption that previously occurred during the ship-to-shore movement of our various C2 functions. Our C2 nodes are afforded enhanced force protection through the ability to stay at sea, and the logistics requirement ashore is reduced.

It is the alignment of concepts and technology that allows this to happen. We could not exercise this concept with yesterday's C2 systems. Their limited range and capability required the commander and a large staff to move off the ship to position themselves where they could control the battle. The means are now available to operate a large portion of our command and control, particularly staff functions, while afloat. As the Navy implements the Information Technology for the 21st Century (IT-21) concept, it is now able to support Naval operations with systems that better support our concepts through direct connections to forces ashore.

Information Technology for the 21st Century (IT-21)

The Navy and Marine Corps are making great strides in developing and streamlining the process for identifying and procuring shipboard C2 systems. Many of these efforts fall under the umbrella of the Navy's IT-21 initiative. We have made progress in ensuring IT-21 includes the systems of Marine Corps interest, as well as ensuring that we work towards common solutions, standards and systems that support the full range of Naval operations. Integration between Marine and Navy IT-21 configurations continues to improve. While there are pieces of this integration that require work, the progress to date has been very supportive of our deploying Marines.

Marines currently deploying are seeing increased bandwidth for both ship-to-ship and ship-to-shore communications supported by a much more robust shipboard local area network. We have passed the stage where it was sufficient to have a robust C2 system on one ship of the Amphibious Ready Group (ARG) and archaic manual systems on all the other ships. Forces

dispersed across all the ships are able to share information and collaborate in operational planning with greatly reduced decision cycle times. Marine Expeditionary Units operating in places as diverse as Kosovo or East Timor are seeing dramatic improvements in their ability to conduct collaborative planning while in the split-ARG operations that are now common. We will build on that success.

We have a close relationship with the Navy and continue to work together in tackling the command and control systems challenges of forces afloat. IT-21 has been a major step forward for those Marine forces that have had the advantage of operating from the IT-21 configured ships. Embarked Marines have access to voice, video and classified high-speed data networks, as well access to the Internet. Additionally, large bandwidth, line of sight radios for voice and data are being installed under IT-21, along with tactical and long haul satellite access to the Defense Information Systems Network (DISN). Continued progress in this area is crucial to our success in an amphibious environment and will become even more critical as the *OMFTS* force evolves.

Marine Corps War Fighting Lab/Extended Littoral Battle Field Technology Demonstration

We are evolving our C2 capabilities through experimentation. The experiments conducted by the Marine Corps Warfighting Lab have been instrumental in highlighting deficiencies in our command and control systems, as well as steering us to technologies to solve these challenges. Our experimentation has highlighted the need for a radio for our small unit leaders to exercise command and control of their forces in an urban environment. We do not have this type of radio in our inventory in sufficient quantities today, despite the obvious need. The Lab has pointed us to a low-cost intra-squad radio solution that has received high praise from our Marines.

The Warfighting Lab continues with a series of battle experiments to determine solutions that will work in various operational environments. In the command and control area, they are determining the information needs of small unit leaders and ways to deliver a scalable Common Tactical Picture (CTP). The lab is also looking for technological solutions to support the over the horizon command and control requirements of *OMFTS*.

The ability to command and control forces when operating over the horizon has been always been a significant challenge for amphibious forces. Through the combined efforts of the Office of Naval Research and the Warfighting Lab, a program called Extending the Littoral Battlespace has successfully demonstrated the employment of airborne hosted wireless wideband technologies from ships off the coast of southern California to the desert in the vicinity of Yuma, Arizona. This experimentation allowed the small unit leaders in the desert to share a common understanding of the tactical environment with other members of the network. This type of capability is essential for us to achieve the full potential of the *OMFTS* force.

INTEROPERABILITY

We define our future warfighting environment to include Joint and Coalition operations. When discussing Naval, Joint or coalition operations, the topic quickly moves to interoperability. The Marine Corps is the model for interoperability. Despite being the smallest of services, the Marine Corps is a combined arms force. We train and fly in combat with the Air Force and the Navy. Ashore, we fight shoulder to shoulder with the Army, and we move forward from the sea with our Navy partners. We are always in a Joint warfighting environment. As you may have heard the Commandant testify, the Marine Corps provides 20 percent of the nation's active infantry battalions, 20 percent of the active fighter/attack squadrons, 17 percent of the attack helicopters, and one third of all ground combat service support in the active forces. Interoperability with our sister services and coalition partners receives the highest priority within the Marine Corps, and we often serve as an honest broker on interoperability issues.

We are primarily a "buyer" -- not a developer -- of systems, including information and command and control systems. Our Year 2000 (Y2K) operational evaluations illustrate this; 52 percent of our systems are developed by the other services.

We can't afford to develop -- nor do we intend to buy -- systems that don't fit into the established Joint architectures. Therefore, we zealously press for Joint solutions to our command and control systems and information systems requirements. To that end, we have recently established a Systems Engineering and Integration (SE&I) Division within the Marine Corps Systems

Command to ensure that our command and control systems acquisitions and developments do in fact comply with the DoD-designated Joint Technical Architecture and are interoperable. The function of the SE&I activity is to establish and enforce an overarching plan to ensure that Marine Corps C4I systems work as a C4I 'system of systems' in the Joint and Allied arena. The SE&I Division centrally identifies, manages, and enforces interoperability standards and integration engineering processes.

Complementing that effort is another Marine Corps Systems Command initiative, the Systems Integration Environment (SIE) at the Marine Corps Tactical System Support Activity. Our developers will use this integration environment to test systems and network configurations, ensuring that our tactical command and control systems perform as advertised, before fielding. The SIE also supports rapid acquisition initiatives since systems and configurations can be tested, adjusted, and retested in a realistic operational environment.

RECENT TACTICAL IMPROVEMENTS

We have made major strides in recent years in upgrading the Corps command and control systems posture, and we thank the Congress for its support in this improvement. Our FY01 budget submission continues our emphasis on upgrading tactical systems.

We have purchased satellite terminals that operate across a broad range of the frequency spectrum to exploit both commercial and exclusive DoD satellite systems. MILSTAR terminals like the SMART-T permit us to operate our critical Marine Air Ground Task Force (MAGTF) command and control systems in a stressed environment. The wideband STAR-T terminals, slated for acquisition starting in FY02, will provide us the flexibility to use both the Defense Satellite Communications System (DSCS), as well as commercial satellites for our long haul and reachback command and control systems requirements. In the meantime, we are working to extend the service life of our current Ground Mobile Forces wideband terminals.

With the fielding of the Tactical Data Network (TDN) and Digital Technical Control (DTC) facility in the FY01/02 timeframe, we will have a solid digital backbone down to the regiment.

Additionally, we procured the enhanced manpack UHF satellite terminals for our lighter, highly mobile Marines. The combination of these acquisitions not only enhances our ability to command and control Marine forces, but it is fundamental to our participation in Joint operations.

The major Information Superiority challenge for the MAGTF lies below the regiment level. We are fielding the Enhanced Position Location and Reporting System (EPLRS) to fill the gap down to the company level until a more robust and capable solution is developed.

Our FY01 Budget requests funding to proceed with the development of a standard Unit Operations Center (UOC) for our warfighting forces. This UOC program will incorporate elements of our present Common Air Command and Control Systems (CAC2S). It will focus on providing our commanders with a relevant Common Operational Picture (COP) that combines, among other things, ground tracks, sensor data, and air command and control information. UOCs will be scalable, using modular technology. Our UOCs will allow commanders of any combat, combat support, and combat service support unit to make faster and better decisions through enhanced situational awareness and state of the art collaborative planning tools.

We heartily endorse the development of the Joint Tactical Radio System (JTRS) and are optimistic that it will provide the solution to our networked voice, data and video requirements below the Division, Wing and Group level. When the JTRS is successfully fielded, it will allow us to "neck down" to a single family of combat net radios capable of meeting the requirements of the multiple families of radios that we currently employ. We expect the JTRS to offer increased operational flexibility, efficiencies in training, and reduced logistics support burden for our operating forces.

An emerging requirement for FY01 is our need for a ruggedized hand-held radio, such as the Multiband Intersquad Tactical Radio (MBITR), currently used by Special Forces in SOCOM. This radio satisfies our Tactical Hand Held Radio (THHR) Mission Needs Statement.

SUPPORTING ESTABLISHMENT INFRASTRUCTURE

Over the past several years, the Corps has invested significant time and money in improving its base infrastructure to ensure it provides a seamless connection between our supporting establishment and operating forces.

The upgrade of the telecommunications infrastructure for our supporting establishment, the fifth element of the MAGTF, remains one of our most pressing priorities. In the networked world we have entered, our bases, posts and stations are both literal and virtual extensions of our operating forces, so we are eliminating the boundaries between our tactical and base systems. We recognize that they are both inextricably linked to our current operations, as well as *OMFTS*.

Our Base Telecommunications and Infrastructure Upgrade Plan has been the bedrock of our garrison network, allowing us to procure and install a variety of network components and applications resulting in the implementation of a centrally managed and defended enterprise network -- the Marine Corps Enterprise Network (MCEN). It has also allowed us to expand connectivity to critical command and control facilities.

With your funding increase last year, we are continuing this expansion. We are reaping significant dividends upgrading the cabling systems and structured wiring at 21 of our 32 bases. This capability increases the bandwidth available at the desktop, improving data flow for graphics, imagery, and video -- a capability that will support reach back for our deployed forces.

There is no doubt when we finish upgrading the supporting establishment telecommunications infrastructure, we will have developed a true force multiplier through our ability to move information rapidly and seamlessly. Examples of this abound. Imagine the ability of a deployed commander to reach back to one of our bases for the functions that can be adequately performed there, thus reducing the lift requirements for his command and/or adding an additional capability of his choosing. For example, a forward deployed Marine Expeditionary Unit, our smallest MAGTF, might be in need of special maintenance support and conduct a video teleconference (VTC) with a subject matter expert at our logistics depot in Albany, Georgia in much the same

manner that Telemedicine is performed. Or, a Marine Expeditionary Brigade commander could reach back to Quantico to model and simulate his operation plan before going into combat.

The potential advantages are boundless, and there is no technical reason to preclude exploiting this capability. When completed, these upgrades will permit us to enhance and exploit our integrated logistics capability (ILC) and provide for adoption of E-commerce and Corps-wide process improvements. These telecommunications upgrades will also allow us to leverage advances in distance learning.

We appreciate your past support, and we seek your continued interest and assistance to complete this initiative at our bases while we continue to strengthen and refresh our network resources to meet the needs of the Corps.

INFORMATION ASSURANCE

The recent, well-publicized distributed denial of service attacks on Yahoo and other commercial websites highlight the inherent vulnerabilities associated with our rapidly evolving network-centric world. They also serve to remind us that we must continue our aggressive efforts to secure our networks and information stores. If these events are any indication of the maturity of coordinated cyber-assaults, then we should feel lucky it was undertaken in the commercial sector. Although we have made substantial progress in this area, our present ability to counter such a threat is minimal. The picture grows even more sobering if we accept that this attack was not the deliberate, malicious work of a Nation-State, but rather the effort of a loosely coupled coalition of hacker groups.

Although the Marine Corps denied these hackers the ability to use Marine Corps sites as jumping off-points, neither we -- nor any other service -- would have been immune to the flood of traffic that choked some of the world's largest, best-constructed web-sites, had the attack been directed at us.

Further, we have learned a great deal from this event. This was a single thread assault: one adversary, or group of adversaries, employing a single attack methodology. A multi-thread

attack -- one that combines, for example, a distributed denial of service attack, the broadcast of a Melissa virus containing a destructive payload, and the synchronized implanting of Trojan Horse 'sniffers' -- has not been conducted to our knowledge. As a result, we have not been forced to test our ability to respond to a coordinated, well-orchestrated attack of this nature.

When a multi-thread attack occurs, our Information Assurance posture must allow us to control the tempo of the cyber-battlefield. To do this, we must have invested sufficiently to ensure our defensive positions are reinforced and all avenues of approach are covered. Our ability to detect intrusions must be multifaceted. Whether it be a frontal assault, such as that experienced by commercial sites, a slow probing of our boundary layer security architecture, or an internal threat to our information integrity, we can not lose the situational awareness provided by a robust intrusion detection architecture. With this capability in place, we can conduct an active defense of our networks and react decisively, effectively, and rapidly to possible intrusions. Only through a combination of these can we hope to stay one step ahead of our adversaries.

Implicit in the previous discussions is the lack of boundaries in this new realm of electronic warfare. We know 'thin red lines' do not exist, and the enemy does not have a most likely avenue of approach. Our adversaries are not constrained by traditional boundaries, so they are able to treat the world as a cyber free-fire zone.

We believe that a robust Information Assurance architecture is built upon seven (7) critical elements. These include:

- A robust network infrastructure;
- Enterprise Information Technology Standards;
- Enterprise Information Technology Policy;
- Centralized control of Information Technology resource acquisition;
- System Administrator training and user education;
- Centralized enterprise network management and configuration control; and,
- Enterprise Defense-in-Depth Strategy.

I'll address each of these elements briefly.

Network Infrastructure. At the core of our Information Assurance architecture is a robust network infrastructure. As noted before, we have been pressing forward aggressively to modernize our bases, posts, and stations. More needs to be done and once again, we seek your support to continue our modernization investment.

Technology Standards. Key to implementing and sustaining a robust Information Assurance architecture is the adherence to enterprise information technology standards. The Corps has a single entity, the Marine Corps Combat Development Command that develops and promulgates internal, as well as external, IT standards. This includes those standards associated with OSD's Global Information Grid (GIG) and the Department of the Navy's Chief Information Officer's (DON CIO) Information Technology Standards Guideline (ITSG) initiatives. These standards govern the hardware and software fielded to our warfighters and supporting establishment. Moreover, these standards cover the spectrum of functionality, from the desktop to the DISN service delivery node.

Policy. Service-level responsibility for developing and promulgating IT policy is central to the establishment of processes necessary to effect Information Assurance on an enterprise scale. The Corps has assigned this authority and responsibility to the Assistant Chief of Staff for Command, Control, Communications, Computers and Intelligence (C4I). Because the Assistant Chief of Staff for C4I both develops policy and has operational control of the MCEN, he has the direct authority to enforce all Information Assurance policies. This tight coupling ensures the focus on information that is essential to ensuring a secure network.

Centralized Acquisition. Leveraging the foundation provided by centralized standards and policy development processes, the Marine Corps has centralized its acquisition of all IT resources in a single entity. Routers, servers, switches, and other network-specific resources have been procured centrally since 1992. At the beginning of this fiscal year, the Marine Corps Systems Command extended this centralization and began procurement of all end-user workstations, software and peripheral devices. By controlling the process that acquires end-user

components, we have taken a major step towards strengthening the end-to-end configuration control of our network -- a mandatory function if an enterprise Information Assurance architecture is to be implemented successfully.

Training and Education. Education and training ensure that policies and practices are understood and exercised. User education is vital to the protection of our networks and mission critical information. Although our focus has been on protecting the transport mechanism, it is just as important to protect the information that traverses these networks. This protection starts at the user level. Regardless of the technology employed, without an educated, disciplined, engaged user community, the security of our networks and information will always be suspect. In response to this challenge, we have instituted a Corps-wide program where all Marines receive annual training designed to raise their level of awareness and emphasize the critical role they play in this network-centric world. In the future, we see the user's role becoming ever more important as new technologies, such as Public Key Infrastructure (PKI) / Smart Card, are deployed throughout DoD. If we fail to leverage our personnel resources at this critical juncture in the development of network functionality, it can only increase the Information Assurance challenges we are certain to face in the future.

Training our information system professionals is critical, too, if we hope to implement a viable Information Assurance architecture in both deployed and garrison environments. Specifically, the Marine Corps is establishing a new MOS within our enlisted ranks that focuses on information security. Marines with this Military Occupational Specialty (MOS) will be specifically trained in security policies, plans and procedures, network security measures, network certification, and information system security analysis.

Additionally, mobile training teams, provided by our Network Operations Center (NOC), are immediately dispatched when a new security technology is fielded before the establishment of a formal training pipeline. Providing 'just-in-time' training in this fashion not only meets our warfighters' operational requirement for security technology and provides a Marine capable of sustaining that technology, it also eliminates the time technicians have to be away from their

units at a formal school, thus reducing training and travel costs. This responds to the dynamics of our changing technology environment.

Enterprise Network Management. The Marine Corps exercises centralized operational, technical and configuration control of the 32 bases, posts, and stations that make up the MCEN. As previously stated, the Marine Corps Network Operations Center manages the enterprise network under the direction of the Assistant Chief of Staff for C4I. To ensure consistency across the Marine Corps network, the Center uses the same set of standard DoD-compliant software tools for our supporting establishment networks as those employed by our Marines in the field.

Centralized configuration control is reflected in our implementation of a contiguous enterprise IP addressing scheme, a standard network operating system, a single electronic messaging system, a single global directory that is capable of reflecting changes world-wide instantaneously, and a common router operating system. We are currently implementing an enterprise resource inventory, configuration management and software distribution system. When completed, the Marine Corps will have 100% visibility of IT resources connected to the enterprise network. Our focus on the warfighter and commitment to interoperability is further reflected in our acquisition of long haul service solely from the Defense Information Systems Agency (DISA). This approach to effecting command and control of our networks allowed us to transition 68,000 seats to a new network operating system and electronic messaging system in less than 14 months.

This network management architecture is the foundation for our enterprise Information Assurance architecture.

Defense in Depth. We have based our Information Assurance architecture on the 'Defense in Depth' strategy. This strategy calls for the implementation of 'layers' of protection.

At the boundary layer, where the MCEN joins the DISN, we are fully covered with firewalls and screening routers. At each of our bases, posts and stations, we have implemented, and centrally manage, screening routers, firewalls, intrusion detection devices, and virtual private network devices. Our firewalls and screening routers are the 'locked front door' --keeping out unwanted

visitors. Our intrusion detection devices let us know when someone is trying to break-in – feeding information back to our central enterprise NOC where immediate action can be taken and correlation analysis conducted. Of note is that each Marine Forces (MARFOR) command element is given a 'feed' of intrusion detection data to provide them situational awareness of the enterprise network that falls within their Area of Responsibility (AOR). Our most recent initiative, installation of Virtual Private Network (VPN) devices, has created a Marine Corps Intranet that allows non-secure and legacy applications to communicate without jeopardizing the security of the enterprise network.

We have duplicated this boundary layer security functionality, and along with the network management capability previously addressed, packaged it in "fly-away, " or deployable transit cases, for our Marine Expeditionary Forces (MEFs). The Deployed Security Interdiction Device (DSID) is currently being fielded, with Full Operational Capability (FOC) targeted for June, 2000.

Three additional layers of defense are encountered as we move deeper into the base, post, or station. One of these layers calls for implementing security devices that support segregating an organization from other entities on the same network, based on mission requirements.

The layer below this supports isolation of user groups within an organization -- again, based on mission requirements. We feel the jury is still out when it comes to answering the question, "How much security is enough?" We must never forget that the information needs of the warfighter remain preeminent. We must continuously review our choices when it comes to balancing security against service and performance. We can never inhibit the flow of information to the warfighters when they are in, or intend to go, in harms-way.

The final layer encountered focuses on the end-user. In this area, we have implemented virus-scanning software on all workstations and application servers. Additionally, we are pressing forward with pilot-site implementations of PKI at Marine Forces Pacific Headquarters and at the Marine Corps Systems Command.

Our Information Assurance architecture is not a static entity. It is a living, dynamic body that must have the flexibility to respond to a wide range of attack methodologies, the capacity to withstand a brute force attack, and the resilience to speed reconstitution. Through the unique combination of centralized network management and the array of security assets described above, we pursue active defense of the MCEN. The Marine Forces component to the Joint Task Force for Computer Network Defense (JTF-CND) is co-located with our Network Operations Center, and is charged with defending the enterprise network. This synergistic relationship provides the framework within which active computer network defense is integrated with network management. In many cases, delay is minimal to non-existent when responding to direction from the JTF-CND.

The Commander of the MARFOR-CND is the Assistant Chief of Staff for C4I. Combined with his operational control of the enterprise NOC, this gives him direct control of the two organizations responsible for defense of the network. As such, the Marine Corps is uniquely postured to respond decisively, effectively and in a timely manner to intrusions and network attacks.

We continue to add to the capabilities of the MARFOR-CND component. Staffed completely with Marines from our Reserve forces, we have established a Web Risk Assessment Cell. The mission of this cell is to test the vulnerability of our web-sites. Through 'virtual drilling,' these reserves check our web-sites for inappropriate content and assess them for vulnerabilities that might leave them open to compromise.

I am confident that FY01 budget will further strengthen our Information Assurance architecture. Significant among these are:

- Continued implementation of PKI;
- Stand-up and staffing of an alternate network operations center;
- Continued expansion of the SIPRNET down to the battalion/squadron;
- Acquiring more – and dynamically allocating -- bandwidth;

- Continued integration of Reserves into the NOC and MARFOR-CND;
- Instituting a quarterly vulnerability assessment program;
- Implementing host level intrusion detection; and
- Leveraging the security functionality of biometric technology.

However, our ability to resource all these initiatives is limited and not fully funded in the current budget. Your continued support of our infrastructure and modernization efforts will enhance our ability to exploit our information systems to their fullest, knowing that they will be available when needed and the information resources protected from inadvertent or malicious compromise.

Successful implementation of information dominance as envisioned in *Joint Vision 2010* is founded on the existence of secure, robust and seamless network connectivity. If we view the aggregation of our networks as a weapons delivery system, then effective, timely, and decisive command and control is the 'round' that must be fired if we are to succeed on a battlefield governed at the 'speed of thought.' Our Information Assurance efforts will ensure we can hit the target.

CHALLENGES AND THREATS TO INFORMATION SUPERIORITY

You have heard many of us speak to the changing military environment -- and nowhere is that more apparent than in the information technology arm of the military. We are faced with a number of challenges and threats. I would like to present some of the more pressing of these today.

Personnel -- The Key Resource

Our tactical, shore and Information Assurance interests are only successful if we have the right people -- an adequate number of trained, motivated Marines -- in place to operate and maintain our systems.

First and foremost, we must recruit and retain Marines with appropriate skills to install, operate and maintain the technology we are employing. As you are aware, our Marines with information technology skills are leaving the Corps at a much too rapid rate. This is true of both our officer and enlisted ranks. The Corps has always been a source of skilled personnel for the civilian work force. However, the boom in technology has increased the civilian sector demand for skilled IT men and women and has rapidly driven commercial salaries well beyond our competitive range. The shortage of skilled personnel in selected technical occupational fields leads to increased personnel tempo and the associated quality of life issues.

Dynamic Technology Environment

The rapid evolution and turnover of technology is another challenge we face. In the past we were able to field a C2 capability with the reasonable expectation that we would be using that solution for ten to fifteen years. The long life cycle of our systems enabled us to establish a systems configuration baseline, develop sound principles for policy and doctrine, and establish our recruiting and training pipelines. We no longer have that long life cycle.

Today, technology can change within a budget cycle. The correct technological solution for today's requirement may require a new approach 24 months from now. While we are actively implementing acquisition reform initiatives and streamlining our processes, adjusting to the need for such rapid procurement and fielding of systems is truly a challenge we all must face.

Spectrum Management

Spectrum management continues to be one of the most challenging and least understood issues with which we are confronted. The global economic benefits derived from the sale of the frequency spectrum are placing major restrictions on the use of what were heretofore exclusive military frequency bands.

These restrictions have significant readiness impacts. In some areas of the world, including the United States, we are not permitted to train on the equipment we will use in combat. In other cases, we cannot develop adequate solutions to our command and control requirements because

there is no clear set of internationally approved frequencies for a specific capability. Yet in other instances, the use of the frequency spectrum is uncontrolled and consequently we are confronted with serious radio frequency interference problems.

Warfighting versus Business

For years now we have loathed the "stovepiped" systems we developed. They were excessively costly, manpower-intensive and inefficient. We are rapidly moving away from this approach. While I certainly don't endorse going back to stovepipes, we need a thorough understanding of the consequences of going to a network-centric world where all our IT services and command and control systems, including secure voice, video and data, ride over a single path to the warfighter or the desktop. While this may be efficient from a business perspective, it doesn't necessarily make sense from a warfighting perspective. We must be careful not to confuse efficiency with effectiveness, nor can we afford the single points of failure inherent in many solutions.

A clear distinction needs to be made between business and warfighting. While some principles apply to both, they are totally different in critical areas. Warfighting is not clean and neat; one must only look at Grozny.

Underestimating the Threat

We must acknowledge that our potential foes are learned and thinking adversaries -- not some benign, static entity. In a warfighting context, for most of the leaps we have taken in command and control systems technology, there is a small, relatively inexpensive, yet effective countermeasure to that technology. Our potential adversaries recognize this -- it is the asymmetric threat with which we must be concerned.

For example, a multi-million dollar wireless network could be rendered irrelevant by the use of a very inexpensive, hard to detect expendable radio frequency jammer.

In my view, if we had been confronted with a significant ground electronic warfare threat during the Gulf War, we might be taking a different approach to command and control systems acquisition today. The disruptions of the electromagnetic spectrum and network attack are a major Information Superiority concern for Marines.

Computer network attack has the potential to be the poor regime's asymmetric counter for our Information Superiority thrust. It requires very little in the way of resources; can be launched from virtually anywhere in the world; and has the potential to mask the originator. It is recognized globally as a force multiplier. Over two years ago as the Director for Command, Control and Communications for the U.S. Pacific Command, I hosted a conference of several Pacific Rim nations to discuss areas of mutual interest.

The one topic that was on every nation's agenda was that of Information Operations. Even the least developed nations had interest in this item and were highly conversant on the topic. They had studied the topic extensively through the Internet, and while many nations didn't have the depth and breadth of computer expertise, they all had a cadre of experts. This area of warfare and study is quickly expanding and is receiving serious foreign military thought as evidenced by the article *Unrestricted Warfare* written by two People's Liberation Army (PLA) colonels in the People's Daily.

The article highlights how real Information Warfare is -- and how seriously many nations are taking it. The authors advocate planning for Internet insurgency, manipulating a stock market crash, a computer virus attack, destabilizing exchange rates, and spreading rumors on the Internet as part of unrestricted warfare.

SUMMARY – MEETING THE CHALLENGE

We have just successfully overcome perhaps the most significant challenge we have faced since the dawn of the information age. The Y2K Challenge taught us many lessons, as well as teaching us more about the systems that we use than we previously knew. How we develop and deploy systems and the extent of the commander's dependence on IT has never been as clearly

defined as it is today -- thanks to our Y2K experience. The fact that we transited the millennium rollover without a single operational impact attests to the degree that we learned our lesson and applied the proper tool -- to our benefit. Our challenge now is to focus this same attention to the issues I have just addressed to achieve our goals in attaining and sustaining Information Superiority to support *Operational Maneuver from the Sea.*

Your support has allowed us to provide a very effective command and control capability. I am convinced that today we have Information Superiority over any challenger and are focused on the Information Assurance elements that will maintain this lead. But with technology changing rapidly, we cannot become complacent. As technology changes, we must change as well.

Given the combination of dynamic changes in technology, the increased complexity of the systems we are fielding, and the loss of our technically skilled Marines, it is clear that we are facing a critical challenge.

We must address this challenge, and it is my belief that our Fiscal Year 2001 budget submission is on target. We can use your continued help with our investments in both tactical systems and base infrastructure. This will allow us to develop the capability needed to provide Information Superiority to America's "911 Force."

"Information Superiority and Information Assurance: Meeting the Challenges of the 21st Century"

Mr. Chairman, Members of the Committee.

I am grateful for the opportunity to again address the committee on the important topic of Information Superiority and its central role in the military transformation process, and to discuss the Joint Staff's campaign plan addressing this complex issue of great importance. I am Lieutenant General Jack Woodward, the Joint Staff Director for Command, Control, Communications, and Computer Systems. I am also the Joint Staff Coordinating Authority for Information Superiority as it relates to implementing and enabling Joint Vision 2010. My testimony will address Information Superiority, focusing on the delivery of assured, protected connectivity to increase combat power for today's warfighter. I will introduce you to an overarching concept referred to as the Global Information Grid (GIG). Finally, I will share with you some of the important progress we have made over the previous year, and I will identify many challenges we face in achieving Information Superiority.

At the dawn of the 21st century, the Joint community is fully engaged in exploiting the warfighting advantages of this high tech era. The Chairman of the Joint Chiefs of Staff published his overarching vision, *Joint Vision 2010* (*JV2010*), that describes warfare in the

information age. It articulates a vision for future warfare where information superiority is the *fundamental enabler* of the four pillar warfighting concepts: Precision Engagement, Dominant Maneuver, Focused Logistics, and Full-Dimensional Protection.. In simple terms, Information Superiority means getting the right information to the right people at the right time in the right format while denying an adversary the same capability. Let me start my discussion by creating a fictional scenario of an information-intensive battlefield and address the Information Superiority concepts it represents.

A Potential Future Scenario

On a potential future battlefield, a US Joint STARS aircraft detects a column of vehicles nearing a sector patrolled by a German reconnaissance company, one of our Coalition Partners, and injects the positional data of the column into the Common Operational Picture (COP). The Combined Joint Forces Air Component Commander (CJFACC) and the Combined Ground Component Commander (CGCC) and the Commander of the Joint Task Force (CJTF) all see this information simultaneously.

The CGCC, using the secret Coalition Wide Area Network (CWAN),

directs an orbiting, US-controlled Unmanned Aerial Vehicle (UAV) to reconnoiter the area and identify the vehicles as friend, foe or neutral. The resulting real time, satellite-relayed video stream is analyzed at Allied intelligence centers on different continents and the vehicles are identified as hostile. The centers quickly coordinate and build an analysis and targeting package with a common collaborative planning tool and forward this information to the Commander of the Joint Task Force (CJTF) and his coalition component commanders.

After studying the information, the CJFACC directs an air strike against the enemy vehicles. A rapid review of real-time status of aircraft in the area reveals the best course of action is to direct an orbiting 4-ship cell of Joint Strike Fighters to engage the target. In addition, a carrier-based EA-6B is directed to provide Electronic Warfare (EW) support. The pilots consult their onboard common tactical picture enroute to the target to verify the German team's position and receive the latest targeting information. Following the air attack by laser-guided precision weapons, satellite systems relay the real-time strike information from the UAV to the CJFACC, the CGCC, and CJTF commander. Immediately after the strike, the UAV collects and transmits battle damage assessment information to the analysts to determine if a re-attack is required.

As this scenario unfolds, operators and analysts are monitoring and assessing the military resources necessary to conduct the operations such as strike and support aircraft, fuel states, weapons loading, system status, and proximity of friendly forces and prohibited targets. The CJTF's C4 coordination center monitors bandwidth requirements to support real-time voice, data, and video streams necessary to coordinate this coalition operation. They are ensuring the networks are properly configured, enough bandwidth is allocated, and the C4 systems are immune to hostile cyber attacks. Operators are alert to jamming and are poised to respond as necessary to ensure uninterrupted radio spectrum availability.

The power of real-time, networked operations depicted here is the basis for the Commanders' ability to share a common operational picture, collaboratively plan strikes, retarget weapons platforms while in flight, and work with a multitude of coalition partners.

We accomplish much of this today, but it's HARD work. Challenges remain in the areas of security and interoperability of our joint and coalition C4 systems.

This scenario highlights the **potential** power of a network-centric force -- force with the capability to dynamically retarget on demand -- a force with the capability to dynamically network sensors, regardless of

platform; shooters, regardless of service or country; and decision makers, regardless of location. This is what the ongoing transformation of military capability is all about.

Increasingly, it is a secure, reliable network that makes an effective warfighting force. As a result, securing the network is not just about securing information. ***It is about enabling assured operations and mission success.***

We plan to achieve Information Superiority through an overarching concept called the Global Information Grid (GIG).

Realizing the Network - The Global Information Grid

The Global Information Grid is a unifying concept and one of the key enablers of Information Superiority. We think of the Global Information Grid in the same way that most people think of the "Internet," a single concept that describes something that is very complicated and constantly evolving. General Shelton, the Chairman of the Joint Chiefs of Staff, told Congress during his recent posture statement: *An important aspect of future operations will be the*

development of a Global Information Grid, or GIG, to provide the network-centric environment required to achieve information superiority. The GIG is the globally interconnected, end-to-end set of information capabilities, associated processes, and personnel to manage and provide information on demand to warfighters, policy makers, and supporting personnel. It will enhance combat power through greatly increased battlespace awareness, improved ability to employ weapons beyond line-of-sight, employment of massed effects instead of massed forces, and reduced decision cycles. It will contribute to the success of non-combat military operations as well."

Achieving the Global Information Grid

The overarching rationale for the Global Information Grid is supported by the ongoing shift to network-centric operations, the principle component of the Revolution in Military Affairs transformation. In the military context, weapon systems are essential for mission success. In times past with platform-centric operations, the link between sensors and shooters was tenuous and lacked the timeliness required. In today's network-centric operations, the timely exchange of information is key to leveraging all available sensors and weapons systems to

generate increased combat power. The secure, networking capabilities inherent in the Global Information Grid provide the fused, timely information essential for joint mission success. It enables commanders to create a dynamically integrated fighting force by linking sensors to shooters to generate massed effects. Because of this inextricable tie to combat power, the Global Information Grid must be treated like the weapon system it has become. Treating the Global Information Grid as a weapon system has several significant implications for its deployment and employment.

Operationalize the GIG: Our CINCs and warfighters must be confident they have the information superiority capabilities they need to fight and win. We must standardize our network operational concepts and doctrine. We must institutionalize our tactics, techniques and procedures (TT&P) and demand the requisite training of our network system administrators and the personnel who employ the GIG's global applications (e.g. Global Command and Control System). We must provide end-to-end visibility into the health and readiness of these critical components to decision makers as they make trade-off decisions to balance limited resources against operational demands.

Organize for Combat: We must organize units that operate, maintain, and protect our networks as an integral part of our warfighting

command structure, just as we do with all other warfighting resources. We need to consolidate responsibility and operational control under a single warfighting commander. This will place the authority for allocating essential, limited resources based on operational exigencies under a commander charged with the responsibility for the Global Information Grid.

Protect and Defend the GIG: Defending our military capabilities is second nature to us. Protecting and defending our networks and the information that is collected, processed, aggregated and stored over them should be as well. We are committed to protecting the network with the same vigor that we protect other important elements of our force structure, such as the deployed Carrier Battle Group or a bomber enroute to its target. All of these weapons systems use an analogous Defense-In-Depth strategy. This strategy employs techniques on the perimeter to detect intruders, capabilities to assess threats within our boundaries and technology to respond to attacks when necessary to restore the force structure.

Improve GIG Performance: As quickly as the technology evolves to allow us to prioritize and manage the flow of information over the network, we must adopt the means to optimize our systems. There must be enough capacity to support the way the warfighter wants to fight

now and in the future. A key lesson learned from *Operation Allied Force* is that today's battlefield is information intensive. Unmanned Aerial Vehicles (UAVs), Video Teleconferencing, and Imagery require lots of bandwidth. Precision guided munitions rely on global positioning data for accuracy. Dispersed units rely on secure voice and data for situational awareness and command and control. Our networks must be optimized to support all of these capabilities when needed. Another key lesson learned was that our ability to manage the radio spectrum and the limitations of current tactical ground terminals directly impact the end-to-end network performance. During *Operation Allied Force*, over 44,000 radio frequencies were deconflicted, permitting an uninterrupted flow of information.

Expand the GIG: The Multinational warfighting and peacekeeping environment in which the military operates today requires an ability to be able to "connect" with allied and coalition partners in order to operate effectively. The need for a Coalition-wide WAN (Wide Area Network) has been validated over and over again in recent operations involving our multi-national partners. Security technology, information releasability and other policy matters are key to making this a reality. We must continue developing technology to reduce the manual burden of information releasability and secure connectivity while also working the policy issues to ensure we can share information within an international

scenario. In addition, improved cryptographic capabilities supporting high speed, high bandwidth communications must be part of the gameplan.

Fund and Acquire GIG Capabilities: We have to compete and resource the Global Information Grid like any other weapon system. The Global Information Grid is a continually evolving system of systems that must be funded in a synchronized and coordinated manner. Training to operate and protect these complex systems must be an integral component of our fielding strategy for successful employment of forces. Research and development for advanced technologies to improve the communications and computing capability of the network must be a priority.

Value the GIG: In today's military, we value what we can depend on for mission success. The Global Information Grid is the linchpin in both our military operations and business processes. We must consider it an essential, precious resource in our arsenal of weapons. The Global Information Grid is the entry fee for the DoD transformation and the combat power associated with our Joint Vision and it must be valued as any other essential component. *Deploying the Global Information Grid is a Strategic, not a Tactical decision. It is not a C4 decision -- it is a decision about combat power.*

The Global Information Grid to Date

The Joint Community is making real and tangible progress towards treating the network like a weapon system and making the GIG a reality. Examples of this transformation are abundant.

United States Pacific Command (PACOM) is in the midst of operationalizing theater networks by establishing a Theater C4ISR Coordination Center (TCCC) and developing associated Techniques, Tactics, and Procedures (TT&P). The TCCC will provide USCINCPAC with unprecedented visibility into theater networks. The TCCC will provide a readiness assessment based on specific metrics enabling USCINCPAC to provide operational direction to Service components and other operators of networks, systems, and applications to optimize the Global Information Grid for current operations. The TCCC will provide health and status information concerning theater networks to the Global Network Operations and Security Center that monitors DoD's backbone communications networks.

The first step in acquiring and funding the components of the Global Information Grid occurs in the requirements generation process. Two separate but interrelated events are currently taking place which have significant impact on the evolution of the Global Information Grid.

U.S. Joint Forces Command is responsible for authoring a Capstone Requirements Document (CRD) describing the essential elements of the Global Information Grid. This is the first time a single, overarching capstone document will provide a definitive architectural framework describing the inter-relationships and components of the weapons systems, connectivity, computing capabilities, applications, basic foundation concepts, network operations and information management components that comprise the Global Information Grid. Rather than disparate, isolated networks, the CRD will call for interoperable, accessible, secure, reliable, inter-networked capabilities to enable effective global military operations.

In addition, the requirements generation system as a whole has been strengthened with the rewrite of the Joint Staff instruction that governs this process. It specifically requires C4 interoperability in future systems be demonstrated at key acquisition milestones. This will improve the link between systems acquisition and end-to-end interoperability in an operational context. The Joint Requirements Oversight Council (JROC) along with the Military Communications-Electronics Board (MCEB) and the new DoD Chief Information Officer (CIO) Executive Board will collaborate throughout the systems acquisition process to ensure capabilities are fielded that meet CINC, Service and Joint interoperability requirements.

End-to-end network performance is being enhanced through modeling and simulation. The Network Warfare Simulation (NETWARS) initiative provides the first modeling and simulation capability to assess the performance of the Global Information Grid. The Joint Staff-led NETWARS program was developed from a leading commercial network simulation tool, OPNET, resulting in a significant operational. NETWARS is being used today to model the effectiveness of operational plans using the Global Information Grid as it currently exists. Not only will we begin to assess the capability of our networks to support specific Joint operations during the planning stage, but NETWARS will help us understand where and how to employ advanced technologies to expand and improve the Global Information Grid. For example, NETWARS will help understand the extent to which a new capability, such as the Advanced Wideband Satellite System, will improve the performance of the Global Information Grid.

Network performance and radio frequency (RF) spectrum usage are inextricably linked. Over the past year, Congress has championed protection of the RF spectrum that is so critical to military operations. You have returned 8 Megahertz of previously reallocated spectrum for DoD use. Under your scrutiny the Federal Communications Commission (FCC) reassigned 50 Megahertz to preserve contiguous bandwidth required by the Navy's Cooperative Engagement Capability - a program

which provides networked sensor capability to shooters. These and similar initiatives saved hundreds of millions of dollars for the Department and had a direct impact on our ability to employ and protect our fighting forces. Thank you for your tenacity and objective assessment of our needs.

Protecting and defending the Global Information Grid is a fundamental, mainstream military imperative. Our strategy for information assurance is one which employs multiple layers that we call "defense in depth." This strategy establishes a set of minimum capabilities required for each of the four levels of Defense in Depth: the network, the enclave, the computing environment and the infrastructure. These capabilities include automated and verifiable access control of database and software applications as well as a department-wide policy for virtual private network configurations. They will enable the Department to keep pace with rapid technological advances while allowing for the integration of legacy equipment with existing capability. Procedural changes are underway as well to take advantage of the technology currently employed. We learned much from our experience with the most significant threat to the Global Information Grid that we have ever experienced – Y2K from both a technological as well as a procedural perspective. We now have the tightest configuration control of the networks and computer systems that we have ever had and we

intend to maintain this standard.

The Department is well on its way to organizing the Global Information Grid for combat operations. A significant development in FY99 was the assignment of the Computer Network Defense (CND) mission to USCINCSPACE through the Unified Command Plan (UCP) 99. This change gave a Commander in Chief (CINC) the responsibility and authority to protect and defend the Global Information Grid for assured operations and mission success. The action arm of USCINCSPACE is the Joint Task Force Computer Network Defense (JTF-CND) operating here in Washington DC and co-located with the Global Network Operations Systems Center (GNOSC) of the Defense Information Systems Agency. The GNOSC can display the operational picture of critical DoD networks worldwide. The co-location of these two operations results in tremendous synergy and synchronization. One of the success stories of placing the CND mission under a CINC was the operationalizing of readiness conditions as they apply to our worldwide networks. Global Information Conditions or INFOCONs, are set by USCINCSPACE based on the level of threat to the Global Information Grid. Each INFOCON level requires specific actions by personnel at every camp, post, base, station, and deployed unit. This standardizes protection of this resource; a resource that is only as strong as its weakest link.

Our ongoing Navigation Warfare (NAVWAR) initiative addresses potential vulnerabilities to the Global Positioning System (GPS). This initiative is a major step in assuring access to the Global Information Grid.

Improvements to the Global Information Grid come from technological as well as procedural advances. There has been much discussion about the challenges associated with exploiting rapidly emerging technology. Let me tell you about some of our successes using Advanced Concept Technology Demonstrations (ACTDs), Joint Warrior Interoperability Demonstrations (JWID), the Joint C4ISR Battle Center and evolutionary acquisition processes.

We currently have a Pilot Program in the Pacific that employs the information dissemination management capabilities developed in the Battlefield Awareness and Data Dissemination Advanced Concept Technology Demonstration (ACTD). This capability will allow Commanders to "pull" information from multiple sources on demand as well as allow information sources to "push" critical information to specific warfighters as required. The Information Assurance: Automated Intrusion Detection Environment (IA: AIDE) ACTD at U.S. Strategic Command promises to provide analysis and warning of information attack by integrating and displaying data from multiple intrusion

detection sensors. This capability will decrease time required to assess attacks on our networks and help discriminate serious threats from casual hacking attempts.

Joint Warrior Interoperability Demonstrations provide an opportunity for the evaluation of emerging technology within a warfighting scenario to solve interoperability problems. The last demonstration focused on coalition interoperability and resulted in establishing a coalition federated battlelab network that continues today. This network will allow further studies in the operation of a secure network with our coalition partners. Upon completion, warfighters identify the most promising, low cost technologies for immediate fielding. Examples of these "golden nuggets" include data compression, collaborative planning tools, and secure information exchange capabilities.

The Joint C4ISR Battle Center (JBC) is focussed on assessing new and emerging technologies to meet current and near-term CINC C4ISR requirements. They measure the efficiency, effectiveness, and technical feasibility of commercial products. For example, the Joint Battle Center evaluated and recommended Rosetta technology as a near-term solution to tactical data link interoperability problems. Once deployed, this technology will help us provide the warfighter with a consistent

composite air/ground picture.

Evolutionary acquisition processes have been developed to leverage the advantages offered by a technology that leaps ahead every 12-18 months. Our Global Command and Control System (GCCS) serves as the model for this novel approach to acquisition. The GCCS model, supported by the Defense Information Infrastructure Common Operating Environment (DII COE) and the Joint Technical Architecture (JTA), allows rapid insertion of applications which add value to the warfighter. Tight configuration control, stringent security and standard software are the keys to GCCS. Our premier command and control capability provides the warfighter with a fused, near real-time common operational picture of the battlespace and the ability to coordinate, direct and respond vertically and horizontally to prosecute the mission. The lessons we have learned in the GCCS program over the last three years are being applied directly to the Global Combat Support System (GCSS) today – an evolving capability whose utility was demonstrated during the war in Kosovo.

Our efforts to partner with Industry are proceeding along a number of fronts. We have entered into a ongoing dialogue to address technological advances in the satellite communications and computing arenas to increase our understanding of how technology can improve our

warfighting capabilities as well relaying our broad requirements for the future. These technical exchange opportunities help pave the way for capability development with an eye toward the feasible and the practical.

Appropriate levels of funding for the components of the Global Information Grid must be considered in relationship to the global capability as a whole. The Global Information Grid satisfies requirements of tactical and strategic missions in an integrated and complex end-to-end fashion. Lack of funding in one area, such as connectivity or computers, impacts the capability of the whole. The Services and Agencies have submitted plans to provide bandwidth, computing power, network operations, information assurance, and applications as well as other related programs, all designed to achieve the single goal of the Global Information Grid. These funding requests approach our minimum requirements today within the resources available. The Services' budget requests are based on operational requirements, many of which were highlighted in demonstrations and experiments. The unifying theme of the Global Information Grid provides a conceptual framework for developing an investment strategy to achieve Information Superiority.

Integrating across Service experimentation efforts has given us insights into the joint combat power enabled by the Global Information

Grid. In the Army's Advanced Warfighting Experiments (AWEs) tactical internets increased combat power by up to 250% as compared to a non-networked environment. The Air Force has demonstrated a 250% increase in the kill ratio of an F-15C employing data links. The Navy has demonstrated significant improvement in warfighting effectiveness in the counter-Special Forces mission area. Similar results have been seen in the Marine Corps.

These capabilities highlight the key role of "the network" in enabling Information Superiority and demonstrates that Information Superiority is not just about technology, but about using people who use information to develop a competitive advantage. This, however, provides both challenges and opportunities.

The Challenges Ahead

There is no shortage of challenges and opportunities in the Information Superiority arena. Let me outline a few of the ones we face, with a special emphasis on Information Assurance.

The Military and Commercial Sectors must co-exist. A strong

economy and a strong military are both increasingly dependent on networks. In some cases, our information rides through the same pipes. In other cases, we are in contention for resources that cannot be shared, such as frequency spectrum. To preclude mutual interference, we continue to work with our civil, commercial and international partners to preserve our access to RF spectrum.

As we move forward in deploying the Global Information Grid, we must continue to balance investments in our satellite communications capacity. Our objective is to determine the appropriate mix of military and commercial capabilities to ensure worldwide coverage for our tactical and strategic users. We are entering an era of great technological improvements in the satellite communications marketplace that provide significant promise for increased capability for the warfighter.

When working with coalition partners, we must accommodate multi-national technologies, many of which are developed outside of the U.S. Our challenge is to ensure interoperability of these different but similar capabilities to ensure success with our coalition partners.

Kosovo pointed out the need for more communications capacity in our theaters. Thanks to some quick reaction by our Services and Agencies, we were able to provide adequate communications capacity to support the Air war. Had we been involved in a ground operation in

Kosovo our communications limitations would have impacted the conduct of operations. Although we are working on ways to reduce the communications demand, our need for bandwidth has grown dramatically in the last few years because of the increased reliance on video teleconferencing, real-time video, imagery and web-based technology. We need your continued support in funding critical components of the Global Information Grid, especially connectivity and computing power. Information Assurance (IA) studies conducted over the past few years have provided ample guidance in determining the technology required for our defense in depth strategy. The challenge before us is to apply precious resources to field capabilities. We can't afford to allow the "best" to get in the way of the "good enough." The difficult part is determining the "good enough."

As we continue to operationalize information assurance, we will field equipment and promulgate policies to optimize CINC-centric operations. We are developing an Information Assurance Concept of Operations (CONOPs) for the deployed environment. This document will help standardize and professionalize IA in every Joint Task Force we send to the field. We are also orchestrating the deployment of a suite of equipment and software to ensure Joint Task Force Commanders leave home with the right IA capabilities to protect initial and follow-on operations rather than evolving to some level of protection over time.

Joint directed exercises and training are critical evolutions in institutionalizing joint doctrine and TT&P associated with operating and securing our critical networks, and maintaining our Global Information Grid. Future exercises will focus on specific cyber threats and risk mitigation techniques as well as dynamic allocation of network resources. We must expand these activities into the coalition training environment.

We are engaged in an aggressive validation of our current doctrine and guidance documentation that provides the direction to the components of the Global Information Grid. These include two doctrinal publications, 22 policy and guidance instructions and five detailed procedural manuals. Particular emphasis is being paid to the Defense in Depth strategy that directs the CINCs, Services and Agencies to put in place a minimum set of capabilities for the network, enclave, computing environment and the critical security infrastructure including use of Public Key Infrastructure (PKI) technology. Although we are moving in the right direction, we are only moving as fast as the funding allows.

Another area needing attention is our ability to "red team"—that is, allowing our technical experts to attack and exploit our own networks. These teams would act as independent assessors, able to show us our own vulnerabilities without fear of reprisal or breaking the law.

Currently, however, the red teaming process requires too much legal preparation and prior approval. As a result, there are very few "no-notice" red teaming efforts today. We must address the legal barriers that inhibit our ability to identify our own weaknesses before the enemy has the opportunity to exploit them.

Although DOD networks were not affected by the rash of recent attacks against commercial web sites such as E-Bay and CNN, DoD continues to see an ever-growing number of attacks against our information systems. It is time to reevaluate the penalties associated with deliberate hacking. The recent case law developed from cases such as Melissa virus attacks, and numerous, highly publicized hacking events provides enough evidence for the legal community to review current laws to determine if they are sufficient to deter future attacks against our systems.

We cannot operate the Global Information Grid without people. We are using "special skill" rewards to attract, train, and retain our best Soldiers, Sailors, Airmen, and Marines. However, our Total Force Information Technology Warriors are faced with choosing between their military professions and opportunities in the commercial sector that will compensate them at a much higher rate. We must continue to assess our retention programs, proficiency pay, and operational tempo, which

affect these highly trained and experienced people. They are truly our Nation's most precious resource.

Finally, we cannot view the command, control, communications and computers (C4) systems and the intelligence, surveillance and reconnaissance (ISR) budgets as bill payers for traditional Weapon Systems, but rather as the entry fee for the transformation that must be paid up front.

Conclusion

Ten to twenty years from now, I believe that people will look back on this period at the beginning of the 21st century and say one of two things. There was an tremendous opportunity for transformation – but it was squandered, because the key role of the Global Information Grid was not appreciated, or... there was a tremendous opportunity and it was capitalized upon by the DoD and Congress working together to make a difference.

In conclusion, I believe we are making solid progress toward implementing a Joint Strategy for Information Superiority that supports

our Warfighters. Mr. Chairman and Members of the Committee, I look forward to helping make the Information Superiority strategies that I have shared with you this afternoon a reality, and to addressing you in the future regarding our successes and way ahead. On behalf of the Chairman of the Joint Chiefs of Staff, I appreciate the opportunity to present the Joint Staff's insights on how to advance this issue of growing national importance – Information Superiority.

Statement of the Honorable William A. Reinsch
Under Secretary of Commerce for Export Administration

Before the

Subcommittee on Communications
Senate Commerce Committee

March 8, 2000

Mr. Chairman, I welcome this opportunity to appear before you to discuss the Federal government's efforts to protect the nation's critical infrastructures.

Inter-dependent computer networks are an integral part of doing business in the Information Age. America is increasingly dependent upon computer networks for essential services, such as banking and finance, emergency services, delivery of water, electricity and gas, transportation, and voice and data communications. New ways of doing business in the 21st century are rapidly evolving. Business is increasingly relying on E-commerce for its commercial transactions. At the same time, recent hacking attempts at some of the most popular commercial Web sites underscore that America's information infrastructure is an attractive target for deliberate attack or sabotage. These attacks can originate from a host of sources, such as terrorists, criminals, hostile nations, or the equivalent of car thief "joyriders." Regardless of the source, however, the potential for cyber damage to our national security and economy is evident.

Protecting our critical infrastructures requires that we draw on various assets of the government. When specific incidents or cyber events occur, the government needs a capacity to issue warnings, investigate the incident, and develop a case to punish the offenders. The National Information Protection Center at the FBI is organized to deal with such events as they occur.

Over the long term, the government also has a duty to be proactive to ensure that our computer systems are protected from attack. Critical infrastructure protection involves assets of both the government and the private sector. A number of agencies have responsibilities with respect to government computer systems. The Department of Defense is well on its way to securing its critical systems, and the Office of Management and Budget (OMB) and the National Institute of Standards and Technology at the Department of Commerce (NIST) have responsibility for information resources management of computer systems in Federal agencies.

I want to make clear that the Federal government's responsibility in this area with respect to the commission of crimes is only part of the equation. The infrastructures at risk are owned and operated by the private sector. The use of information technology is so embedded in the core operations and customer service that inevitably, it will be they who must work together to take the steps necessary to protect themselves. We can help. The first major step is the elevation of

awareness across industry of the "business case for action" for leaders within industry. They have a commercial interest in maintaining a secure business environment that assures public confidence in their institutions. We can also help identify problems, good practices in management policies and strategies, and publicize them, encourage planning, promote research and development, convene meetings. In short, we can act as a catalyst for industry to mobilize. That is precisely the role the Commerce Department is playing in several ways.

Another active area is the development of the Partnership for Critical Infrastructure Security. The Partnership is a collaborative effort between industry and government. This undertaking brings representatives of the infrastructure sectors together in a dialogue with each other and other stakeholders, including the risk management and investment communities, mainstream businesses, and state and local governments. It complements the NIPC's focus on cyber-terrorism by encouraging industry to collaborate on information security issues. Secretary Daley and I met with senior members of Partnership companies in December in New York. We will met-again last month in Washington, D.C., with over 220 senior members of more than 120 - Partnership companies to encourage business leaders to adopt information security as an integral business practice. The Partnership agreed to address such important issues as, cross-sector vulnerability assessments, information sharing, and R&D requirements.

CIAO also is assisting Federal agencies in conducting analyses of their own dependencies on critical infrastructures. CIAO has just finished an ambitious pilot program that identifies the critical assets of the Commerce Department and maps out dependencies on governmental and private sector infrastructures. This program will provide important input to managers and security officials as they seek to assure their critical assets against cyber attacks.

President Clinton has increased funding for critical infrastructure protection substantially over the past three years, including a 15% increase in his FY 2001 budget to $2.01 billion. He has also developed and funded new initiatives to defend the nation's systems from cyber attack.

The Commerce Department, through its Critical Infrastructure Assurance Office (CIAO), coordinated the development of the *National Plan for Information Systems Protection*. President Clinton announced the release of Version 1.0 of the Plan on January 7.

It represents the first attempt by any national Government to design a way to protect those infrastructures essential to the delivery of electric power, oil and gas, communications, transportation services, banking and financial services, and vital human services. Increasingly, these infrastructures are being operated and controlled through the use of computers and computer networks.

The current version of the Plan focuses mainly on the domestic efforts being undertaken by the Federal Government to protect the Nation's critical cyber-based infrastructures. Later versions will focus on the efforts of the infrastructure owners and operators, as well as the risk management and broader business community. Subsequent versions will also reflect to a greater degree the interests and concerns expressed by Congress and the general public based on their feedback. That is why the Plan is designated *Version 1.0* and subtitled *An Invitation to a*

Dialogue -- to indicate that it is still a work in progress and that a broader range of perspectives must be taken into account if the Plan is truly to be "national" in scope and treatment.

II. The Plan: Overview and Highlights

President Clinton directed the development of this Plan to chart the way toward the attainment of a national capability to defend our critical infrastructures by the end of 2003. To meet this ambitious goal, the Plan establishes 10 programs for achieving three broad objectives. They are:

Objective 1: Prepare and Prevent: Undertake those steps necessary to minimize the possibility of a significant and successful attack on our critical information networks, and build an infrastructure that remains effective in the face of such attacks.

> Program 1 calls for the Government and the private sector to identify significant assets, interdependencies, and vulnerabilities of critical information networks from attack, and to develop and implement realistic programs to remedy the vulnerabilities, while continuously updating assessment and remediation efforts.

Objective 2: Detect and Respond: Develop the means required to identify and assess attacks in a timely way, contain such attacks, recover quickly from them, and reconstitute those systems affected.

> Program 2 will install multi-layered protection on sensitive computer systems, including advanced firewalls, intrusion detection monitors, anomalous behavior identifiers, enterprise-wide management systems, and malicious code scanners. To protect critical Federal systems, computer security operations centers will receive warnings from these detection devices, as well as Computer Emergency Response Teams (CERTs) and other means, in order to analyze the attacks, and assist sites in defeating attacks.
>
> Program 3 will develop robust intelligence and law enforcement capabilities to protect critical information systems, consistent with the law. It will assist, transform, and strengthen U.S. law enforcement and intelligence Agencies to be able to deal with a new kind of threat and a new kind of criminal -- one that acts against computer networks.
>
> Program 4 calls for a more effective nationwide system to share attack warnings and information in a timely manner. This includes improving information sharing within the Federal Government and encouraging private industry, as well as state and local Governments, to create Information Sharing and Analysis Centers (ISACs), which would share information among corporations and state and local Governments, and could receive warning information from the Federal Government. Program 4 additionally calls for removal of existing legal barriers to information sharing.
>
> Program 5 will create capabilities for response, reconstitution, and recovery to limit an attack while it is underway and to build into corporate and Agency continuity and recovery plans the ability to deal with information attacks. The goal for Government and

the recommendation for industry is that every critical information system have a recovery plan in place that includes provisions for rapidly employing additional defensive measures (e.g., more stringent firewall instructions), cutting off or shutting down parts of the network under certain predetermined circumstances (through enterprise-wide management systems), shifting minimal essential operations to "clean" systems, and to quickly reconstitute affected systems.

Objective 3: Build Strong Foundations: Take all actions necessary to create and support the Nation's commitment to Prepare and Prevent and to Detect and Respond to attacks on our critical information networks.

Program 6 will systematically establish research requirements and priorities needed to implement the Plan, ensure funding, and create a system to ensure that our information security technology stays abreast with changes in the threat environment.

Program 7 will survey the numbers of people and the skills required for information security specialists within the Federal Government and the private sector, and takes action to train current Federal IT workers and recruit and educate additional personnel to meet shortfalls.

Program 8 will explain publicly the need to act now, before a catastrophic event, to improve our ability to defend against deliberate cyber-based attacks.

Program 9 will develop the legislative framework necessary to support initiatives proposed in other programs. This action requires intense cooperation within the Federal Government, including Congress, and between the Government and private industry.

Program 10 builds mechanisms to highlight and address privacy issues in the development of each and every program. Infrastructure assurance goals must be accomplished in a manner that maintains, and even strengthens, American's privacy and civil liberties. The Plan outlines nine specific solutions, which include consulting with various communities; focusing on and highlighting the impact of programs on personal information; committing to fair information practices and other solutions developed by various working groups in multiple industries; and working closely with Congress to ensure that each program meets standards established in existing Congressional protections.

The Clinton Administration has developed and provided full or pilot funding for the following key initiatives designed to protect our computer systems:

* Establishing a permanent Expert Review Team (ERT) at NIST that will help agencies conduct vulnerability analyses and develop critical infrastructure protection plans. ($5 million).

* Funding seven Public Key Infrastructure model pilot programs in FY 2001 at different

Federal agencies. ($7 million).

* Designing a Federal Intrusion Detection Network (FIDNET) to protect vital systems in Federal civilian agencies, and in ensuring the rapid implementation of system "patches" for known software defects. FIDNET will operate in full compliance with all existing privacy laws. ($10 million).

* Developing Federal R&D Efforts. R&D investments in computer security will grow by 31% in the FY 2001 budget. ($606 million).

* Establishing an Institute for Information Infrastructure Protection. The Institute would identify and address serious R&D gaps that neither the private sector nor the Government's national security community would otherwise address, but that are necessary to ensure the robust, reliable operation of the national information infrastructure. The President announced he would propose initial funding of $50 million for the Institute in his FY2001 Budget. Funding would be provided through the Commerce Department's National Institute of Standards and Technology (NIST) to this organization. The Institute was first proposed by the scientists and corporate officials who served on the President's Committee of Advisors on Science and Technology, and supported by leading corporate Chief Technology ($50 million).

* National Infrastructure Assurance Council (NIAC). The President signed an Executive order creating this Advisory Council last year. Its members are now being recruited from senior ranks of the critical infrastructure-industries, including the information technology, and state and local governments.

In addition, the President announced a number of new initiatives designed to support efforts for enhancing computer security, including a $9 million FY 2000 budget supplemental to jump-start key elements of next year's budget.

In early February, Secretary Daley met with the President and 25 senior executives concerned about the recent disruptions to the Internet. This meeting reinforced the need for further cooperation between government and industry to help the private sector develop its action agenda for cyber security. The incidents of early February are not cause for pushing the panic button, but they are a wake up call for action. As the President said, "I think there is a way that we can clearly promote security." The President has submitted a budget proposal that funds a number of initiatives that address critical information systems protection. If we are to reap the benefits of the Information Age, we need to take action to maintain public confidence in a secure business environment that ensures both our national security and the growth of our economy.

JoAnn Ward 03/06/2000 02:23:07 PM

Record Type: Record

To: Steven M. Rinaldi/OSTP/EOP@EOP

cc: Gerald L. Epstein/OSTP/EOP@EOP
Subject: Additional Commerce Critical Infrastructure Testimony for a Senate Commerce subcommittee hearing

Steve: Your action. Due Tuesday, 3/7, at 10 AM. jw
---------- Forwarded by JoAnn Ward/OSTP/EOP on 03/06/2000 02:17 PM ----------

Richard A. Kostro
03/06/2000 01:42:35 PM

Record Type: Record

To: JoAnn Ward/OSTP/EOP@EOP

cc:
Subject: Additional Commerce Critical Infrastructure Testimony for a Senate Commerce subcommittee hearing

---------- Forwarded by Richard A. Kostro/OSTP/EOP on 03/06/2000 01:45 PM ----------

Richard A. Kostro
03/06/2000 12:50:36 PM

Record Type: Record

To: Karen R. Heitkotter/OSTP/EOP@EOP

cc:
Subject: Additional Commerce Critical Infrastructure Testimony for a Senate Commerce subcommittee hearing

---------- Forwarded by Richard A. Kostro/OSTP/EOP on 03/06/2000 12:53 PM ----------

From: E. Holly Fitter on 03/06/2000 12:39:02 PM
Record Type: Record

To: See the distribution list at the bottom of this message

cc: John D. Burnim/OMB/EOP@EOP
Subject: Additional Commerce Critical Infrastructure Testimony for a Senate Commerce subcommittee hearing

66028

cc Rinaldi

March 3, 2000 File: M. 446

DRAFT NIST HEARING TESTIMONY

TO:

John Gray
Jon Orszag/Laureen Daly
Mark Bohannon
Kelly Carnes
Mike Rubin
John Sparrow
Greg Finley
Matt Bailey
Verna Hines/Kevin Kimball

Ed Roback
Roman Sloniewsky
Cathleen Wasilewski
Krysten Jenci
Rosemary Warren
Anstr Davidson

FROM: Sabrina McLaughlin/ Office of the Assistant General Counsel for Legislation and Regulation

SUBJECT: *Draft NIST Testimony Concerning Critical Infrastructure Protection and More!*

Attached for your review is the draft testimony of NIST's Deputy Director, Karen H. Brown, scheduled to be delivered on March 9, 2000 before the House Committee on Government Reform's Subcommittee on Government Management, Information, and Technology. Brown's testimony discusses NIST's role in computer security in general, cryptography, and critical infrastructure protection, as well as initiatives such as the Institute for Information Infrastructure Protection and the Expert Review Team.

It is unknown what other Government officials have been invited to testify. Please forward me any concerns that you may have with the attached testimony no later than:

2:00 PM, Monday, March 6, 2000.

I apologize for the short turnaround time, but will proceed with the clearance process on the assumption that you have no objections if I have not heard from you by that time. Please call me at 482-0445 or fax this cover sheet to (202) 482-0512 if you have any questions concerning this request. Thank you.

cc: M. Levitt; K. Clark; P. Dalmut; Janet Miller

Agency: _____ Date: _____

Name: _____

__ Concur

__ Do not object

__ Have no comment

__ Have comments (see the following ___ pages)

Karen H. Brown

Deputy Director

National Institute of Standards and Technology

Technology Administration

U.S. Department of Commerce

before the

Committee on Government Reform
Subcommittee on Government Management,
Information, and Technology

March 9, 2000

Mr. Chairman and members of the subcommittee thank you for the invitation to speak to you today about computer security issues. I am Karen Brown, Deputy Director of National Institute of Standards and Technolgoy of the Department of Commerce's Technology Administration.

Computer security continues to be an ongoing and challenging problem that demands the attention of the Congress, the Executive Branch, industry, academia, and the public. Computer security is not a narrow, technical concern. The explosive growth in Electronic Commerce highlights the nation's ever increasing dependence upon the secure and reliable operation of our computer systems. Computer security, therefore, has a vital influence on our economic health and our nation's security and we commend the Committee for your focus on security.

Today I would like to address NIST's computer security activities that contribute to improving computer security for the Federal Government and the private sector. I also would like to briefly describe for you our proposed new program activities for next year as requested in the President's budget.

Under NIST's statutory federal responsibilities, we develop standards and guidelines for agencies to help protect their sensitive unclassified information systems. Additionally, we work with the IT industry and IT users in the private sector on computer security in support of our broad mission to strengthen the U.S. economy, and especially to improve the competitiveness of the U.S. information technology (IT) industry. As awareness of the need for security grows, more secure products will be more competitive in the marketplace. Addressing security will also help ensure that Electronic Commerce growth is not limited because of security concerns.

In meeting the needs of our customers in both the public and private sector, we work closely with industry, Federal agencies, testing organizations, standards groups, academia, and private sector users. Cooperation and collaboration are essential to tackle many common problems facing users throughout the country.

What does NIST do specifically? To meet these responsibilities and customer needs, we first work to improve the awareness of the need for computer security. This helps increase demand for secure and reliable products. Additionally, we research new technologies and their security implications and vulnerabilities and develop guidance to advise users accordingly. We work to develop security standards and specifications to help users specify security needs in their procurements and establish minimum security requirements for Federal systems. We develop and manage security testing programs, in cooperation with private sector testing laboratories, to enable users to have confidence that a product meets a security specification. We also produce security guidance to promote security planning, and secure system operations and administration. I will briefly discuss the need and benefits of each.

First, there is a need for timely, relevant, and easily accessible information to raise awareness about the risks, vulnerabilities and requirements for protection of information systems. This is particularly true for new and rapidly emerging technologies, which are being deliver with such alacrity by our industry. We host and sponsor information sharing among security educators, the Federal Computer Security Program Managers' Forum, and industry. We seek advice from our advisory board of computer experts (Computer System Security and Privacy Advisory Board). We meet regularly with members of the Federal computer security community, including the Chief Information Officers' Security Committee, and the Critical Information Assurance Office. We actively support information sharing through our conferences, workshops, web pages, publications, and bulletins. Raising awareness helps ensure appropriate attention is accorded security and helps increase the demand for secure products and security services.

A second need is for research on information technology vulnerabilities and the development of techniques for the cost-effective security. When we identify new technologies that could potentially influence our customers' security practices, we research the technologies and their potential vulnerabilities. We also work to find ways to apply new technologies in a secure manner. The solutions that we develop are made available to both public and private users. Some examples are methods for authorization management and policy management, ways to detect intrusions to systems, and demonstrations of mobile agents. Research helps us find more cost-effective ways to implement and address security requirements.

Third is the need for standards, and for ways to test that standards are properly implemented in products. For example, cryptographic algorithms and techniques are essential for protecting sensitive data and electronic transactions. NIST has long been active in developing Federal cryptographic standards and working in cooperation with industry consensus voluntary standards organizations in this area. Moreover, in the standards area we have been working with the private sector in preparing for the future. We are leading a public process to develop the Advanced Encryption Standard (AES), which will serve 21st century security needs. Another aspect of our standards activities concerns Public Key and Key Management Infrastructures. The use of cryptographic services across networks requires the use of "certificates" that bind cryptographic keys and other security information to specific users or entities in the network. We have been actively involved in working with industry to promote the security and interoperability of such infrastructures.

Standards help users know what security specifications may be appropriate for their needs. Testing complements this by helping users have confidence that security standards and specifications are correctly implemented in the products they buy. Testing also helps reduce the potential that products contain vulnerabilities that could be used to attack systems.

For over five years, we have led the Cryptographic Module Validation Program, which has now validated about 90 modules with another 50 expected this year. This successful program utilizes private sector accredited laboratories to conduct security conformance testing of cryptographic modules against a Federal standard we develop and maintain. More recently, we have been working with the international security community to define security criteria in an international standard that can be used to develop security specifications for products, such as firewalls or operating systems. We are actively working with industry partners in the smart card, health care, and telecommunications fields to accomplish such development of specifications.

Many of these activities are being done in cooperation with the Defense Department's National Security Agency in our National Information Assurance Partnership. Private sector laboratories are being accredited under the National Voluntary Laboratory Accreditation program to conduct such testing. The effort involves developing testing competencies and a process for accrediting testing organizations. The goal is to enable product developers to get their products tested easily and voluntarily, and for users to have access to information about tested products. Under this program we have also led the development of an international mutual recognition arrangement whereby the results of testing in the U.S. are recognized by our international partners, thus reducing the costs to industry.

Advice and technical assistance for both government organizations and private sector users is the fourth need. For example, we have issued guidance including telecommuting and security, security concerns inherent in PBX technology, security requirements in PKI implementation, use of firewalls, and intrusion detection in networks. We are also provide program guidance to agencies and are working to complete a document on security program metrics and self-assessment. The assistance information and guidelines that we have developed are available to all users free-of-charge via our web site. We also support agencies on specific security projects on a cost-reimbursable basis when NIST expertise is required.

While I have given you a few examples of NIST's work, I obviously have not covered everything. I want to emphasize that there is still much more to be done to address the continuing challenges of computer security. To put our program in perspective, please keep in mind that approximately $6 million of direct Congressional funding supports both our Federal and industry computer security responsibilities. (In addition, we receive approximately $2 million in outside agency funding to provide technical assistance on particular projects.) This is plainly not enough.

As reflected in the requests made in the White House's FY-2001 budget, NIST needs additional resources to help improve the security posture of the Federal government. Looking at the critical information infrastructures of the nation, we also need substantial investments in security research to find ways to protect our infrastructures.

To address the need for additional research to protect our critical infrastructures, the White House has proposed establishing a $50 million Institute for Information Infrastructure Protection, which was initially recommended by the President's Committee of Advisors on Science & Technology (PCAST). This Institute will identify and fill the gaps not being met by private sector market demands or Government agency mission objectives in critical infrastructure protection and provide a strong and secure foundation to protect the various critical infrastructures upon which the Nation's security and economy rely. The Institute's R&D will include work that can be applied to protect multiple sectors' infrastructures, and thus will complement sector-specific R&D underway elsewhere in the government and private sector. This initiative will help strengthen the focused existing and planned security architectures within the critical infrastructure sectors and help prepare the owners/operators of those infrastructures to survive potential hostile activities. The Institute will not have any direct role in support of law enforcement or deterring attacks, but will fund R&D to develop new generations of IT security solutions that DoJ/FBI, other agencies, and the private sector can use to prevent and respond to future cyber-threats. The Institute will be a partnership among industry, academia and the government (including both state and local governments). At the core of the partnership is the Institute's selection of information infrastructure protection R&D focus areas, which will rely heavily on advice and guidance obtained from outside experts.

The security of Federal systems must also be improved. These systems contain sensitive information about our citizens and provide services upon which our citizens' safety and well-being depend. The government should exert leadership and set an example for the nation in protecting against risks and vulnerabilities. Two of the budget proposals focus primarily upon the security of Federal systems. Specifically, we propose to establish an Expert Review Team (comprised of eight people) to advise agencies of their vulnerabilities, help prioritize and develop strategies for security fixes, assist agencies in preparing for future security threats, and help agencies plan for security in new system developments. This will complement the reporting activities of programs such as FedCIRC. Secondly, we seek a five million dollar increase to enable additional critical activities in the area of cryptography, security management and best practices guidance, and the protection of supervisory control systems.

So let me close by again emphasizing that our national commitment to improve security must be increased. NIST stands ready to play a key role through supporting the proposed Institute, leading the Expert Review Team, and conducting additional work to developing needed security guideline and standards, research in security technology, leading testing programs, and raising awareness and demand for security products and services. This will augment the already important activities we have underway. We look forward to continuing this work, and believe that your support of the critical new activities would help us to do so.

I will be pleased to answer any questions.