[H.A.S.C. No. 108–12]

INFORMATION TECHNOLOGY IN 21ST CENTURY BATTLESPACE

BEFORE THE

TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

HEARINGS HELD
JULY 24, AND OCTOBER 21, 2003

U.S. GOVERNMENT PRINTING OFFICE
94–542 WASHINGTON : 2004

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

[H.A.S.C. No. 108–12]

INFORMATION TECHNOLOGY IN 21ST CENTURY BATTLESPACE

BEFORE THE

TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

HEARINGS HELD
JULY 24, AND OCTOBER 21, 2003

U.S. GOVERNMENT PRINTING OFFICE
94–542 WASHINGTON : 2004

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

TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE

JIM SAXTON, New Jersey, *Chairman*

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

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

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

CONTENTS

CHRONOLOGICAL LIST OF HEARINGS

2003

THURSDAY, JULY 24, 2003

CYBER TERRORISM: THE NEW ASYMMETRIC THREAT

STATEMENTS PRESENTED BY MEMBERS OF CONGRESS

WITNESSES

APPENDIX

TUESDAY, OCTOBER 21, 2003

C4I INTEROPERABILITY: NEW CHALLENGES IN 21ST CENTURY WARFARE

STATEMENTS PRESENTED BY MEMBERS OF CONGRESS

WITNESSES

APPENDIX

CYBER TERRORISM: THE NEW ASYMMETRIC THREAT

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES,
Washington, DC, Thursday, July 24, 2003.

The subcommittee met, pursuant to call, at 10:01 a.m., in room 2118, Rayburn House Office Building, Hon. Jim Saxton (chairman of the subcommittee) presiding.

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

Mr. SAXTON. Good morning. The Subcommittee on Terrorism, Unconventional Threats and Capabilities meets this morning to assess the new asymmetric threat of cyber terrorism. In particular, we would like to have a better understanding of this threat against the Department of Defense (DOD) information technology (IT) systems and networks.

Information dominance is a cornerstone of the Department's force transformation in the 21st century. We have witnessed these remarkable technological capabilities—from sensors gathering intelligence to sending that information to shooters in the air or on the ground or both. And both in Operation Enduring Freedom and Operation Iraqi Freedom, these issues were crucial.

This incredible transmission of data was accomplished with greater accuracy, in a shorter amount of time and with fewer casualties. Armed with these incredible capabilities, our military forces have gone into battle with more situational awareness than any other troops in history.

While new technological advances bring information superiority, it also brings new responsibilities and new challenges. Technology evolves rapidly.

While programmers and software developers build more advanced systems to run more tasks, criminals become more creative in their methods to break into these systems. Their purpose may be to steal information, wreak havoc or send out false commands or information.

Without a defense-wide information assurance policy and implemented practices, the Department of Defense's networks may be vulnerable to anyone who has a computer, the knowledge and the willpower to launch cyber attacks.

Information assurance (IA) is a critical issue in the Department because it operates approximately 3 million computers, 100,000 local area networks and 100 long-distance networks. These systems

include military service-based, joint defense and intelligence computers and networks are a part of the Global Information Grid (GIG), part of which is dependent on the commercial civilian systems.

All of these systems are susceptible to acts of cyber terrorists 24 hours a day. I wholeheartedly agree with Secretary of Defense Donald Rumsfeld that IT is the enabler behind defense transformation.

What we need is the ability to leverage the technology and commercial best practices to ensure the security and integrity of the Department's networks. This is a major undertaking with extraordinary consequences.

While the subcommittee recognizes the critical efforts and difficulty of implementing the Defense-wide Information Assurance Program (DIAP), concerns have been raised that there is not sufficient oversight or management at the Department to achieve the objectives contained in the program.

The subcommittee is interested to learn more about the Department's information assurance policy and the immediate and potential cyber threats against the Department's IT systems and networks. Additionally, the subcommittee is interested to learn about the procedures or defense mechanisms presently in place at the department to counter cyber attacks.

Finally, the subcommittee would like to know more about the processes or best commercial practices that private industry has implemented to handle cyber security issues and whether these practices are applicable to the Department. This hearing will attempt to determine what progress the Department has made in implementing its DIAP.

We are also interested to learn what challenges lie ahead for the Department as it confronts cyber terrorists in cyberspace.

I would like to yield at this point to Mr. Meehan, our ranking member, for any comments he may wish to make.

[The prepared statement of Mr. Saxton can be found in the Appendix on page 41.]

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

Mr. MEEHAN. Thank you, Mr. Chairman. And I commend you for holding this hearing. And I join you in welcoming our guests this morning.

Mr. Chairman, I view information technology or IT as critical to both the national security and the economic strength of the United States. You may remember that at a hearing this past April, I raised this very point and questioned Secretary Stenbit about his vision of IT for enabling military transformation.

We heard a great many things that day. And many were positive. Yet we also learned that all is not rosy.

Many of the existing DOD IT systems remain redundant, outdated or inefficient. And many are vulnerable to cyber attacks from terrorists, criminals, hackers and even foreign intelligence services.

That day's testimony also brought forth the importance of the Department of Defense IT modernization budget, something that

our panel subsequently proposed to cut. This cut, nearly $2 billion, is currently under consideration before the full House-Senate Defense Authorization Conference. And as I have said before, I question the wisdom of such a proposal.

Today, we receive further testimony about the increasing nature of threats to the information systems, the pervasive weaknesses to the DOD IT systems and the challenges and proposed solutions that we must consider. I am particularly concerned with the status of the Department's enterprise architecture and the investment management controls needed to implement it.

But my concern also includes our Nation's overall approach to this evolving and growing challenge during this era. I hope that today's guests will help us better understand these issues and also, I think, assist us in our efforts to plan down the road, for we have many, many important decisions that must be made, both in terms of this subcommittee and the full committee. And again, Mr. Chairman, I thank you for putting this hearing together.

Mr. SAXTON. Thank you, Mr. Meehan. We have one very distinguished panel today. We are very pleased to welcome you all here. And let me just, by way of introduction, say that I would like to welcome Professor Eugene H. Spafford, who is the director of Purdue University's Center for Education and Research and Information Assurance and Security.

We also will hear from Mr. Robert F. Lentz, director of information assurance, Office of the Assistant Secretary of Defense for Networks and Information Integration and the Chief Information Officer (CIO) at the Department of Defense.

In addition: Mr. Robert Dacey, Director of the General Accounting Office technology team; and Mr. Scott Charney, Chief Security Strategist for the Microsoft Corporation.

Welcome. And thank all of you for coming. I know that you have obviously made some sacrifices to be with us here today. And we appreciate your time and effort to get here.

At the outset, I would like to ask unanimous consent that all members' and witnesses' written opening statements will be included in the record. And also I would like to ask unanimous consent that all articles, exhibits and extraneous or tabular material referred to be included in the record. Without objection on both counts, so we will begin to hear from our witnesses.

Professor Spafford, if you would like to begin, we would appreciate it.

STATEMENT OF EUGENE SPAFFORD, DIRECTOR AND PROFESSOR, CENTER FOR EDUCATION AND RESEARCH AND INFORMATION ASSURANCE AND SECURITY, PURDUE UNIVERSITY

Mr. SPAFFORD. Thank you, Chairman Saxton and Ranking Member Meehan and members of the committee. Thank you very much for inviting me here to speak to you.

This is an area where I have been conducting research and education for 20 years. And it is one of great importance to the country and to me as well, as an individual.

I have provided in my written testimony background and history of a number of the software threats that can be committed against

our infrastructure, our information infrastructure. And I am not going to go into detail on all of those here.

I would like to single out two of those issues in particular that I believe are particularly important. As you know, we have an extremely well trained, well equipped military. And they demonstrate their excellence repeatedly on behalf of the country.

However, the technology and the training that they have is very dependent upon the information technology that they use. There is computing technology at the heart of the command and control systems, communications systems, smart weapons systems and the logistics that provide the material that they need to carry out their mission.

If that is disrupted, if that is altered, if that is denied, it creates a great hardship and puts them in harm's way, as well as interfering with their missions. So of the many issues that face them, I believe there are two that we should consider especially.

The first is that over the last two decades, we have adopted a policy, we followed a policy of using COTS products—commercial, off-the-shelf products—whenever possible. This has had great benefit to our military and to our taxpayers because the software has developed very quickly. We have been able to get advance software quickly, deploy it and use it in a cost-effective manner to provide capabilities that our military might not otherwise have.

There is, however, a downside to our increasing dependence upon the commercial, off-the-shelf products. Most of those products are not written to be used in an environment where there is significant threat.

Today's threat environment is major. We have, as was noted in your opening remarks, attacks being committed by hackers, by anarchists, by criminals, probably by foreign intelligence services and, in some cases, perhaps more active attacks against our resources.

The COTS products have not been developed to be reliable and robust under those kinds of circumstances, particularly when used in high-stress environments such as occurs in the battlefield. We have furthermore gone to a very small set of COTS products for a majority of our platforms. And this forms a near monoculture.

When a new attack is found that is effective against one of these products, it sweeps through the entire network, not only the military, but government, academia and the public infrastructure. This should be of great concern to us, that these points of weakness occur.

And it is not just a few now and then. The Computer Security Emergency Response Team Coordination Center (CERT CC), the response center at the Software Engineering Institute (SEI), noted that last year there were 2,000 vulnerabilities reported for common COTS products alone.

This means that operators of systems may be in the position of applying three to five security-critical patches per week to every system under their control. That really is unacceptable for us to be in a state of high readiness.

The second issue that I believe bears considerable concern is the fact that we have much of this software and an increasing amount of this software is being written by individuals that we would not allow into the environments where it is operated. And the reason

for that is because they are not U.S. citizens. They have criminal records. They do not have any kind of background check.

A recent study that I saw quoted in a newspaper article said that 80 percent of all of our software companies either currently outsource to other countries some of their development or are planning to do so. This is wonderful for the world economy. It is very good for our U.S. economy.

It provides low-cost labor that allows our companies to compete better and produce software more effectively. But it also introduces a tremendous vulnerability to our systems because the software is being developed, sometimes tens of millions of lines, by individuals whose motivations and agenda may not be fully known.

We do not have the tools or the technology to fully examine that software to understand all of the features that may have been added without our request. As a result, we may be placing some of our critical operations and their personnel in danger from hidden logic bombs, Trojan horses and other kinds of mailware that will have been written into that software.

This is something that we need to be very cautious about and rethink out policies, as to how we are obtaining software and deploying it.

With that, I will leave any further comments in response to your questions. And I thank you for your attention.

[The prepared statement of Mr. Spafford can be found in the Appendix on page 107.]

Mr. SAXTON. Thank you very much. Mr. Dacey.

STATEMENT OF ROBERT DACEY, DIRECTOR, INFORMATION TECHNOLOGY TEAM, GENERAL ACCOUNTING OFFICE

Mr. DACEY. Mr. Chairman and members of the subcommittee, I am pleased to be here today to discuss the status of efforts by the Department of Defense to protect its information systems from cyber attacks.

As you requested, I will briefly summarize my written statement.

Dramatic increases in reported security incidents, the ease of obtaining and using hacking tools, the steady advance in sophistication and effectiveness of attack technologies, dire warnings of potential and more destructive attacks, including combined cyber and physical attacks, an increasing dependence on and standardization of information systems continue to evidence the growing threat of cyber attacks to our infrastructures.

The potential sources of attacks include individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence gathering and acts of war, as well as insiders. At the same time, although there have been some individual agency improvements, our most recent analysis of audit and evaluation reports for 23 major federal agencies continued to highlight significant information security weaknesses that place a broad array of federal operations at risk.

Concerned that significant weaknesses in federal information security make them vulnerable to attack, in October 2000, the Congress passed and the President signed Government Information Security Reform Provisions, commonly known as GISRA, requirements that are now permanently authorized and strengthened

through the recently enacted Federal Information Security Management Act, or FISMA.

In its fiscal year 2002 GISRA report, DOD reported that the Department has an aggressive information assurance posture and highlighted several initiatives and accomplishments, which include development of an overall Department-wide strategy that identifies goals and objectives for information assurance and in the process of aligning its strategic objectives and the strategy in developing milestones and performance measures for gauging success; two, the issuance of numerous information security policy directives, instructions, manuals and policy memoranda to establish a Department-wide information assurance policy framework; three, completing certification and accreditation of security controls for a sample of its networks; and four, significant progress in developing network defense capabilities.

However, DOD's reporting also acknowledges that a number of challenges remain for the Department in implementing both its policies and procedures and statutory information security requirements, including: completing actions to correct reported material weaknesses in information assurance; implementing key FISMA requirements for the systems reviewed. And another challenge will be eventually expanding FISMA reviews to all Department systems and networks.

Our past work has shown that an important challenge Federal agencies face in implementing information security management is ensuring that they have appropriate management structures and processes in place to strategically manage information security, as well as ensure the reliability of performance information.

For example, disciplined processes can routinely provide the agency with reliable, useful and timely information for day-to-day management of information security. DOD has undertaken its Defense-wide Information Assurance Program, or DIAP, to promote an integrated, comprehensive and consistent information assurance practice across the Department.

However, as indicated by the GISRA report, DOD's audit community indicated that DOD did not yet have a mechanism in place for comprehensively measuring compliance with department policies.

With the first agency reporting under FISMA expected in September of this year, updated information on the status of DOD's information assurance efforts will be available for continued congressional oversight.

Mr. Chairman, this concludes my testimony. I would be pleased to answer any questions that you or other members of the subcommittee may have.

[The prepared statement of Mr. Dacey can be found in the Appendix on page 55.]

Mr. SAXTON. Thank you very much, Mr. Dacey. Mr. Lentz.

STATEMENT OF ROBERT LENTZ, DIRECTOR, INFORMATION ASSURANCE, DEPARTMENT OF DEFENSE

Mr. LENTZ. Thank you, Mr. Chairman and members of the subcommittee. I am honored to be here and pleased to have the opportunity to speak with your committee as the DOD Information Assurance, or IA, Director about actions the Department of Defense

is taking to address the threats to the security of its network, systems and information.

We have and continue to make significant progress in our quest to secure and defend our computer networks. This committee has been briefed extensively on leveraging information technology to create a seamless, interoperable, net-centric environment.

I must underscore that our dependence on information technology is critical. IT and IA go hand in hand. The criticality of protecting and defending our information has become even more important as our adversaries see the way we conduct operations, both in peace time and in war time. In recognition of this, the Secretary established the protection of U.S. information networks from attack as another foundational transformation goal.

And Mr. Stenbit, the CIO, recently testified before your committee and has made IA one of his top three goals. To guide and manage the Department's IA portfolio, we established, with strong congressional support, the Defense-wide Information Assurance Program, the DIAP.

The DIAP is critical to guiding DOD investments, promoting enterprise decisionmaking and interoperability and is responsible for overseeing policy and architecture development. To enable transformation to net-centric operations, we are executing a comprehensive IA policy framework.

We have also designed an IA strategic plan that provides a corporate blueprint to leverage IT for business and warfighting environments and are in the process of developing a comprehensive IA end-to-end architecture to tie all the pieces together.

In addition, an IA senior, two-star working group has been put together to provide oversight over all these IA activities. This group has challenged us to make the policy process more open, visible, collaborative and, as a consequence, faster.

We are working with the private sector, the academic community and our closest allies to ensure sound management practices for governing our vast network. Our IA strategic plan, our road map, has five major goals.

Protecting information is goal one. This means that all information must be protected from end to end and through its life cycle from our most sensitive nuclear command and control to business transactions.

DOD has already invested in programs such as public key infrastructure, biometrics and a common access card program, so that by the end of the year, nearly all DOD personnel will be outfitted with a capability for identifying itself and accessing the network. It is a world-class network. We are also aggressively modernizing all of our cryptographic systems.

Goal two is defending the system and the network. Specifically, we must be able to recognize, to react and to respond to threats.

DOD systems and networks are constantly under attack and must be continuously defended, 24 x 7. Intrusion attempts into DOD continue to grow. And the speed and complexity of these attacks are increasing. Last year, we successfully defended against approximately 50,000 attempts to gain root-level access into the DOD network.

Goal three emphasizes situation awareness in IA command and control. We must provide the combatant commanders sufficient visibility into their network's threats and into their operations to gain full awareness of their situation at all times. This extends to other government and private sector partners as well. In addition, our international allies are closely aligned with us in this strategy.

We must be able to proactively defend our forces, both at home and globally. The growing sophistication of attacks makes speed of detection and response absolutely essential.

Goal four is focused on process improvements and research. We realize DOD is not an island. The net-centric warfare environment requires innovation.

We have published our IA hardest problems to challenge the research community to help us develop new capabilities. We are also challenging industry to be more responsible in the security of current commercial software products and are aggressively looking at ways to improve the overall software assurance area. DOD is actively enforcing security testing.

Lastly and most important is goal five, which focuses on creating an IA-empowered workforce that is trained, highly skilled, knowledgeable and aware of its role in assuring information. We are leveraging initiatives to create centers of academic excellence, now up to 50 universities and colleagues around the United States, as well as IA scholarships with the goal to improve our recruitment and retention.

Through efforts like these and our system and security administrative efforts, we are certifying our system administrators. And we are beginning to make significant progress overall in empowering our workforce.

The Federal Information Security Management Act of 2002, FISMA—as Bob was talking about—is the most influential statutory requirement for DOD with respect to IA. The policies and strategic plan I described for you are our tools to meet those responsibilities. And we take them very seriously.

In both 2001 and 2002 GISRA reports to Congress, Office of Management and Budget (OMB) mentioned that training and incident response areas, within the Department of Defense, we excel. And in fact, our Incident and Response Center is an integral part of the federal community's cyber warning network, set up soon after 9/11.

We have road maps. And we are working diligently to improve our system certification and accreditation practices and databases that will help us track those certifications. This is a very important priority of ours.

The challenges we face are similar to those found throughout the government and industry and with our allies. Size, global presence, dynamic technical and operational requirements all contribute to the complexity of our environment.

But we are adapting. We are making progress. We are managing the risk and are managing it successfully across all of our national security missions.

Most important, however, our progress is reflected in our ability to act as an enabler, not an impediment, in the conduct of net-centric operations in several theaters around the globe.

I appreciate the opportunity to appear before the subcommittee and look forward to your continued support and questions. Thank you.

[The prepared statement of Mr. Lentz can be found in the Appendix on page 43.]

Mr. SAXTON. Thank you very much for your statement. Mr. Charney.

STATEMENT OF SCOTT CHARNEY, CHIEF SECURITY STRATEGIST, MICROSOFT

Mr. CHARNEY. Chairman Saxton, Ranking Member Meehan and members of the subcommittee, thank you for the opportunity to appear here today. As Microsoft's chief security strategist, I oversee the development of strategies to implement our long-term trustworthy computing initiative, the objective of which is to create more secure software, services and infrastructures.

At Microsoft, we are deeply committed to cyber security. And we recognize our responsibility, as well as the responsibility of our industry, to make our products ever more secure.

It is for this reason that our trustworthy computing initiative is our top priority and involves every aspect of our company. The focus of trustworthy computing is on four key pillars: security, privacy, reliability and business integrity.

The security pillar is most relevant for today's hearing. Here, we work to create products and services for the Department of Defense and for all of our customers that are secure by design, secure by default and secure in deployment.

Secure by design means two things: writing more secure code and architecting more secure software and services. Secure by default means that computer software is secure out of the box, whether it is in a home environment or an IT department.

Secure in deployment means making it easier for consumers, commercial and government users and IT professionals to maintain the security of their systems. One thing is clear: no matter the investment, there will be vulnerabilities in complex software.

Last week one was discovered and patched for Windows Server 2003. While disappointing, all platforms—including Windows, Linux and Unix—will have vulnerabilities.

Today, however, Microsoft is making unprecedented efforts to create secure code. And we have also provided a state-of-the-art Security Response Center.

Notwithstanding the robust nature of our own efforts, we recognize that trustworthy computing and improved cyber security will not result from the efforts of any one company alone. As described in more detail in my written statement, we work with industry and government leaders to make security a reality for the entire industry.

We are also committed to working closely with DOD to support its information technology and research. For example, we are providing DOD with patch management solutions and developing tools to increase DOD's efficiency while properly controlling access to sensitive information.

Additionally, using commercial, off-the-shelf applications such as Microsoft Exchange and Outlook, we are supporting the Defense Messaging Service.

I would also like to spend just one moment talking about some of my experiences at the Justice Department. That experience suggests that the government generally, and DOD in particular, faces new challenges in cyber space.

The notion that only states have access to weapons of war is no longer correct, at least not if information warfare is considered. Simply put, we have distributed a technology that is far more powerful than most that have been placed in the public domain.

Although the Defense Department has traditionally focused on states of concern, it must now concern itself with terrorist groups and individuals of concern, a far larger pool and one that is harder to identify and police. Today, an attack upon DOD may come not only from a foreign nation or a terrorist group conducting information warfare, but also from juveniles on the West Coast, as it did in Solar Sunrise, the case name for a widespread attack against DOD that appeared initially to come from the Middle East.

To the extent the nation detects a cyber attack but does not know who is attacking—a juvenile, a criminal, a spy or a nation state or terrorist group bent on committing information warfare—the role of the Department of Defense may not be entirely clear.

In the face of this cyber security challenge, I want to outline a few specific areas where government policy can be particularly helpful in promoting cyber security within the government and throughout our infrastructures. First, the government can lead by example by securing its own system through the use of reasonable security practices, such as buying products evaluated and certified under the common criteria.

We applaud DOD's recent efforts to make clear that its security policies apply to all software, regardless of development and licensing models.

Second, we support additional federal funding for cyber security research and development. And it is equally important that the government maintains a traditional support for transferring the results of federally funded R&D under permissive licenses to the private sector.

Third, government has a critical role to play in facilitating information sharing. In short, the government must be an active provider, as well as an avid consumer of, valuable threat and vulnerability information.

In closing, Microsoft is committed to strengthening the security of our software and services and are equally committed to working with Congress, DOD, other government agencies and our industry peers on security issues, whether by offering our views on proposed regulatory or policy measures or participating in joint public and private security initiatives.

[The prepared statement of Mr. Charney can be found in the Appendix on page 89.]

Mr. SAXTON. Thank you each very much. We are going to go to Mr. Meehan first for questions. But at least let me make an observation, if I may, in thanking each of you for your opening statements. It is impossible to listen without being concerned because

of the challenges that you have each outlined in a slightly different way. So it looks like we have a big job ahead of us. And we want to be partners of DOD in helping to solve or bring into focus—clear focus—some of these issues that we need to deal with. And so we look forward to working with you. Mr. Meehan.

Mr. MEEHAN. Thank you, Mr. Chairman. Mr. Lentz—and actually, I would appreciate it if all the witnesses could comment on this question—it is my understanding that large portions of the commercial off-the-shelf software may actually be produced outside the United States. The media has reported that software production is moving offshore to India, due to cheaper labor costs.

How can we ensure that the software is not corrupted by unscrupulous persons or even, in some instances, our allies? And how can the Department of Defense create secure computing capabilities using this COTS software that may have been produced outside of the United States?

Mr. LENTZ. Thank you, sir. That is a very important priority of ours within the Department of Defense and, for that matter, throughout the entire community.

The President challenged us over a year ago to begin working in earnest to get a handle on that particular issue. We have a very aggressive series of working groups going on within the community as we speak, to identify a very definitive course of action on how to address that particular problem.

I will tell you that clearly one of the big gaps that needs to be filled immediately is the need to do more research in this area. We, I think, have to live with the reality that products and software are going to be designed overseas. That is the nature of the world we live in.

But I think by putting in investments in research and technology, we can develop the right tools and techniques to be able to allow us to inspect that software—we hope—in a way that we can have higher confidence in its implementation within DOD or within other infrastructures. But it is clearly a major concern of ours. And I will underscore that we have a series of working groups working throughout the community. And we are going to work with industry and the academic community in order to deal with it.

Mr. MEEHAN. Mr. Charney, I am interested——

Mr. CHARNEY. Yes, as a large software developer, I would like to address this question. And I might respectfully suggest that we might be asking the wrong question. And I say that because although most of our core components and our core products are developed in the United States, if you walked around the Redmond Campus, you would get quite an international flavor.

And at the same time, we have to remember that Timothy McVeigh and Aldridge James and Robert Hanssen were all Americans. And two of the three had security clearances.

I think the issue might not be where the code is developed, but rather the quality assurance techniques that are placed around the code. So one of the things you have to have is very rigorous processes in place to examine your code, test your code and have quality assurance built in, so that you know the code——

Mr. MEEHAN. Would you agree that it would be more difficult to do that with software made outside of the United States?

Mr. CHARNEY. It depends on the development process. Although most of our software is here, if you are getting components from overseas, for example, and actually reviewing, the vendors reviewing the quality of the component and testing the component, you will know what is in your code.

And the difficulty is, as well, that a lot of code developed in the United States is actually developed by foreigners who are residing here and doing software development. So it really comes back to quality assurance for the code.

Mr. SPAFFORD. I would echo Mr. Charney's comments that the location where the code is produced is not the only factor. It certainly has a great deal to do with the parties involved, their training, the tools available to them.

As an underline to this, it is really going to be, unfortunately, a question of cost and time. To get higher assurance of software may require that the U.S. government have a process for obtaining source code and running extra tests against that code or extra examinations.

That will undoubtedly cost more to acquire than simply buying it in bulk and shrink-wrapped packages. However, for mission-critical applications where we have to depend on that code, I think it is certainly important that we do so.

The current quality assurance methodologies that are being used allow literally hundreds of software flaws to slip past. So clearly, what we are doing now is not going to be sufficient.

Mr. DACEY. I would also echo the comments that it is certainly a challenge and it does need to be looked at. And certainly, GAO is working on a request right now from Congress to look at that in certain areas.

In terms of the process though, there needs to be a quality assurance process built in to provide some reasonable assurance that something has not gotten in there, whether it is intentional or unintentional, into that code. And the challenges of that are, if someone else is developing it, coming up with—I agree with Mr. Lentz—research and development.

It is very difficult right now to fully analyze the code. And I think some additional research would be certainly appropriate to try to find better ways to look at it for these kinds of problems.

Mr. MEEHAN. Let me ask each of the panelists again, is there any analysis of terrorist organizations' plans to grow cyber terrorism capabilities? In other words, are there terrorist training camps for computer geeks, designed to raise the skill level of cyber terrorists?

Is there any analysis or evidence that any of the panelists could present to the committee?

Mr. LENTZ. Well, I think probably that might be left for a classified discussion. I think we can provide you more details on that at a later time.

[The information referred to can found in the Appendix beginning on page 131.]

Mr. SPAFFORD. I will observe that there are bulletin boards and discussion lists where techniques are taught, where tools are available, so that anyone—and as Mr. Charney mentioned earlier, even juveniles spending a minimal amount of time online are able to

learn some very sophisticated attack methodologies, download those tools and modify them for their own use.

So we have, perhaps, a virtual worldwide training camp going on, on a regular basis, of individuals with various motivations using these tools and techniques, trying them out against our civilian and military infrastructures around the world.

Mr. MEEHAN. I will stop here.

Mr. SAXTON. Thank you. Dr. Spafford, help me with some terms. If we talk about a system or systems, can you just define for us what we are talking about when we use the term "system?"

Mr. SPAFFORD. That, sir, is a bit difficult because of the interdependence of communications and distributed processing that currently occurs. Sometimes, a system will be a stand-alone computer with memory and input-output devices.

Other times, a system requires the interoperation with other computers in other locations, such as a sensor network system or a communications system that requires processing nodes at different locations with wires between them. All of those as a system, however, behave at their heart as a processor that takes information in, manipulates it, puts it out and may have local storage. And that is about as close as I can come, sir.

Mr. SAXTON. Right. Mr. Lentz, DOD systems have grown up in a, I guess I would call it, appear to have grown up in a kind of a fragmented way. None of the services has a system, a single system, from what we have been able to understand. And the systems have grown up as, I guess the term we use around this institution is a stovepipe effect.

And we know that is true because now, for the first, the Navy and Marine Corps are trying to develop the Navy-Marine Corps Information System. And that is hard to do because of the fragmented nature of the way we develop the system. Do we know how many systems, following the definition of Dr. Spafford, we have in DOD?

Mr. LENTZ. Yeah, I agree with the doctor. It is a very difficult question to answer because you have so many different ways to look at it.

You have local systems that could be on an Air Force base, isolated in one department versus integrated networks that tie multiple systems together. It is an extremely hard question to answer. But I do believe——

Mr. SAXTON. It is hard just to define the term "system," is it not?

Mr. LENTZ. It is.

Mr. SAXTON. To know what a system is? If it is hard to define the term system and we have all these interrelated, sometimes independent, sometimes systems, how do we secure them? If we cannot get our arms around what the system is and where they are and how many we have, how do we secure them?

Mr. LENTZ. Well, I think the one way that we are addressing that within DOD is we most recently put out a DOD IA policy. In fact, it is our capstone policy for information assurance. It was put out in October of last year.

We identify a number of parameters. And it really comes down to providing what we call designated approval authorities, or DAAs, who are responsible for identifying those systems or net-

works that they believe they are responsible for within their area of responsibility.

And in working with their CIOs, they then will put together the right template of areas of responsibility. And through that process, we are enforcing certain security controls that they will have to make the risk management decisions on.

So we are following this new IA policy. And it has been our top priority, over the past couple of years, to get this policy out.

And we are very pleased that it is out on the streets. And that is going to be the mechanism we are going to use to bring all these pieces together to provide the right governance for the overall network.

Mr. SAXTON. Mr. Dacey, is this a problem?

Mr. DACEY. I think one of the challenges is trying to figure out how you put this group of systems together. Some of the discussions we have had here on interconnectivity are probably the most challenging because even if you define systems across any agency, there is likely to be interconnectivity that you have to consider.

So in looking at security, one of the ways in which FISMA is addressing some of those challenges is to require the development of different risk levels and minimum standards for each of those risk levels. And given that, if we have a process where we can at least identify what the risk level of that system is, which would include all the relevant data and processing capabilities, then you can better understand connectivity.

And you do not want to have situations where you have a high-risk system attached to a low-risk system and not have good controls between those two. So I think that will be a key effort.

I would note that the Department of Defense, in their policy, actually has already developed a structure of risk levels, as well as connectivity agreements, on how those systems can be connected in a process. So that gets to be the key, is really identifying what is the sensitivity or risk in these systems and making sure that we are protecting the boundaries and the interconnectivity of those systems with others. And I think that is going to be the challenge for the federal government as a whole.

Mr. SAXTON. Mr. Lentz, have we identified all the systems?

Mr. LENTZ. It goes back to what I said. We are in the process, following the policy that Mr. Dacey talked about, which we are very proud of because it is providing that template.

We have three areas we call mission-critical, mission support and administrative. And in regards to Dr. Spafford's area, that might be the template in how to overlay software assurance at some point in time, in terms of focusing on maybe those three areas.

But the policy lays that out. And that will provide us the road map in order to be able to pull together, using these designated approval authorities with the CIOs, what is going to be the overall way we are managing the network.

Mr. SAXTON. Thank you. Mr. Charney, is this an issue that is of concern in the private sector?

Mr. CHARNEY. Oh, absolutely. I mean, one of the difficulties is getting your arms around the problem. And what most people focus on is people, process and technology.

And this is an oversimplification. But if you think about the highway system, for example, you have a lot of different entities that build roads.

You have a lot of different entities that test drivers. You have a lot of different entities that make sure that cars meet certain standards.

But at the end of the day, when you think about people, you want drivers to be trained on how to use the cars effectively. You want processes in place, like rules of the road, that everyone adheres to. And you want technology that is safe.

And in some respects, that applies to this too. You want users to be trained on how to use the technology safely. You want IT administrators to know how to secure their systems.

You want processes in place, which means you want accountability for who is responsible for security. You want a documented information security program.

And then you want to buy good technology that enables those people and processes. And you actually have to take each piece and then make sure that each one is done well.

Mr. SAXTON. Thank you.

Mr. Dacey, where do you think we are, in terms of meeting the goals that need to be met by DOD, with regard to the general subject of cyber security?

Mr. DACEY. I think in an overall analysis, I would look at the work that is being done for their FISMA reporting. I think on the positive side, there has been an acknowledgement of what the challenges are. There has also been a lot of work that is being done to implement a security framework, which we have recommended in our prior report.

So there is certainly quite a bit of effort taking place there. At the same time, there are a number of challenges, which I think DOD has acknowledged in their reporting and is setting out this strategy and currently developing a more detailed plan, I believe, and guidelines and goals, timeframes, if you will.

So I think those are going to be important to continue to look at in the process. At the same time, I would like to acknowledge that DOD has been, given its challenges, DOD has been at the forefront of many information security initiatives in the federal government.

We have been doing work there over a number of years. And certainly, they started doing red team testing, which is actively trying to break into systems, in the early to mid-1990s, before most agencies had thought about it.

They had also developed a process, at least within the Defense Information Systems Agency (DISA), to set standards and measure those standards from management, not from the auditor, but management doing that. So there have been a number of efforts underway that have really been at the forefront.

At the same time, the whole government is challenged, as we reported, with security issues.

Mr. SAXTON. Thank you very much.

We are going to move to Mr. Larsen now. We are also going to move to use the five-minute rule at this point. There is obviously a lot of interest and many members here to ask questions.

So Mr. Larsen, if you would like to begin?

Mr. LARSEN OF WASHINGTON. Thank you, Mr. Chairman. I want to thank you for calling this hearing as well. And given the five-minute rule, I will be hanging around for another five minutes.

Mr. SAXTON. Let me thank you for advocating for this hearing. This was a great idea. Thank you.

Mr. LARSEN OF WASHINGTON. Appreciate that very much.

First set of questions is for Mr. Lentz. And for the panel, I appreciate all of you taking time to come and help us understand cyber security at the Department of Defense.

Earlier this year, as Mr. Meehan mentioned, Mr. Lentz, the full committee—and this is the subcommittee and the full committee—proposed and passed a cut of $2 billion out of a $28 billion DOD IT budget, on the authorizing side. And that got me thinking about what does that mean for security?

But it also got me thinking about what that may mean for security? There was a Frontline documentary entitled, "Cyber Wars" that ran earlier this year. And I forced some of the committee staff to sit in my office and watch a portion of it on my computer screen to sort of bring these issues out about security.

Given the cuts that we proposed on the authorizing side and some of the concerns that were brought out through this Frontline documentary, I want to talk about what that might mean—these cuts might mean—for security. Can you just briefly though start by giving me your view, your own description, of what the DOD IT programs play in creating our current joint warfighting capability?

Mr. LENTZ. Well clearly, as I said in my opening remarks, IT and IA go hand in hand. You cannot have one without the other.

When I go and visit the combatant commanders and I see the combatant commanders using very aged computer systems in order to operate their systems, it is very troubling. Because you cannot overlay information assurance on an old age technology.

I talked earlier about public key infrastructure; that is, the common access card that all DOD employees are going to have very shortly. You cannot, as an example, allow a Public Key Infrastructure (PKI) system to be deployed on a Windows 95 system. And there are lots—still—of Windows 95 systems, IT systems out there. It just will not work effectively.

So as a result, you need IT modernization to be able to do that. And as the chairman was talking about, as you have legacy systems out there, the sooner you get rid of those legacy systems and move to more modern systems.

As an example, our net-centric enterprise server. It is a very, very essential program. It is the hub of how we are going to move information throughout the department to allow the warfighters to be able to pull information wherever they are going to be around the world. And we know in this global war on terrorism, that is going to be the name of the game.

And you have to have a modern IT infrastructure at the applications level to be able to allow the users to pull that information. That gives us things like configuration management. It gives us new ways to put patches—as was mentioned by Mr. Charney—down to the lowest echelons of the field. It allows you to manage it to client level. That is all part of IT modernization.

Mr. LARSEN OF WASHINGTON. I could not agree with you more.

I want to move forward to one of the questions that emerged from watching this particular documentary. And it has to do with one exercise that was done in 1997-1998 in the Department of Defense called Eligible Receiver. And the results of that were published widely in the public domain.

And also Moonlight Maze, which was not a DOD exercise, you are probably aware. I was wondering though, Eligible Receiver and Moonlight Maze got me thinking, if we implanted these cuts, how might those cuts erode in key Pentagon capabilities to ensure that there are adequate firewalls or to draw down our ability to keep pace in the future with hackers? If we are making across-the-board cuts in DOD IT programs, at what point does that begin eroding our ability to put in the security to prevent things like Eligible Receiver or a future Moonlight Maze?

Mr. LENTZ. Well, clearly, what Eligible Receiver did—and Eligible Receiver was one of the red teams that Mr. Dacey was talking about—and what it does, it attacks the weakest point in any network. And once it goes inside the network, it is the soft underbelly.

And as Dr. Spafford said, the inside problem is probably our greatest problem. But when an outside entity gets in, it can wreak havoc within your network, without a strong IT fabric providing defense in-depth mechanisms to be able to stop and deter an adversary, either coming from the outside or from the inside and also to monitor those activities. And that is one of the keys, to monitor activities, to monitor behavior on the network.

The Eligible Receivers of the world, the red teams, are going to be able to have their day every single time they launch themselves. And that translates to the adversaries.

Mr. LARSEN OF WASHINGTON. Thank you.

Mr. Chairman, at some point, I would like to come back for another set of questions. Thank you.

Mr. SAXTON. Mr. Kline?

Mr. KLINE. Thank you, Mr. Chairman. Thank you all for coming today. I want to follow up a little bit on what the chairman was discussing earlier about the Navy-Marine Internet, for example.

As the department is moving to put everybody on the same page, I am wondering if that makes it harder or easier for people to get into the system?

Mr. LENTZ. From my vantage point, I think, by having positive configuration control at all layers, I think that only makes it more difficult because it synchronizes all your efforts.

I often like to use the analogy of I coach little kids on a soccer field. The best way to learn to win on a soccer field is everybody is in their positions and knowing what to do.

And that is what you do with things like Navy-Marine Corps Internet (NMCI). It has strong configuration management, a system view of that, tying all the pieces together.

And that is the best way to be able to defend your networks.

Mr. KLINE. I guess the weakness that seems to occur, sort of intuitively, is if there is only one system, only one Internet, and you get into it, you have hit everybody; whereas, if you have the sort of hodgepodge system we have now, you would not hit everybody at the same time. Is that not so?

Mr. LENTZ. Well, I know Dr. Spafford has written quite a bit on the idea of the differences between a homogeneous system versus the other side. I think there needs to be a mix of both.

I think you have to use both techniques in defending your network. That is why you have to modernize at all times, if you know what I mean. I think it does not do you any good to really have chaos on your network if you want to plan to defend it.

Mr. KLINE. Okay. Assuming that you had a common Internet like the Navy-Marine Corps Internet, how do you address the proliferation of sort of individual systems; that is, that there is a system, an Internet, but each individual sailor or Marine now is running around with his own laptop and his own BlackBerry and his own cell phone and so forth. Is that just a matter of discipline and keeping people from using those?

Or would it be impossible then for individual systems to access that Internet because of its own protections?

Mr. LENTZ. Well, first of all, it is something that FISMA advocates and one that we are taking very seriously, which is strong policy controls and enforcement in governance. That is what it really is all about.

Mr. KLINE. Okay. Thank you. I yield back.

Mr. SAXTON. Mr. Thornberry?

Mr. THORNBERRY. Thank you, Mr. Chairman. Let me thank you for having this hearing.

Over the past several weeks, in Homeland Security, we have had three hearings on cyber security. And one of the things that comes across and one of the reasons it is challenging is because it is a national security, a homeland security, as well as a legal and economic issue and that it is hard to know what level you are dealing with.

So I guess I would like to ask Dr. Spafford first to just comment briefly, if you will, on cyber terrorism as a national security concern, not an economic security, not stealing a bunch of credit card numbers, not slowing down email necessarily. Help us get a perspective on why the Armed Services Committee ought to be concerned about that.

In addition, of course, to interfering with the DOD's ability to conduct warfighting, beyond that, as cyber terrorism, why should we worry about this?

Mr. SPAFFORD. Well, sir, one of the goals of terrorists certainly is to disrupt, to spread confusion, to spread terror. And a way to do that is, in conjunction with a physical event, would be to disable communications to disrupt processing to reduce the responsiveness of agencies to provide aid; those agencies being civilian, as well as some of the military—the National Guard in a state level, for instance, or the military in something of a wide scale nature.

When they construct cyber threats, these may be untargeted. They can be network, self-propagating kinds of viruses or worms that, because we have a shared kind of architecture, we have shared networks, those would spread not only to civilian infrastructure, first responders, but also into the military systems. Causing that disruption, using them as platforms and amplifiers, would further disrupt those systems and add to their overall goals.

Mr. THORNBERRY. Thank you.

Mr. Lentz, it is estimated that something like 90 percent of DOD communications go through public backbone or public systems? I would like to know pretty specifically what communication interaction are you having now with the Department of Homeland Security about trying to protect those systems and about making sure that your reliance upon them is protected?

Mr. LENTZ. Well, we have and we will continue to have a very, very strong relationship with organizations like the National Communications System that was previously led by DISA that is now in Homeland Security. We have a tremendous working relationship with the National Infrastructure Protection Center (NIPC), which was formerly in the FBI.

And worked also very closely with Federal Computer Emergency Response Team (FedCERT) at the federal level. So we have and will continue to have a very strong relationship with those entities. In fact, we have put military personnel, as an example, in the NIPC.

Mr. THORNBERRY. But do you have daily contact now with the Department of Homeland Security?

Mr. LENTZ. Yes, we do. We work with a number of members of the department.

Mr. THORNBERRY. Do you talk to them at all about the research? Several times it has come up already, about research into various areas. How is that coordinated? Or are you coordinating at all, the Department of Defense with the Department of Homeland Security? And I realize that is not completely your bailiwick, but——

Mr. LENTZ. I have had some discussions with them on research objectives. I have not had and my staff has not had specific dealings with them on the research topics.

But clearly, that is something we have said amongst ourselves, because the national cyber strategy calls it out, as something that we have to collaborate on as they become more organized and be able to deal with these issues.

Mr. THORNBERRY. Mr. Chairman, I have a number of other questions that I would like to submit for the record.

But finally, I would like to invite Dr. Spafford and also Mr. Charney to comment on Mr. Kline's question. Because I think maybe Dr. Spafford has a slightly different perspective.

But Mr. Charney, you have to worry about this too. If Microsoft has the position it has, does that not make us more vulnerable? Because if you break into Microsoft, then you are into all sorts of things. And so, I think it is a good question that I would appreciate a little additional perspectives on.

Mr. CHARNEY. I would say that actually reasonable minds are debating whether a homogenous environment or a heterogeneous environment is better and increases or decreases risk. And to be frank, I think there are arguments on both sides.

The advantage of a homogeneous environment or more of a monoculture is that it is much easier to manage. You train your people on a particular system.

And they manage that system. They know all the security settings. They can run tools to make sure they have locked it down. When you run a lot of different software in the same environment,

you need different expertise. And sometimes, connecting those different systems raises its own vulnerability.

The flip side is when you have a monoculture, you worry about the risk that if there is an event that affects a particular product, it will have a broader impact. And then the flip side about that is, if that is true and the software vendor is actually very responsive in providing security, then a single patch may take care of the problem. So I think at the end of the day, there are both pluses and minuses. And it is really a question of risk management.

Mr. SPAFFORD. I would basically echo that there are advantages to having a common platform. The situation here, however, is giving network access, giving computing access to as many individuals as we do, including not only our enlisted personnel, but our contractors and others, perhaps family members of some of the military, in the cases of communicating with their loved ones remotely, is in effect the equivalent to giving an automatic weapon to each one of those individuals without them even knowing that it is an automatic weapon.

They do not have the training. They do not have the background. The safety is not in place. And as a result, any one of them becomes a potential launching point for a problem. If everybody is using the same platform, that problem has a farther reach.

So until we get to the point where we have the appropriate training, we have the appropriate safeguards in place for every one of those individuals and the reach of what they do is limited, it is perhaps better to have some partitions in place—some internal firewalls, if you will—that may be also brought about not simply by logical means, but by different vendors and different platforms so that we do not have a wide-ranging incident.

Mr. SAXTON. Thank you very much for those great questions.

Mr. Akin.

Mr. AKIN. Thank you, Mr. Chairman. I do not know if you can answer my question.

I do recall a hearing, I think it was probably 3 years ago or so, about the fact that one of the most supposedly internally secure of our government databases or files was rummaged through. Somebody had accessed it. And we found out 6 months later, or something like that, that it had been reviewed.

And they had come and gone. And we had not been aware of it for some time.

Is there some truth to that? Or is that one of those things that was not supposed to have leaked out?

Mr. LENTZ. Yeah, I am not particularly aware of the details of that particular topic to be able to answer at this point in time. I am sorry.

Mr. AKIN. I do not remember the details. Thank you.

Mr. SAXTON. Mr. Rodriguez?

Mr. RODRIGUEZ. Thank you, Mr. Chairman. I want to thank you also for holding this particular hearing on cyber terrorism.

And I live in San Antonio. And I have the pleasure of also having the Air Intelligence Agency there. And we also have the Center for Infrastructure Assurance and Security there at UT at San Antonio.

I am also pleased that we have the Dark Screen project going on. And maybe later on, we can get a little feedback on what is hap-

pening with the Dark Screen exercise in San Antonio that has been occurring.

But I wanted to also share with you that in the process of going through that Dark Screen that has been going on for about a year, that there has been some real needs that have come up. And one of those has been in terms of looking at how both the private and the public sector—and this goes for Microsoft and the others to maybe provide feedback—there is a real need to see how we can dialogue and communicate.

No on is willing to share. We have the Federal Bureau of Investigations (FBI) participating, the Central Intelligence Agency (CIA). We have the local government and the mayor, the county government, the state. We have the private sector, some of the banks.

And maybe you can also give me some feedback on some current laws that we need to look at for sharing, both from private to public, as to how. And we are even having difficulty within the utility companies and the water systems and those kind of things, in terms of that sharing. So I wanted to get some feedback, both from the private sector and maybe from DOD, on those things, especially as it relates to current law that we might have to look at, that we might have to look at changing some of those things.

Mr. CHARNEY. Yes. So I believe everyone in government and industry agrees that information sharing, especially about threats and vulnerabilities, is critical. Historically, information sharing has not been very good. And there is a host of both cultural and legal reasons for that. From a cultural perspective, governments are used to holding information closely because of its sensitivity.

And on the industry side, the same can be said. They hold a lot of information closely because sometimes exposing information has business risk, especially vulnerability information. If you disclose vulnerability information without having a patch in place, you really run the risk that your customers will be injured, as opposed to helped.

And then there are also legal aspects to information sharing. The concern for industry was that if we shared information with the government, it might be released pursuant to a Freedom of Information Act (FOIA) request and be put in the public domain.

Some of that has been resolved, of course, by exemptions to the FOIA for information that industry voluntarily provides to the government in this regard. There are some who want to roll back or repeal those exemptions. We think they are very important. And they open up a possibility of greater information sharing.

The other thing I would say is that historically information sharing has occurred when the individuals on both sides—the government and industry person—trusted each other and had a relationship. And what industry and government have been working hard to do, through information sharing and analysis centers and other industry and industry-government groups, is to basically institutionalize the trust; that is, come up with protocols and methods for sharing information that are institutional in nature, so they are not dependent on the personal relationships of the industry and government member.

And some of those efforts are just starting to bear fruit. And it is important that we, of course, continue to protect this information so that we can share it more freely.

Mr. RODRIGUEZ. I was wondering maybe if DOD, because I know with Dark Screen, we have had a little difficulty in terms of that sharing and that dialogue and in terms of gathering the information that is needed.

Mr. LENTZ. Yeah, I am not aware of any difficulties in that area. I know our position has been that we do not believe that additional legislation is needed in this area. We are quite satisfied with the current state in that regard.

Mr. RODRIGUEZ. Can I ask you specifically? For example, we know and we anticipate that if we have problems, one of the first things of any major attack is going to be through cyber.

And sometimes, that will come in the private sector, which you might not have any idea that it is coming down. How do we get access to that? And that has been one of the difficulties.

If they hit, if the intent of a terrorist is to hit the private sector, DOD will be the last one to know if that is the case, unless there is some dialogue going on.

Mr. LENTZ. Well, I think that is an excellent question. And in fact, I often will say that a great deal of the events that have affected DOD or the nation at large has actually been detected by the private sector.

And they in fact have notified DOD very quickly upon their detection of those events. And they have helped us analyze those events cooperatively. There has not been any impediment for that sharing of information.

Mr. RODRIGUEZ. You said there had been no impediment?

Mr. LENTZ. That is correct.

Mr. RODRIGUEZ. Because I know it is a concern that the private sector has when they start having difficulties. And I will make the analogy, because I sit on a higher education board, it is difficult to get the universities to report how many rapes they have had on their own campuses.

And so I know how difficult it is for a company to report how many intrusions they have had or how many difficulties that they had and when they have come. And so the timing is critical. And that is important.

I do not know if the GAO wants to make a comment on that. But I think that that is one of the areas that we really need to make some inroads.

Would you want to comment?

Mr. DACEY. I just wanted to echo what Mr. Charney said. We have done a fair amount of work on information sharing and issued several products which lay out some of the issues. Mr. Charney summarized most of those issues.

But the other part of that, I guess, is there has been some action—a lot of action—both by agencies, by the private sector and certain provisions of the Homeland Security Act, including a whole section on Information Sharing Act, which is designed to help facilitate the communication of information out to the private sector and sharing information.

I believe the act calls for reporting by November by the Department of Homeland Security on their plans for doing that. So I think, hopefully soon, we will be seeing some more concrete plans by the Homeland Security Department.

But they have assumed responsibility for coordinating efforts with the private sector and the federal government on cyber and physical threats.

Mr. RODRIGUEZ. Mr. Chairman, I apologize for going over.

Mr. SAXTON. Thank you very much, Mr. Rodriguez.

Mr. Bartlett.

Mr. BARTLETT. Thank you very much. As a consequence of 9/11, all of our government agencies and I suspect most of our private sector entities now have a Continuation of Operation Plan; that is a COOP plan.

If your main facility is gone as a result of a terrorist act, these COOP plans assure that you will be able to continue your operation. I want to use that as an analogy for the cyber concern that we have this morning.

If the main facility of the FBI, for instance, is analogous to our computer system, I am concerned if it is possible to have the equivalent of a COOP plan. It seems to me that all we are doing now relative to this asset and the fact that we just cannot do without it is the equivalent of putting more guards around the facility, making the fence higher, having a better system to put out the fires more quickly after the event occurs. Is it possible to have the equivalent of a COOP plan? Or are we just through if our computers and that system do not work?

It appears to me that if it were possible to have a COOP plan where we could make do in the event that we could not expel the intruder and reconstitute the system, that we ought to be doing it. I do not know if that is even doable.

Have we come to the point where, without computers, we just cannot?

Mr. LENTZ. I guess the one comment I would say is that as part of our certification and accreditation process that we have within DOD—and I believe it is the same with the national level process—when you do a certification and accreditation, one of the things you have to lay out is COOP issues, continuity of operation, reconstitution of your resources.

So from a cyber standpoint, we view that as a very critical element of any certification and accreditation of a network.

Mr. BARTLETT. So is that just starting up another capability at another site? The presumption here, I think, is that an intruder could just simply take down our system. If the system is taken down, you cannot reconstitute the system.

Is there a way of doing what we are now doing without the computers? Or are we just through if we do not have the computers? Is this the Achilles heel? Is this an insult for which we have no response?

Mr. CHARNEY. I guess what I would say is certainly computers and networks today are a critical asset. And there are a lot of other critical assets that, you know, if you think what would happen if the water supply went away or the power supply went away.

These networks are critical in that regard. But having said that, there is a lot of resiliency and redundancy built into the network. And when the networks have been broadly affected, they have been reconstituted fairly quickly. And so yes, we are heavily reliant on them. If they went away, it would be really hard to live our lives as we are used to. And that is why we need to protect them and build in appropriate redundancy and resiliency.

Mr. BARTLETT. Is anybody looking at what we would do if they went away and were not coming back?

Mr. CHARNEY. I think the answer to that, in terms of having a disaster relief plan that says there are no computers in the world, I would be surprised if anyone is planning for that contingency. I would say probably not.

Mr. DACEY. I would just like to add the point that I think that continuity of operations is a critical element of information security. Obviously, you need to secure your networks and systems to the extent you can. But in the event of something happening, you need to be prepared not only to have the plan, but to test it.

In terms of our analysis of the federal agencies as a whole, that is probably one of the most critical issues is the lack of testing of these plans—if they exist—to see if they work. So I think that is important. And I think those plans need to consider the criticality of those systems.

I think it would be hard to imagine a lot of functions happening without those systems in place, particularly with the high volume transactions and real-time nature of many of our commerce and the things we do. So I think we need to plan to have that capability to come back.

And that can be done in different ways. That can be done through a very sophisticated process of concurrent processing so that if one site goes down, the other immediately takes over.

But that gets into assessing the sensitivity and criticality of those systems. And your plan needs to take that into consideration. So if you have a highly critical system that you really need to have, you better be putting in extremely strong procedures to come back, not only of the system, but the people that operate and maintain the system are as important as well.

Mr. BARTLETT. That is a bit like putting out the fire quickly. But it is not really a COOP. So I wonder if the professor has an observation on this, if you had looked at that, sir.

Mr. SPAFFORD. Very quickly, sir. Taking out all of the computers would be a very difficult thing to do. However, there are key points where there are potential threats. They may not be very large at the moment.

For instance, I believe Mr. Kline noted that we have 90 percent or so of our communications traffic going through commercial networks. If a number of communications satellites or major links were taken down, that would be very disruptive of our systems. I am not sure how well we would be able to recover full capacity as a result of that.

And then to follow up on Mr. Dacey's remark, we have not really tested many of these things. Our systems and interconnections are so complex that there are emergent effects that we have not anticipated and cannot anticipate until potentially they occur. So I do

hope that there is considerable planning going into redundant systems. But we may not know until an incident actually occurs.

Mr. BARTLETT. Thank you, Mr. Chairman.

Mr. SAXTON. Thank you.

We are going to go to Mr. Meehan and then back to Mr. Wilson.

Mr. MEEHAN. I think I will submit my question for the record in the interest of time. I know Mr. Larsen has some questions as well. But I just want to comment, this has been an excellent panel. The information has been very, very good. Thank you.

Mr. SAXTON. Great staff work.

Mr. Wilson.

Mr. WILSON. Thank you, Mr. Chairman. And thank you all for coming today. I apologize that I was late.

But what you are doing is so important in working together. This is very interesting. And I appreciate what you have done to protect our country.

A question that I have is: is there an analysis of terrorist organizations' plans to grow their cyber terrorism capabilities? And for all of you, does anyone know if there are any terrorist training camps for computer experts, designed to raise the skill of cyber terrorists?

Mr. LENTZ. I think earlier we talked a little bit about that. And we can provide you classified information later on for the record on that particular issue if you would like.

Mr. SPAFFORD. I will reiterate the comment I made earlier that there is a great deal of information in the public domain on the networks, even in the bookstores, that anyone can become a terrorist effectively, similar to downloading plans on how to make a fertilizer explosive. They can do the same thing in cyber offense.

Mr. DACEY. I would also reiterate the same comments. If someone were really intent on doing it, it would not take them a great deal of effort to become fairly knowledgeable and to be able to use fairly sophisticated tools—but easy to use tools—to launch attacks.

Mr. CHARNEY. I think we have to assume that, as people become more computer literate, including our adversaries and terrorist groups, they will be more prone to use this technology since it has global reach. And it is very hard to trace back events to their source.

So there are a lot of reasons this could be a medium of choice for those kinds of attacks. And we have to prepare for it.

Mr. WILSON. In taking into account what Dr. Spafford said about public domain, could you share with me your perspectives about the "Introduction to Hacking" sites on the Internet, which list known vulnerabilities in computing and communications systems. And in particular, who would post that? And for what purpose?

Mr. SPAFFORD. Well, there are a number of different motivations that have been expressed. And talking to some of the individuals, I believe they are sincere.

There are some individuals who believe that this is the only way to get vendors to respond to fixing those problems. And historically, that was true. I am not sure that is the case now. I know some companies such as Microsoft are very, very aggressive about fixing problems when they are reported.

A second motivation, some claim, is to make others empowered so that they can check their own systems that may be different, to

see if those problems occur in their different configuration. A third motivation is to make it available for study by researchers or hobbyists.

And then there are the anarchists who simply wish to cause disruption, those who wish to embarrass or inconvenience particular companies, those who hope that it is used as a background for political activity. And it may be the case that there are some elements who are introducing these to create background noise so that they can use that as a cover for targeted attacks against industry or government.

Mr. WILSON. And finally, is there a relationship between cyber terrorists and physical attacks? Do any of you have any knowledge of synchronized acts of terrorism? And is there a correlation between these acts?

Mr. LENTZ. I am not aware of any specific examples that I could cite at this point in time in that regard.

Mr. SPAFFORD. The potential certainly exists.

Mr. DACEY. Yeah, I think there is a significant potential for those combined attacks. And in that case, it is possible to either use cyber to do some damage or to use cyber to actually delay or interfere with the response of the appropriate people to that particular physical event.

Mr. WILSON. And I think you indicated correctly too, that possibly cover prior to or simultaneously as to acts occurring. But thank you all again for being here today. I yield the balance of my time.

Mr. SAXTON. Professor Spafford, you seem to be quite good at putting technical subjects and language into language that we can understand as laymen. So let me ask you a question that has been talked about by staff here at some length.

It is our understanding that the official request for comment for the future Internet network layer protocol has proposed some security and quality of service features. Could you give us your perspective on this subject?

Mr. SPAFFORD. The Internet protocols are constantly evolving. The protocol right now that is at the heart of much of our network communication was written at a time when there were only a few thousand machines on the network. It has served admirably in that regard. But the environment has changed. Now worldwide network with millions of hosts.

The next evolution of this protocol includes capabilities for making it possible to add security to communications. It is not a requirement. It is simply an addition. There are some extra bits in place. There is some extra capability.

However, that is not backwards-compatible with existing equipment. And as Mr. Lentz noted that we would have to replace a large number of machines in government use, in commercial use, to take advantage of those capabilities.

So it is a very valuable step forward. And it probably is not going to be the last protocol that is suggested because as we grow, perhaps we will end up with interplanetary networks that will require yet another addition. That might be nice to think about, perhaps.

But we have to make sure that all of our underlying software and hardware is compatible with that to take advantage of it. And

that is actually the biggest step to move in that direction is all of the legacy hardware that we have out there.

Mr. SAXTON. Can you comment on Internet Protocol version 6 (IPv6) in terms of quality of service?

Mr. SPAFFORD. It has extra features to provide some quality of service, to ensure that we have end-to-end Parallel Access Volumes (PAVs) with enough capacity to move messages along, to increase their priority. But that has to be respected at all steps along the way.

Because of the way we route messages, it is based on good faith of the behavior of the processors along the way. And if we have network nodes that are being operated by individuals who do not wish to adhere to that—it is not a requirement, it is a request—then they are not a firm guarantee. Does that answer your question?

Mr. SAXTON. Others like to comment?

Mr. LENTZ. I guess two points. And Mr. Stenbit, our CIO, you probably are aware, just recently put out a policy regarding IPv6. And I think that was a very visionary step in his direction that recognizes the importance of that protocol.

And he said by 2008, we are going to be involved in implementing fully that particular protocol. So I think that has put the department on a firm direction in working with industry and the academic community to deal with those issues.

And clearly, there are a number of information assurance advantages by moving to IPv6.

Mr. CHARNEY. I can certainly say Microsoft has been supporting IPv6. But as Dr. Spafford notes, because it is essentially changing the language of the Internet, it requires everyone to convert.

And although in the interim you try and build some backwards compatibility through translation essentially between two languages, that poses its own problems. But we are strongly supportive of it. And as Dr. Spafford noted, when the current Internet protocols were adopted, security was not the primary focus.

Mr. SAXTON. Thank you very much.

Mr. Larsen.

Mr. LARSEN OF WASHINGTON. Thank you, Mr. Chairman.

I cannot help but think, in listening to the panel today and listening to the discussion about the need to replace legacy systems and upgrade systems to have secure, upgraded systems to help the joint warfighter, to have security investments to prevent any draw down of our ability to protect the DOD IT systems, that the cuts that we authorized in the DOD IT budgets, we could have benefited from this discussion earlier this year. And I would hope that as we move forward into next year, that we remember this panel today as we move forward into the authorizing exercise next year. Because I think it is the security of the DOD systems, to the joint warfighter, to the building itself and to everything that is taking place in the Pentagon building and around the world, we need to keep what we are hearing today in our minds as we move forward on that budget exercise next year.

I want to ask Mr. Charney a few questions. And this gets into the heterogeneity and homogeneity discussion a little bit.

Your response was quality assurance (QA). The answer to developing code is to make sure that you have a QA system involved as

you are moving through this. But it occurred to me that your response might be more of certainly a private sector response, as opposed to considering the specific needs, say, of a defense system and mission-critical functions. So can you help me out a little bit in thinking through how you develop a quality assurance system that looks specifically for things that an Armed Services Committee or the Pentagon might be looking for? What is in that code to prevent the kinds of problems that would be more detrimental than not for our joint warfighter and our ability to communicate?

Mr. CHARNEY. Sure. So the Defense Department, in addition to using commercial, off-the-shelf products, also uses proprietary code that they specifically hired to be built. And for the companies that develop code, there are certain things that we found that you need to do to make sure that that code is secure.

The first thing is you have to give your developers training on writing secure code because most programmers historically have been taught to write functional code. And when Microsoft started training its 8,500 developers in Windows Server 2003, we took our learnings and actually published it in a book. It is publicly available because we want to share those learnings.

The next thing is someone is going to write the code. And there should always be a quality code review process, where other people review the code of the first programmer. There is a couple of reasons for that. One is the obvious one that you want to look for mistakes and do an extensive code review.

But not unlike having two tellers count the money at a bank ATM machine, having business controls in place make it harder for someone to put improper, unauthorized code in the code base.

The next thing we found was effective is what we call threat modeling, which is where you figure out how someone would attack your code because knowing how the attack may occur gives you an idea of where you need to batten down the hatches and better secure your code.

And then the third thing in the code assurance area is penetration testing; basically, having people attack your code as if they were hackers. We actually do that on three different levels. Each product group does penetration testing. That is good because they know their product. It is also bad because they know their product. And they may not think outside the box.

The second thing is when a group responsible for delivering the code is testing the code, if they see a problem, it creates a natural business tension between delivery and non-delivery. So we have a second group of penetration testers who work for me. I am a cost center. I report to the chief technical officer, who reports to Bill Gates.

And then we have a third, we bring outside pen-testers in from private companies. In addition to all of that security, you also need business controls in place for the code itself. So when developers create code, they need to sign the code, digitally sign it. And it has to basically keep chain of custody over the code in every step from development to production.

This does a couple of things. One is if there is a problem with the code, you can figure out where the problem was introduced. It creates a general deterrence. It allows the code to be quickly identi-

fied if there is a problem. So it is really a question of building good code and then putting business controls over the process so you can ensure its integrity.

Mr. LARSEN OF WASHINGTON. Did the staff get all that? I think it is important that you run through that because the question I want to ask Mr. Lentz has to do with one of the GAO's conclusions about, a lot of advancements have been accomplished in IA within DOD. But there is still a few gaps, including regular testing, as opposed to some of the pilot testing that is taking place.

I was wondering, Mr. Lentz, if you used what Charney said as a benchmark, how close are we? And what do you need from us to help you get to implementing the plan that you talked about earlier that you have in place? What do you need from us to help you then moving forward to implement your plan?

Mr. LENTZ. First of all, I would like to compliment Microsoft for their initiative. I think it is a very solid way to address that particular problem. One of the things that DOD did—and it was started at the national level—is we created a formal process using the international common criteria that has been discussed already in order to test products.

There is not an IA or IA-enabled product that is going to be installed in the DOD network today that has not gone through that process. And through the certification and accreditation process, if a product is found to not be compliant with that policy, that system will not be certified. So that is our first step in that regard. And it is our most significant step.

Mr. SAXTON. Mr. Bartlett.

Mr. BARTLETT. Thank you very much.

Mr. Chairman, there may be some dispute as to what a large extra atmospheric nuclear detonation would do to our ground-based computers. But I think there is no dispute as to what it would do to the communications satellite. I think it was Mr. Dacey who mentioned how critical they were in our communications.

It is my understanding that they are the softest link of our communications net, that a large extra-atmospheric nuclear detonation, producing a surge of Compton electrons, would take out all of the satellites that were in line of sight. And those that were not would shortly die because of pumped Van Allen belts. So they would decay very quickly.

I have only two or three or so hardened satellites, radiation-hardened satellites, the Milstar satellites. They carry a tiny percentage of even our military communications, to say nothing of other communications.

And by the way, you cannot launch a new satellite if this happens because Van Allen belts are still pumped up, will remain so for a year or so. So to get communications through satellites, you would have to build some radiation-hardened satellites and launch those. And clearly, by that time, the Van Allen belts would have receded and you could now launch conventional satellites.

And by the way, this could all happen with an "Oops, I am sorry," kind of an event, an accidental launch. And they detonate the missile high in space so that it is not going to hurt anybody on Earth. What would we do if that happened? This is the ultimate in asymmetric terrorist attack, of course?

Just an "Oops, I am sorry," kind of thing, you know, that was an accident. But now all of our communications satellites are gone and will be gone for probably a year or so.

What will we do? And is there a COOP plan for that?

Mr. LENTZ. What I would like to respectfully do is take that question for the record. And we will get back to you on that as soon as possible.

Mr. BARTLETT. Professor Spafford, you, I noted, reflected an interest in this?

Mr. SPAFFORD. I am unaware. But I am not privy to the plans that have been made like this. I believe it would certainly be quite disruptive for some time, not only to the military, but certainly to the civilian population. It would be very difficult to recover from.

Mr. BARTLETT. This is not an impossible event. It is a bit like a fire in your home. That is not very likely to happen. But none of you would sleep very well tonight if you did not have fire insurance on your home.

I think that having a plan as to what we would do if this happened is pretty much the equivalent of investing a bit in a fire insurance policy for your home. I am not aware that we have any of the equivalent of a fire insurance policy for this.

Don't you think that we ought to? Because this is not an impossible event at all. I am not sure it is an even unlikely event in today's world.

Has no one looked at this and been concerned about what would we do? Now there are an increasing number of countries that could do this—North Korea.

China now has I think 13 Long March missiles, each tipped with a 4.4 megaton weapon, we believe pointed at our 13 largest metropolitan areas in this country. The detonation of just one of those extra-atmospherically, anywhere around the globe, by the way, it really does not matter where it happens, it has exactly the same effect.

Is anybody looking at the consequences of this and what would we do? If they are not, do you think we ought to?

Yes, sir?

Mr. SPAFFORD. Sir, I would just observe that in addition to communications, our GPS systems used in all our smart weapons and other systems would also be affected.

Mr. BARTLETT. That is all gone, sir, unless they are hardened. And I do not know whether we have hardened any of the GPS assets or not. I doubt it.

Mr. DACEY. I would just make one side comment. I cannot address your central question. But I can say that we did a report last year, which indicated a need for some further consideration of the reliance upon commercial satellites by the government.

That does not fix your problem. But at least there were some issues. And one of the issues raised was that they typically are not as hardened as the military satellites.

But anyway, I can certainly provide you a reference to that report, if you are interested.

Mr. BARTLETT. As the professor pointed out, not only can you not talk to each other, you do not even know where you are if the GPS is gone. It is a whole new world that we could quickly be thrust

into. And I am concerned that apparently there is little thought being given to what we would do in that eventuality.

Thank you very much, Mr. Chairman.

Mr. SAXTON. Thank you.

Mr. Rodriguez.

Mr. RODRIGUEZ. Thank you very much. Let me start off by just indicating that I am going to ask the chairman. And I know there were some comments about initially that there was over 50,000 hits just in the last year.

Maybe we can have, Mr. Chairman, a closed meeting on maybe the sources and the character and the patterns that we might have. And we have not had one of those for a while. And talk about some of those things.

In addition to that, I know that there was a little dialogue about the importance of the people that are working. I know and I keep bringing this up. Because we always talk about immigration, you know, but we have been also a brain drain on the rest of the world.

And out of those 300,000 people that we brought in each year, right prior to 9/11, a large number of them were in computers. And I know that DOD has made a tremendous effort at reaching out to our universities and starting that process.

But I also know that we are way behind. And I was just wondering, in terms of the fact that I really feel that we need to allocate more resources for the training and so we can grow our own computer people, instead of bringing them from abroad.

Mr. LENTZ. I cannot agree with you more, that this is a very, very important priority. And funding is always an issue in the education and training area.

We are getting ready to issue, this September, the first comprehensive information assurance policy directive on education and training and awareness. It is going to lay out specific requirements for the schoolhouses, certification standards, the ways we are going to codify people in particular specialties. We are working with the Under Secretary for Personnel and Readiness to be able to do that in the military services. So we are taking that very seriously.

And I agree with you 100 percent. It is absolutely a vital. And it is the most important goal that we have in our five-point strategy plan.

Mr. RODRIGUEZ. Thank you. Because I know we have to grow our own. It is okay sometimes to bring them from abroad. But when it comes to the Department of Defense, we have to make sure that we can grow our own.

So I think that is critical. And if we can have a closed meeting on the discussions, I would be interested to see some of the new occurrences that have been happening. I know one of the patterns that we have had is that every time we had an international incident, the number of hits would jump up from just the regular hackers to some organized efforts. And I know that there has been some worldwide efforts at increasing that.

And then they are educating themselves. And they are getting tougher and tougher in seeing what we might need to do in order to be able to cope with that.

So thank you very much, Mr. Chairman.

Mr. SAXTON. Let me just ask a couple of questions and then if Mr. Larsen has any. We have talked on a couple of occasions today about the possibility of terrorist groups having so-called training camps or whatever to teach people these skills necessary for this.

And I understand the answers to that. But a related question is, with regard to terrorist groups such as al-Qaeda, do they have the capability or is there any evidence that they have the capability to employ or coordinate cyber attacks?

Mr. LENTZ. Well, clearly, as I think we have discussed on the panel, the availability of these technologies on the Internet certainly provides them the technology to be able to wage cyber warfare as they so desire. As to the specifics of what they are capable of doing and how they might do that, I prefer to put that on the record and give you a more classified report on that.

Mr. SAXTON. We will look forward to it. We know they are creative. And we know that we have to be creative to deal with them. And sometimes, some of the things that we find ourselves doing surprise us. General Handy, who is the commander of FORCECOM, was in my office the other day. And I showed him this picture on my wall of two of our special operators in Afghanistan, working with the Mujahideen, the B–52 overhead and regular conventional soldiers marching down the road.

And he said, "You know what surprised us the most about Afghanistan was that RC–17s doing air drops were dropping bales of hay and other things that were necessary to keep our soldiers comfortable while they were riding horses." And so we go all the way from those kinds of things that we have to creatively figure out, as we deal with terrorists, to the most technically sophisticated things that are involved in cyber attacks and other technical types of attacks that we might face.

So it is a complicated world. And this is one of the issues that I think is really important for us to look at. And that is why we are having the hearing, thanks to Mr. Larsen.

Mr. Lentz, what is the department's plan for an integrated response to attacks across multiple networks? Is it possible that an attack could remove the department's ability to coordinate a recovery effort across sites?

Mr. LENTZ. The third goal of our strategic plan deals with situational awareness and command and control. It is clearly a goal that we are taking very seriously. And we are putting as many resources into it that we can.

The good news is that with the establishment of strategic command as the focal point for managing computer network defense activities and what I believe is probably the most vivid good example of what has occurred in the past several years, which is the establishment of the Joint Task Force (JTF) for computer network operations, we are able to coordinate across the globe, across each one of our combatant commands, to be able to respond effectively.

In addition, in my opening remarks, I mentioned we have a very close partnership with our international partners. So that a virus that may strike in Australia, as an example, their command center and their computer emergency response center will notify us immediately upon the indication of that particular event, giving us hours of notice to be able to react, as an example.

So this is a global activity, from a command and control standpoint. And I think we are doing a good job in that regard.

Mr. SAXTON. Mr. Dacey, do you want to comment?

Mr. DACEY. We did work on the JTF and the incident reporting capabilities and handling capabilities back in 2001. But we really have not done any work since then. So I do not really have any comments on the current state of efforts. I do know we made several recommendations. And the department has implemented or is in the process of implementing most of those.

Mr. SAXTON. Okay. Thank you.

Mr. Larsen.

Mr. LARSEN OF WASHINGTON. Mr. Chairman, I have no more questions for this setting. I want to really thank you for taking the leadership in calling this hearing today.

And I want to second what Mr. Rodriguez said about perhaps a follow up hearing in a classified setting. Because I do have some additional questions, which I suspect I will get an answer that will be along the lines of, "Perhaps those are better for another setting."

But I think it is going to be important to have a follow up to get at some of those questions. And so with that, I again want to thank you and thank the panel for making their time available and answering the questions of the committee.

Mr. SAXTON. Thank you.

Mr. Bartlett has one final——

Mr. BARTLETT. Thank you, Mr. Chairman. I too would like to thank you for a very important and timely hearing.

Gentlemen, I have had a concern—I hope a concern I need not have—that there could be a virus or a worm that lay there dormant until there was a surge in activity, such as would occur during an emergency. It would then become active and we could then be denied our assets just when we needed them most.

Can our security systems detect a dormant virus or a worm? Or do they have to be squirming before we can see them?

Mr. CHARNEY. There are virus checkers, of course. And if the worm is a known worm and usually most——

Mr. BARTLETT. But suppose, sir, that they are there and doing absolutely nothing. They are just totally dormant, waiting for a surge in activity.

And they are queued to become active as the surge in activity, which would occur during an emergency. Then they would become active and deny us our assets when we needed them most.

Do our security systems have the capability of detecting a virus or a worm that is doing nothing?

Mr. CHARNEY. Yes. If it is a known worm for which we have a signature or virus——

Mr. BARTLETT. But if it is not a known worm for which we have a signature or virus. It is a new one that they plant in there and it will stay there quietly, awaiting a surge in activity, at which time it will become active. Can we or can we not detect that?

Mr. CHARNEY. There are some techniques to detect it. But I would not say that there are 100 percent certain techniques.

We have seen cases when I was in the Justice Department of time bombs in systems, things that were set to go off at a certain date and time. But there have been very, very few cases of what

we call zero-day vulnerabilities, where something happens in terms of an exploit, that no researcher or the community was completely unaware of.

Usually, there is prior awareness. Most exploits happen after the vulnerability has been widely reported.

And anti-virus vendors constantly update their signature files. The key is that when the vendors put out these updated signature files, it is incumbent upon users at all levels to make sure they download the most current files and run them against their machines.

Is it possible that there would be a time bomb of unknown proportion that activates? Yes, it is possible.

Mr. BARTLETT. Dr. Spafford.

Mr. SPAFFORD. Yes, there are two ways that this could occur. One would be something external to the installed system, a traditional kind of virus or worm that has been inserted on to the system through the network, for instance, that would then lie dormant.

There are techniques to find that: system configuration scanning tools, things that know what the system should look like and then compare to see if there has been any change. It would be found on some machines, eventually reported into the signature files, as Mr. Charney was speaking about. And then we would find that that was there.

The insider problem, however, the one that I referred to earlier, there could be code that has been added to software that is supposed to be on the system that we do not know is there. And that could be what is awaiting a trigger.

We do not have any kind of mechanism to look for that. We have to depend on whoever has produced the software to have done a good job of quality assurance. And we also have to depend on the contractors and the people who have installed it and operated it not to have manipulated it. I would say, for that case, we really do not have the guarantees in place that you would like to have.

Mr. BARTLETT. Thank you. Thank you very much. And thank you, Mr. Chairman.

Mr. SAXTON. Thank you, Mr. Bartlett, for your questions. Let me just ask one final question, kind of a general kind of a thing. The Congress of the United States would like nothing better than to say that we have done a good job in this area. And we have had a couple of hours worth of conversation here today about a variety of subjects.

Have we missed anything? Is there something that Congress should be doing that you are aware of that we are not? Do you have any suggestions for us?

Mr. SPAFFORD. I made several suggestions in my written testimony. And rather than reiterate those here, they are on the record.

I believe there are some things we could do better. I am pleased, however, at the efforts that have been represented by industry and by the government.

We have made great progress in the last few years. But there is a great more that we can do yet.

Mr. DACEY. I would just like to say that I think holding oversight hearings like this are very important. And one of the key issues

with issuing FISMA was that the agencies, including the Department of Defense, would be providing annual—and now they are going to some quarterly reporting on certain information—about information security.

So I think that will provide an opportunity. It was meant to provide an opportunity, I believe, for congressional oversight.

And those reports are due out in September for the first year of the FISMA implementation. And those will provide a gauge and comparative information from year to year on progress that is being made.

Mr. LENTZ. Yes, sir. I would like to concur with what Mr. Dacey says completely. The fact that we are having these types of hearings, I think awareness is the number one, I think, advantage that we have. Making everybody understand what the problems and challenges are is, I think, the key element of this.

As I mentioned in my opening remarks and Mr. Larsen echoed that, we are very dependent upon IT modernization for our ability to be able to protect the network. It is the foundation, the bedrock, for our success.

And I think having hearings like this, I think, will give us a chance to be able to emphasize that. And I think the closed door session will also provide further insight into that.

Thank you.

Mr. CHARNEY. And I too had recommendations in my testimony. So——

Mr. SAXTON. Well, thank you very much. Unless there are other questions, we will thank you for being here today. And your input has been extremely valuable.

And I would also like to thank Mr. Meehan and Mr. Larsen and Mr. Bartlett and Mr. Wilson and the other members that took place, and the staff, who worked so hard to bring this all together.

Thank you very much. I believe it is been insightful. And unless there is something further, the subcommittee stands in recess. And we will hopefully see you all again sometime soon.

Thank you.

[Whereupon, at 11:52 p.m., the subcommittee was adjourned.]

APPENDIX

JULY 24, 2003

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

JULY 24, 2003

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

---

Subcommittee Hearing

"Cyber Terrorism: The New Asymmetric Threat"

July 24th, 2003

Good morning ladies and gentlemen. The Subcommittee on Terrorism, Unconventional Threats and Capabilities meets this morning to assess the new asymmetric threat of cyber terrorism. In particular, we would like to have a better understanding of this threat against the Department of Defense information technology (IT) systems and networks.

Information dominance is a cornerstone of the Department's Force Transformation in the 21st Century. We have witnessed these remarkable technological capabilities—from sensors gathering intelligence to sending that information to shooters in the air or on the ground in both Operation Enduring Freedom and Operation Iraqi Freedom. This incredible transmission of data was accomplished with greater accuracy, in a shorter amount of time with fewer casualties. Armed with these incredible capabilities, our military forces have gone into battle with more situational awareness than any other troops in history. While new technological advances bring information superiority, it also brings new responsibilities and challenges.

Technology evolves rapidly. While programmers and software developers build more advanced systems to run more tasks, criminals become more creative in their methods to break into these systems. Their purpose may be to steal information, wreak havoc, or send out false commands or information. Without a defense-wide information assurance policy and implemented practices, the Defense Department's networks may be vulnerable to anyone who has a computer, the knowledge, and willpower to launch cyber attacks.

Information assurance (IA) is a critical issue for the Department because it operates approximately 3 million computers, 100,000 local area networks (LANs), and 100 long-distance networks. These systems including military service-based, joint defense, and intelligence computers and networks are a part of the Global Information Grid (GIG), part of which is dependent on commercial civilian systems. All of these systems are susceptible to acts of cyber terrorists twenty-four hours a day.

I whole-heartedly agree with Secretary of Defense Donald Rumsfeld that IT is the enabler behind defense transformation. What we need is the ability to leverage the

technology and commercial best practices to ensure the security and integrity of the Departments' networks. This is a major undertaking with extraordinary consequences.

While the subcommittee recognizes the critical efforts and difficulty of implementing the Defense-wide Information Assurance Program (DIAP), concerns have been raised that there is not sufficient oversight and management at the Department to achieve the objectives contained in the program.

The Subcommittee is interested to learn more about the Department's information assurance (IA) policy and the immediate and potential cyber threats against the Department's IT systems and networks. Additionally, the Subcommittee is interested to learn about the procedures or defense mechanisms presently in place at the Department to counter cyber attacks. Finally, the Subcommittee would like to know more about the processes or best commercial practices that private industry has implemented to handle cyber security issues and whether these practices are applicable to the Department. This hearing will attempt to determine what progress the Defense Department has made in its implementation of the DIAP. We are also interested to learn what challenges lie ahead for the Department as it confronts cyber terrorists in cyberspace.

Statement by

Robert F. Lentz

Director of Information Assurance

Office of the Assistant Secretary of Defense for

Networks and Information Integration

and

DoD Chief Information Officer

Before The

House Armed Services Committee

Subcommittee on

Terrorism, Unconventional Threats and Capabilities

Hearing on

Cyber-Terrorism

July 24, 2003

For Official Use Only
Until Release by the
Committee on Armed Services
U.S. House of Representatives

Thank you Mr. Chairman and members of the Subcommittee. I am honored to be here and pleased to have the opportunity to speak with your committee about actions the Department of Defense is taking to address threats to the security of its networks, systems and information. We have and continue to make significant progress in our quest to secure and defend our computer networks. My testimony will highlight some efforts we have initiated, successes we have achieved and the challenges we face.

Secretary Rumsfeld, in one of his initial testimonies before the House Appropriations Defense Subcommittee, identified six key transformational goals for the Department around which we focus our defense strategy and develop our force. Leveraging information technology to create a seamless, interoperable, network-centric environment is one of those foundation transformational goals. As demonstrated in recent operations, U.S. Forces have unparalleled battlefield awareness; they can "see" the entire battlefield while the enemy cannot. They have translated information technology into combat power beginning the transformation from Platform-Centric to Network-Centric Operations. And the transformation has just begun. A new era of warfare has emerged, one based on the concept that connections provide greater power, agility, and speed. Multiple connections enable U.S. Forces to fight and mass combat effects virtually anywhere, anytime, and with a smaller "real" force. Through connections, smaller forces operating locally can leverage almost the full weight of global U.S. combat power. However, as our dependence on information networks increases, it creates new vulnerabilities, as adversaries develop new ways of attacking and disrupting U.S. Forces. In recognition of this dichotomy, the Secretary established the protection of U.S. information networks from attack as another foundation transformational goal.

Emphasizing that transformation is not an event, Secretary Rumsfeld described it as an ongoing process, a journey that begins with a transformed "leading edge" force, which, in turn, leads the U.S. Armed Forces into the future. Mr. John Stenbit, Assistant Secretary of Defense for Networks and Information Integration and the DoD Chief Information Officer (CIO), is committed to support our transformation by providing the power of information to that leading edge. To bring power to the edge, he established the

following goals for his supporting effort: (1) develop a ubiquitous network environment, (2) richly populate with information of value, as determined by the consumer, (3) ensure the network is highly available, secure and reliable. My role in bringing power to the edge is to support Mr. Stenbit's goals by guiding and overseeing the Department's Information Assurance (IA) Program: the strategy, policy and resources required to create a trusted, reliable network.

No one agency, organization, or person is capable of assuring this vast network of capabilities — the Department as a whole must assure our Global Information Grid (GIG). Everyone who uses, builds, operates, researches, develops, tests, and explores information technology is responsible for IA. Everyone must be aware of his or her role in assuring the nation's information. A clear and coherent policy framework is required to achieve that awareness and the synergy it creates. The Department's transformation to Network-Centric Operations is most prevailing policy driver. For IA, net-centricity is a transformation of what we do, because the way we protect information and defend information systems and networks is fundamentally different in a globally interconnected world.

In October of last year DoD published its capstone directive on IA followed by a supporting instruction in March of this year. The directive establishes basic policy and assigns responsibilities to achieve IA through what we refer to as a 'Defense-in-Depth' approach that integrates the capabilities of technology, operations and personnel. The instruction implements policy by further assigning responsibilities and prescribing procedures for applying integrated, layered protection of DoD information systems and networks. These two documents establish the IA framework for the transformation from Platform-Centric to Network-Centric Operations. The new directive and instruction are comprehensive, focusing on the confidentiality, availability, integrity, authentication and non-repudiation of information; essentially all IA services not just the traditional confidentiality aspects.

These documents set the tone and lay the foundation for all remaining IA policies such as those for System Certification and Accreditation, Network Ports and Protocol Management, Computer Network Defense (CND), and CND Response Actions. They establish management boundaries and responsibilities at the Department level, the Component level, and the individual system level. They also organize information systems into 4 types [1] in order to better focus accountability for addressing IA during system development, during operations, in the acquisition of IT services, and in network interconnections.

The new policies also establish a banded risk model to help information and system owners determine appropriate target levels of confidentiality, availability, and integrity. These target levels are expressed as IA Controls, which address security best practices for general threats and system exposures, federal and DoD policy requirements, and IA interoperability across the GIG. The intent is to use these IA Controls as standard terms of reference for metrics and reporting. The Joint Staff has already taken a first step in that direction by cross-referencing them in the Joint Quarterly Readiness Review (JQRR) guidance, and we are working to make them the foundation of our FISMA (Federal Information Security Management Act) reporting. DoD's Operational Test and Evaluation directorate will test the controls during the conduct of 'Red Team' assessments of newly deployed systems.

As I mentioned earlier, our IA directive and instruction are the foundation of our IA policy framework. That framework is organized into 9 sub-categories (General; IA Certification & Accreditation; Security Management; Computer Network Defense; Interconnectivity / Multiple Security Levels; Network and Web; Assessments; Education, Training and Awareness, and Other IA (Integration)). The General sub-category

---

[1] The four types of information systems are:
Enclaves – operational networks and computing centers with IA focus on security management and administration
AIS Applications - IT acquisition or development initiatives with IA focus on building protection in
Outsourced IT-based processes - acquisition of IT services with IA focus good source selection factors and allocation of IA responsibilities between service provider and government users
Platform IT Interconnections – network connections of weapons systems and other platforms with embedded IT (e.g., medical systems, utilities systems) with the IA focus on managing connection risk

currently contains the IA directive and instruction I mentioned previously. A Handbook and Manual are in development. We have published policy for our core missions of Protect and Defend, policies that guide the Computer Network Defense mission. We also have policies in progress to support other goals and missions. We are making good progress in the formulation of policies that support multiple goals and missions such as Ports and Protocols Management, Interconnectivity, and Assessments. Formal policies covering Identity Management, Public Key Infrastructure, Public Key Enabling, and Biometrics are not as mature. However, strong acquisition programs and memo policies support these areas.

There will be major challenges in the maturation of the IA policy framework. Our DoD IA community is large and diverse, and IA is both pervasive and interdependent upon many other policies and processes –a particular challenge for the policy formulation process. There are, however, opportunities to improve the formulation process. We are examining ways to make the process more open, more visible, more collaborative, and, as a consequence, faster. A second challenge is the dissemination of new policy along with the vision and intent behind the policy. Published and draft versions of DoD IA policy are available online. We have also published Frequently Asked Questions and tutorials for the two foundation documents, and we are looking at ways to provide an online, web-based environment that helps users navigate through the IA policy library at the right level of readership – executive, manager, practitioner. A third challenge that we will continue to address is the integration of IA into related policies and programs. We have effort underway to work the integration of IA into the acquisition process to include designating IA as a Key Performance Parameter in major systems acquisition programs. We will be expanding that effort to also cover requirements generation. The last and perhaps most important challenge is IA policy change management and the effect of DoD IA policy changes on Combatant Command, Service and Agency implementing policies and programs.

DoD IA policy establishes top level who, what, and the procedural how. DoD has also developed and is implementing an Information Assurance (IA) Strategic Plan. The plan defines the Department's goals and strategic objectives for IA, providing a consistent, Department-wide approach to assuring our information. It was prepared through the cooperative efforts of the Combatant Commands, Services, and Agencies (C/S/As) and is intended to be a living document. We are aligning our investments and strategic initiatives to the objectives in the plan and are developing milestones and performance measures to gauge their success. All of this is done in close coordination with the Department's Global Information Grid architects, product and system developers, and acquisition executives. The Strategic Plan or roadmap has five major goal areas aligned to the technology, operations and personnel capabilities of our 'Defense-in-Depth' approach to IA. Each goal has supporting strategic objectives, sub-objectives, timelines and associated metrics. The goal areas are:

1. Protect Information to safeguard data (as information) as it is being created, used, modified, stored, moved, and destroyed, at the client (desktop), within the enclave (base network), at the enclave boundary (interface with global transport network), and within the computing environment (applications and operating systems), to ensure that all information has a level of trust commensurate with mission needs. The goal of the Global Information Grid is to allow information originating from anywhere on the network to be available throughout the network. Often the originator has little foreknowledge of who will use this information. Therefore, the new burden on IA is to ensure that all information is protectable. This means that all information can be protected from "end to end" and throughout its life cycle.

DoD has already invested in programs such as Public Key Infrastructure, Biometrics, and Common Access Control (CAC) Cards to support this goal. By the end of this year, we expect nearly all DoD personnel to be outfitted with a CAC card for identification and access to the network. However, more effort is needed to ensure that these tools are implemented throughout the DoD enterprise. DoD is focusing hard on the use of open standards and Extensible Markup Language for interoperability both within DoD and

with industry and the business community. The key is to do that securely. We are involved intimately with the rest of the Federal government in identification and identity management efforts. We want to insure that the mechanisms we use in our defense missions do not have to be duplicated in our interactions with the rest of government. Coalition, cross security-domain, and collaborative communications require "tagging" of people and information in order to provide agility for dynamic access control decisions. Our supporting protection infrastructures (Key Management Infrastructure, PKI, and network management systems) must have a higher level of assurance in order to provide an integrated systems security posture. Achieving this goal requires partnerships and combined efforts with other components of the security community: physical security, personnel security, and critical infrastructure protection.

2. Defend Systems and Networks by recognizing, reacting to, and responding to threats, vulnerabilities, and deficiencies, ensuring that no access is uncontrolled and all systems and networks are capable of self-defense. DoD systems and networks are constantly under attack and must be continuously defended. To ensure success, defensive mechanisms must be an integral part of the design and implementation of systems and networks across the enterprise. In addition, capabilities must be deployed to react and respond to internal as well as external threats and attacks.

3. Provide Situational Awareness/IA Command and Control (C2) integrating the IA posture into common operational pictures to provide a shared understanding among decision makers through decision tools that assist in the planning, execution and monitoring of coordinated actions. Combatant Commanders must have sufficient visibility of their networks, threats, and operations to gain a full awareness of their situation. The complex and interdependent nature of our networks and the demands of Network-Centric Warfare require shared awareness and understanding across the enterprise. The role of the IA community is to work closely with Combatant Commanders and key agencies in building the requirements for the Common Operational Picture and the Standing Joint Force Headquarters (SJFHQ). The DoD must have IA Situational Awareness and C2 requirements built in if it is to share information, process it

effectively, gain a shared understanding, and act in a synchronized fashion to respond in an effective and appropriate manner. This extends to other government and private sector partners as well as to our international allies to provide us a worldwide situational awareness critical to proactively defending our forces both at home and globally.

4. Transform and Enable IA Capabilities to develop and deliver dynamic IA capabilities and to improve inter and intra entity coordination (government to government, government to industry, and intra-defense) to reduce risk and increase return on investment. Network-Centric operations demand greater process agility and integration. As such, this goal focuses on improving the processes integral to developing and delivering IA capabilities supporting the transformation of the force. DoD's processes are generally designed to follow a cycle of deliberate planning, operations, and disengagement. Decision support processes are designed to function in a time-linear way. As a result, our responsiveness is often too slow or ill matched to the environment in which we now operate. The Network-Centric Warfare environment requires rethinking and innovation in how we reshape the processes of planning, programming, and resourcing in order to be responsive to ideas that take hold and become marketed in time frames faster than current processes can accommodate.

The ever-changing and evolving information technology industry stresses DoD's processes and challenges them to keep pace. Maintaining a competitive edge over our adversaries demands that we transform the mechanisms used to develop and deliver new and dynamic capabilities to become more responsive to ever-changing needs. Agility must be a goal that every process meets to maintain a competitive edge. Continuous improvement is mandated. This approach places great importance on harvesting and prioritizing ideas and the rapid development and deployment of concepts and capabilities to enable constant and continuous preparation, shaping, and execution of our responses to the environment.

5. Create an IA-Empowered Workforce that is trained, highly skilled, knowledgeable, and aware of its role in assuring information. Well-trained people are the cornerstone of any successful IA/IT program. Given today's threats against IT systems and networks, it is important that all personnel understand the critical role of IA within their daily work activities. In order to maintain a DoD workforce that is technologically sound, various programs must be instituted to support the IA mission (i.e., training and education, IA/IT awareness, and recruitment and retention initiatives). To create an IA-empowered workforce, there are three critical success factors: (1) a need for constant vigilance, (2) well-equipped IA/IT personnel, and (3) buy-in from key decision makers. The need for constant vigilance in information security and awareness is key to deterring threats and mitigating vulnerabilities. Establishing an IA/IT workforce that is equipped with the proper skill sets and tools allows the Department to create and implement value-added solutions that are agile and technologically advanced. We are also leveraging initiatives to create centers of academic excellence in our colleges and universities as well as IA scholarships with the goal to improve our recruitment and retention. Through efforts like these and our System and Security Administrator Certification Program, we will achieve this goal.

This Strategic Plan is the roadmap for DoD in assuring our information, and it serves as a guide for all Services and Agencies within the Department. At DoD's enterprise-wide IA conference last January, then NSC member Howard Schmidt while describing the National Strategy to Secure Cyberspace pointed to the common themes and complementary nature of both our documents. We will continue to review our vision, goals, and objectives for relevancy, currency, and applicability. Implementing the IA Strategic Plan requires the involvement of all Combatant Commands, Services, and Agencies and will require the continued support and commitment of DoD leadership, to include the IA Senior Leadership Group (senior IA leaders from the Department's Combatant Commands, Services, and Agencies), the DoD Chief Information Officer, and the Military Communications and Electronics Board (MCEB). Oversight of the implementation, reviews, and updates to the Strategic Plan falls to the IA Senior Steering

Group. My directorate will serve as the Strategic Management Office for the IA Strategic Plan, and a Goal Lead internal to my organization has been assigned to each of the five IA goals. The Plan, supported by our policy framework, is a dynamic roadmap designed to support Secretary Rumsfeld's transformational force.

While the Network-Centric transformation of national defense capabilities is the primary driver of DoD IA policy and our IA Strategic Plan, we must also address federal and statutory requirements. These requirements influence how we organize, interact, and manage. They also tell us that there are many consumers of information assurance management information – program analysts, budget analysts, auditors – who are not IA technical specialists. Our challenge in creating a management or command and control language for Information Assurance is to ensure that it is expansive enough to serve all audiences – military, technical, business management, and oversight.

The Federal Information Security Management Act of 2002 (FISMA) is perhaps the most influential statutory requirement for DoD with respect to IA. A strengthened version of the Government Information Security Reform (GISR) provisions of the FY 2001 Defense Authorization Act, it requires DoD as well as other agencies to … provide information security protections…comply with information security standards… ensure information security management processes are integrated with agency strategic and operational planning processes…as well as numerous other responsibilities. The policies and strategic plan I described for you are our tools to meet those responsibilities. In both the FY2001 and FY2002 GISR reports to Congress, OMB mentioned areas where the Department excels. Our IA training program is, "the most comprehensive training program and processes of any Federal department or agency." The Department has a fully functional and effective incident response capability. Guidance and procedural frameworks for detecting, reporting, and sharing vulnerabilities are documented. In fact our incident and response center is an integral part of the Federal community's cyber warning network. The report also mentions that DoD has undertaken aggressive action to improve and expand its information assurance capabilities by implementing the Information Assurance Vulnerability Alert (IAVA) process to all Services and agencies;

ensuring timely distribution of effective computer security policies and procedures; and improving DOD business processes to ensure that all systems are protected. We are far from perfect, however, and are working diligently to improve our system certification and accreditation practices and the databases that help us track those certifications. That effort is more than an accounting drill. It is a comprehensive effort to get near real time visibility of our entire network, manage configuration enterprise wide, distribute changes and security patches, and perform consequence management when something effects the operation of our systems and networks.

The challenges we face are the same challenges found throughout government and industry. Those are the challenges we are addressing in our IA Strategic Plan. Do we have unique challenges? Yes, but they are not insurmountable. Size, global presence, dynamic technical and operational requirements all contribute to the complexity of our environment. But, we are adapting. We are making progress. We are managing the risk and managing it successfully across all of our National Security missions within DoD. That success is documented in our GISR, now FISMA reports as well as in our Annual IA report to Congress. Most important, however, it is reflected in our ability to act as an enabler, not an impediment, in the conduct of Network-Centric Operations in several theaters across the globe.

We have come to realize that we will never be able to achieve absolute protection of our information, systems and networks. However, we also realize that we can effectively mitigate the effects of challenges to the security of our information, systems and networks. We have created a robust Computer Network Defense capability within the Department, a capability that continues to evolve and transform itself in pace with the evolving and transforming threat.

IA is a journey, not a destination. That may be a hackneyed phrase but it accurately depicts The IA environment in DoD. All systems are legacy systems as soon as they go online. The demand for greater bandwidth, functionality, connectivity and other features is constantly expanding. That demand will be met. Our task within the Department is to

insure it is met securely. IA must be baked in and not spread on as an afterthought. We are stepping up to that challenge. DoD's IA community is intimately involved not only in the development of protective technologies for space-based laser, advanced fiber optic, and wireless transport networks but also in the development of end-to end IA architectures and technologies. From the labeling of information and people for controlled access to the security of enterprise computing environments, we are working now to ensure IA is baked in from both the protect and defense perspectives.

I appreciate the opportunity to appear before the Subcommittee and look forward to your continuing support on this very critical issue. Thank you.

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Terrorism, Unconventional Threats and Capabilities, Committee on Armed Services, House of Representatives

For Release on Delivery
Expected at 10 a.m. EDT
Thursday, July 24, 2003

INFORMATION SECURITY

Further Efforts Needed to Fully Implement Statutory Requirements in DOD

Statement of Robert F. Dacey
Director, Information Security Issues

GAO-03-1037T

GAO
Accountability · Integrity · Reliability

Highlights

Highlights of GAO-03-1037T, a report to Subcommittee on Terrorism, Unconventional Threats and Capabilities, Committee on Armed Services, House of Representatives

Why GAO Did This Study

The Department of Defense (DOD) faces many risks in its use of globally networked computer systems to perform operational missions—such as identifying and tracking enemy targets—and daily management functions—such as paying soldiers and managing supplies. Weaknesses in these systems, if present, could give hackers and other unauthorized users the opportunity to modify, steal, inappropriately disclose, and destroy sensitive military data.

GAO was asked, among other things, to discuss DOD's efforts to protect its information systems and networks from cyber attack, focusing on its reported progress in implementing statutory information security requirements.

www.gao.gov/cgi-bin/getrpt?GAO-03-1037T

To view the full product, click on the link above.
For more information, contact Robert F. Dacey at (202) 512-3317 or daceyr@gao.gov.

July 24, 2003

INFORMATION SECURITY

Further Efforts Needed to Fully Implement Statutory Requirements in DOD

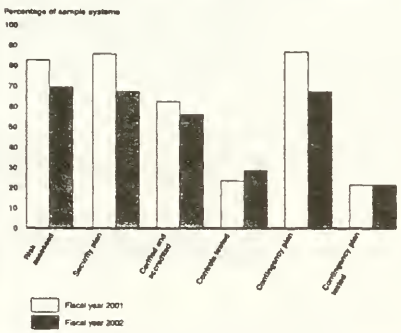
What GAO Found

In its fiscal year 2002 report on efforts to implement information security requirements under Government Information Security Reform law, DOD reported that it has an aggressive information assurance program and highlighted several initiatives to improve it. These initiatives included developing an overall strategy and issuing numerous departmentwide information security policy documents. DOD's reporting highlighted other accomplishments, but acknowledged that a number of challenges remain for the department in implementing both its policies and procedures and statutory information security requirements.

DOD reported several material control weaknesses, which included needing to decrease the time necessary for correcting reported weaknesses and ensuring that computer security policies are enforced and security capabilities are tested regularly. Further, performance data DOD reported for a sample of its systems showed that further efforts are needed to fully implement key information security requirements, such as testing systems' security controls, throughout the department (see figure).

Although DOD has undertaken its Defense-wide Information Assurance Program to promote integrated, comprehensive, and consistent practices across the department and has recently issued both policy guidance and implementation instructions, it does not have mechanisms in place for comprehensively measuring compliance with federal and Defense information security policies and ensuring that those policies are consistently practiced throughout DOD.

Reported Results for Selected DOD Information Security Performance Measures



Source: OMB FY 2002 Report to Congress on Federal Information Security Reform, and GAO (analysis)

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss the status of efforts by the Department of Defense (DOD) to protect its information systems and networks from cyber attack. DOD's military services and agencies face many risks in their use of globally networked computer systems to perform operational missions, such as identifying and tracking enemy targets, and daily management functions, such as paying soldiers and managing supplies. Weaknesses in these systems, if present, could give hackers and other unauthorized users the opportunity to modify, steal, inappropriately disclose, and destroy sensitive military data.

Since 1996,[1] we have reported that poor information security in federal agencies is a widespread problem with potentially devastating consequences. Further, we have identified information security as a governmentwide high-risk issue in reports to the Congress since 1997—most recently in January 2003.[2] Concerned that significant weaknesses in federal computer systems make them vulnerable to attack, in October 2000 the Congress passed and the President signed into law Government Information Security Reform provisions (commonly known as GISRA)[3] to establish information security program, evaluation, and reporting requirements for federal agencies—requirements that are now permanently authorized and strengthened through the recently enacted Federal Information Security Management Act of 2002 (FISMA).[4]

In my testimony today, I will first provide an overview of the increasing nature of cyber security threats and vulnerabilities and of the continuing pervasive weaknesses across the federal government that led GAO to initially begin reporting information security as a high-risk issue. I will then discuss the status of DOD's efforts to ensure the security of its information systems and to implement the statutory information security requirements, focusing on the performance data that DOD reported to the Office of Management and Budget (OMB). Finally, I will discuss some of

[1] U.S. General Accounting Office, *Information Security: Opportunities for Improved OMB Oversight of Agency Practices*, GAO/AIMD-96-110 (Washington, D.C.: Sept. 24, 1996).
[2] U.S. General Accounting Office, High Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures, GAO-03-121 (Washington, D.C.: January 2003).
[3] *Title X, Subtitle G—Government Information Security Reform, Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001*, P.L.106-398, October 30, 2000.
[4] *Title III—Federal Information Security Management Act of 2002, E-Government Act of 2002*, P.L. 107-347, December 17, 2002. This act superseded an earlier version of FISMA that was enacted as Title X of the Homeland Security Act of 2002.

the challenges for the department in establishing an effective information security management program.

In preparing this testimony, we relied on prior reports and testimony on information security both governmentwide and for DOD. We also analyzed reports prepared by the DOD chief information officer and the DOD inspector general (IG) for fiscal year 2002 GISRA reporting, as well as recent DOD policy and guidance documents related to information security. Further, we analyzed OMB's May 2003 report to the Congress on fiscal year 2002 GISRA implementation.[5] We did not validate the accuracy of the data reported by DOD or OMB. We performed our work in July 2003, in accordance with generally accepted government auditing standards.

Results in Brief

Protecting the computer systems that support our nation's critical operations and infrastructures has never been more important. Telecommunications, power distribution, water supply, public health services, national defense (including the military's warfighting capability), law enforcement, government services, and emergency services all depend on the security of their computer operations. Yet with this dependency comes an increasing concern about attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence gathering, and acts of war. Such concerns are well founded for a number of reasons, including the dramatic increases in reported computer security incidents, the ease of obtaining and using hacking tools, the steady advance in the sophistication and effectiveness of attack technology, and the dire warnings of new and more destructive attacks.

Although there have been some individual agency improvements, our most recent analyses of audit and evaluation reports for the 24 major departments and agencies continued to highlight significant information security weaknesses that place a broad array of federal operations and assets at risk of fraud, misuse, and disruption. For example, resources, such as federal payments and collections, could be lost or stolen; sensitive information, such as taxpayer data, social security records, medical records, and proprietary business information, could be inappropriately disclosed, browsed, or copied for purposes of espionage or other types of

[5]Office of Management and Budget, *FY 2002 Report to Congress on Federal Government Information Security Reform*, May 16, 2003.

crime; and critical operations, such as those supporting national defense and emergency services, could be disrupted.

In its fiscal year 2002 GISRA report, DOD reported that the department has an aggressive information assurance (IA) posture and highlighted several initiatives to improve its IA program.[6] These initiatives included developing an overall strategy that identifies goals and objectives for the program and issuing numerous information security policy directives, instructions, manuals, and policy memorandums. Further, DOD's GISRA reporting highlighted other accomplishments, such as evaluating security controls for a sample of its networks. However, this reporting also showed that a number of challenges remain for the department in implementing both its policies and procedures and statutory information security requirements, as indicated by the material weaknesses it reported related to its IA capabilities, and its performance data that showed further efforts are needed to implement key requirements. For example, specific deficiencies related to DOD's material weaknesses included the need to decrease the time necessary for correcting reported weaknesses and to ensure that computer security policies are enforced and security capabilities are tested regularly. Also, performance data reported by DOD for a sample of its systems showed that further effort is needed by the department to report on all its systems and to fully implement key information security requirements, such as testing systems' information security controls and their contingency plans.

Our past work has shown that an important challenge agencies face in implementing an effective information security management program is ensuring that they have the appropriate management structures and processes in place to strategically manage information security, as well as to ensure the reliability of performance information. For example, disciplined processes can routinely provide the agency with timely, useful information for day-to-day management of information security. DOD has undertaken its Defense-wide Information Assurance Program (DIAP) to promote integrated, comprehensive, and consistent IA practices across the department and has recently issued both policy guidance and implementation instructions. However, as indicated by the Defense audit community's assessment of the DOD's fiscal year 2001 GISRA data, DOD does not have mechanisms in place for comprehensively measuring compliance with federal and Defense information security policies and

[6]IA refers to the range of information security activities and functions needed to protect DOD's information and systems.

ensuring that those policies are consistently practiced throughout the department.

Background

Dramatic increases in computer interconnectivity, especially in the use of the Internet, continue to revolutionize the way our government, our nation, and much of the world communicate and conduct business. The benefits have been enormous. Vast amounts of information are now literally at our fingertips, facilitating research on virtually every topic imaginable; financial and other business transactions can be executed almost instantaneously, often 24 hours a day; and electronic mail, Internet Web sites, and computer bulletin boards allow us to communicate quickly and easily with a virtually unlimited number of individuals and groups.

However, in addition to such benefits, this widespread interconnectivity poses significant risks to the government's and our nation's computer systems and, more important, to the critical operations and infrastructures they support. For example, telecommunications, power distribution, water supply, public health services, national defense (including the military's warfighting capability), law enforcement, government services, and emergency services all depend on the security of their computer operations. The speed and accessibility that create the enormous benefits of the computer age on the other hand, if not properly controlled, allow individuals and organizations to inexpensively eavesdrop on or interfere with these operations from remote locations for mischievous or malicious purposes, including fraud or sabotage. Table 1 summarizes the key threats to our nation's infrastructures, as observed by the Federal Bureau of Investigation (FBI).

Table 1: Threats to Critical Infrastructure Observed by the FBI

Threat	Description
Criminal groups	There is an increased use of cyber intrusions by criminal groups who attack systems for purposes of monetary gain.
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information gathering and espionage activities.
Hackers	Hackers sometimes crack into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use.
Hacktivists	Hacktivism refers to politically motivated attacks on publicly accessible Web pages or E-mail servers. These groups and individuals overload E-mail servers and hack into Web sites to send a political message.
Information warfare	Several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that, according to the Director of Central Intelligence,* can affect the daily lives of Americans across the country.
Insider threat	The disgruntled organization insider is a principal source of computer crimes. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a victim system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors.
Virus writers	Virus writers are posing an increasingly serious threat. Several destructive computer viruses and "worms" have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, and Code Red.

Source: Federal Bureau of Investigation unless otherwise indicated

*Prepared Statement of George J. Tenet, Director of Central Intelligence, before the Senate Select Committee on Intelligence, February 2, 2000.

Government officials remain concerned about attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence gathering, and acts of war. According to the FBI, terrorists, transnational criminals, and intelligence services are quickly becoming aware of and using information exploitation tools such as computer viruses, Trojan horses, worms, logic bombs, and eavesdropping sniffers

that can destroy, intercept, degrade the integrity of, or deny access to data.[1] In addition, the disgruntled organization insider is a significant threat, since these individuals often have knowledge that allows them to gain unrestricted access and inflict damage or steal assets without possessing a great deal of knowledge about computer intrusions. As greater amounts of money are transferred through computer systems, as more sensitive economic and commercial information is exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on commercially available information technology (IT), the likelihood increases that information attacks will threaten vital national interests.

As the number of individuals with computer skills has increased, more intrusion or "hacking" tools have become readily available and relatively easy to use. A hacker can literally download tools from the Internet and "point and click" to start an attack. Experts also agree that there has been a steady advance in the sophistication and effectiveness of attack technology. Intruders quickly develop attacks to exploit vulnerabilities discovered in products, use these attacks to compromise computers, and share them with other attackers. In addition, they can combine these attacks with other forms of technology to develop programs that automatically scan the network for vulnerable systems, attack them, compromise them, and use them to spread the attack even further.

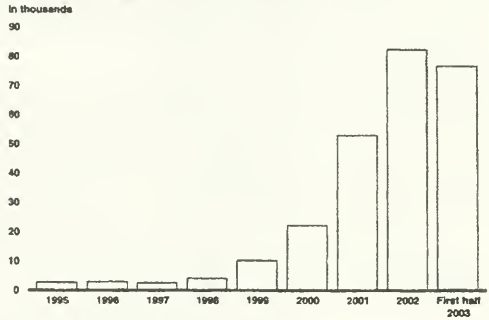
Along with these increasing threats, the number of computer security incidents reported to the CERT® Coordination Center[2] has also risen dramatically from 9,859 in 1999 to 82,094 in 2002 and 76,404 for just the first half of 2003. And these are only the reported attacks. The Director of CERT Centers stated that he estimates that as much as 80 percent of actual security incidents goes unreported, in most cases because (1) the organization was unable to recognize that its systems had been penetrated

[1] *Virus*: a program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the "infected" file is loaded into memory, allowing the virus to infect other files. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate. *Trojan horse*: a computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute. *Worm*: an independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate. *Logic bomb*: in programming, a form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer's employment. *Sniffer*: synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.

[2] The CERT® Coordination Center (CERT® CC) is a center of Internet security expertise at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

or there were no indications of penetration or attack or (2) the organization was reluctant to report. Figure 1 shows the number of incidents reported to the CERT Coordination Center from 1995 through the first half of 2003.

Figure 1: Information Security Incidents Reported to Carnegie-Mellon's CERT Coordination Center from 1995 through the First Half of 2003



Source: Carnegie-Mellon's CERT® Coordination Center.

According to the National Security Agency, foreign governments already have or are developing computer attack capabilities, and potential adversaries are developing a body of knowledge about U.S. systems and methods to attack these systems. Since the terrorist attacks of September 11, 2001, warnings of the potential for terrorist cyber attacks against our critical infrastructures have also increased. For example, in February 2002, the threat to these infrastructures was highlighted by the Special Advisor to the President for Cyberspace Security in a Senate briefing when he stated that although to date none of the traditional terrorists groups, such as al Qaeda, have used the Internet to launch a known assault on the United States' infrastructure, information on water systems was discovered on computers found in al Qaeda camps in Afghanistan.[9] Also, in

[9]"Administrative Oversight: Are We Ready for A CyberTerror Attack?" Testimony before the Senate Committee on the Judiciary, Subcommittee on Administrative Oversight and the Courts, by Richard A. Clarke, Special Advisor to the President for Cyberspace Security and Chairman of the President's Critical Infrastructure Protection Board (Feb. 13, 2002).

his February 2002 statement for the Senate Select Committee on Intelligence, the director of central intelligence discussed the possibility of cyber warfare attack by terrorists.[10] He stated that the September 11 attacks demonstrated the nation's dependence on critical infrastructure systems that rely on electronic and computer networks. Further, he noted that attacks of this nature would become an increasingly viable option for terrorists as they and other foreign adversaries become more familiar with these targets and the technologies required to attack them.

Since September 11, 2001, the critical link between cyberspace and physical space has been increasingly recognized. In his November 2002 congressional testimony, the Director of the CERT Centers at Carnegie-Mellon University noted that supervisory control and data acquisition (SCADA) systems and other forms of networked computer systems have been used for years to control power grids, gas and oil distribution pipelines, water treatment and distribution systems, hydroelectric and flood control dams, oil and chemical refineries, and other physical systems, and that these control systems are increasingly being connected to communications links and networks to reduce operational costs by supporting remote maintenance, remote control, and remote update functions.[11] These computer-controlled and network-connected systems are potential targets for individuals bent on causing massive disruption and physical damage, and the use of commercial, off-the-shelf technologies for these systems without adequate security enhancements can significantly limit available approaches to protection and may increase the number of potential attackers.

The risks posed by this increasing and evolving threat are demonstrated in reports of actual and potential attacks and disruptions. For example:

- On February 11, 2003, the National Infrastructure Protection Center (NIPC) issued an advisory to heighten the awareness of an increase in global hacking activities as a result of the increasing tensions between the United States and Iraq.[12] This advisory noted that during a time of increased international tension, illegal cyber activity often escalates, such

[10]Testimony of George J. Tenet, Director of Central Intelligence, before the Senate Select Committee on Intelligence, Feb. 6, 2002.
[11]Testimony of Richard D. Pethia, Director, CERT Centers, Software Engineering Institute, Carnegie Mellon University, before the House Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, November 19, 2002.
[12]National Infrastructure Protection Center, *National Infrastructure Protection Center Encourages Heightened Cyber Security as Iraq—U.S. Tensions Increase*, Advisory 03-002 (Washington, D.C.: Feb. 11, 2003).

as spamming, Web page defacements, and denial-of-service attacks. Further, this activity can originate within another country that is party to the tension, can be state sponsored or encouraged, or can come from domestic organizations or individuals independently. The advisory also stated that attacks may have one of several objectives, including political activism targeting Iraq or those sympathetic to Iraq by self-described "patriot" hackers, political activism or disruptive attacks targeting U.S. systems by those opposed to any potential conflict with Iraq, or even criminal activity masquerading or using the current crisis to further personal goals.

- According to a preliminary study coordinated by the Cooperative Association for Internet Data Analysis (CAIDA), on January 25, 2003, the SQL Slammer worm (also known as "Sapphire") infected more than 90 percent of vulnerable computers worldwide within 10 minutes of its release on the Internet, making it the fastest computer worm in history. As the study reports, exploiting a known vulnerability for which a patch has been available since July 2002, Slammer doubled in size every 8.5 seconds and achieved its full scanning rate (55 million scans per second) after about 3 minutes. It caused considerable harm through network outages and such unforeseen consequences as canceled airline flights and automated teller machine (ATM) failures. Further, the study emphasizes that the effects would likely have been more severe had Slammer carried a malicious payload, attacked a more widespread vulnerability, or targeted a more popular service.

- In November 2002, news reports indicated that a British computer administrator was indicted on charges that he broke into 92 U.S. computer networks in 14 states; these networks belonged to the Pentagon, private companies, and the National Aeronautics and Space Administration during the past year, causing some $900,000 in damage to computers. According to a Justice Department official, these attacks were one of the biggest hacks ever against the U.S. military. This official also said that the attacker used his home computer and automated software available on the Internet to scan tens of thousands of computers on U.S. military networks looking for ones that might suffer from flaws in Microsoft Corporation's Windows NT operating system software.

- On October 21, 2002, NIPC reported that all the 13 root-name servers that provide the primary roadmap for almost all Internet communications were targeted in a massive "distributed denial of service" attack. Seven of the servers failed to respond to legitimate network traffic, and two others failed intermittently during the attack. Because of safeguards, most Internet users experienced no slowdowns or outages.

- In July 2002, NIPC reported that the potential for compound cyber and physical attacks, referred to as "swarming attacks," is an emerging threat to the U.S. critical infrastructure.[12] As NIPC reports, the effects of a swarming attack include slowing or complicating the response to a physical attack. For example, cyber attacks can be used to delay the notification of emergency services and to deny the resources needed to manage the consequences of a physical attack. In addition, a swarming attack could be used to worsen the effects of a physical attack. For instance, a cyber attack on a natural gas distribution pipeline that opens safety valves and releases fuels or gas in the area of a planned physical attack could enhance the force of the physical attack. Consistent with this threat, NIPC also released an information bulletin in April 2002 warning against possible physical attacks on U.S. financial institutions by unspecified terrorists.[13]
- In August 2001, we reported to a subcommittee of the House Government Reform Committee that the attacks referred to as Code Red, Code Red II, and SirCam had affected millions of computer users, shut down Web sites, slowed Internet service, and disrupted business and government operations.[14] Then in September 2001, the Nimda worm appeared using some of the most significant attack profile aspects of Code Red II and 1999's infamous Melissa virus that allowed it to spread widely in a short amount of time. Security experts estimate that Code Red, Sircam, and Nimda have caused billions of dollars in damage.

Significant Weaknesses Persist in Federal Information Security

To better understand the risks facing DOD systems, it is useful to consider the overall status of information security for the federal government. Our analyses of information security at major federal agencies have shown that federal systems were not being adequately protected from computer-based threats, even though these systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations. For the past several years, we have analyzed audit results for

[12]National Infrastructure Protection Center, *Swarming Attacks: Infrastructure Attacks for Destruction and Disruption* (Washington, D.C.: July 2002).
[13]National Infrastructure Protection Center, *Possible Terrorism Targeting of US Financial System–Information Bulletin 02-003* (Washington, D.C.: Apr. 19, 2002).
[14]U.S. General Accounting Office, *Information Security: Code Red, Code Red II, and SirCam Attacks Highlight Need for Proactive Measures*, GAO-01-1073T (Washington, D.C.: Aug. 29, 2001).

24 of the largest federal agencies and found that all 24 had significant information security weaknesses.[16]

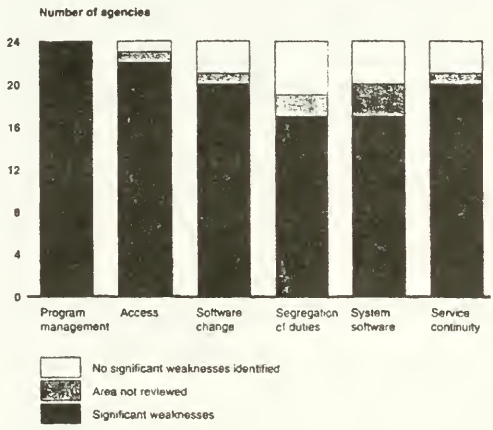
As reported in November 2002, our latest analyses of reports issued from October 2001 through October 2002, continued to show significant weaknesses in federal computer systems that put critical operations and assets at risk.[17] Weaknesses continued to be reported in each of the 24 agencies included in our review,[18] and they covered all six major areas of general controls—the policies, procedures, and technical controls that apply to all or a large segment of an entity's information systems and help ensure their proper operation. These six areas are (1) security program management, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented; (2) access controls, which ensure that only authorized individuals can read, alter, or delete data; (3) software development and change controls, which ensure that only authorized software programs are implemented; (4) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (5) operating systems controls, which protect sensitive programs that support multiple applications from tampering and misuse; and (6) service continuity, which ensures that computer-dependent operations experience no significant disruptions. Figure 2 illustrates the distribution of weaknesses for the six general control areas across the 24 agencies.

[16]U.S. General Accounting Office, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk*, GAO/AIMD-98-92 (Washington, D.C.: Sept. 23, 1998); *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies*, GAO/AIMD-00-295 (Washington, D.C.: Sept. 6, 2000); *Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets*, GAO-02-231T (Washington, D.C.: Nov. 9, 2001); and *Computer Security: Progress Made, but Critical Federal Operations and Assets Remain at Risk*, GAO-03-303T (Washington, D.C.: Nov. 19, 2002).

[17]GAO-03-303T.

[18]Does not include the Department of Homeland Security that was created by the Homeland Security Act in November 2002.

Figure 2: Computer Security Weaknesses at 24 Major Federal Agencies



Source: Audit reports issued October 2001 through October 2002.

Although our analyses showed that most agencies had significant weaknesses in these six control areas, as in past years' analyses, weaknesses were most often identified for security program management and access controls.

For security program management, we identified weaknesses for all 24 agencies in 2002—the same as reported for 2001, and compared to 21 of the 24 agencies (88 percent) in 2000. Security program management, which is fundamental to the appropriate selection and effectiveness of the other categories of controls, covers a range of activities related to understanding information security risks; selecting and implementing controls commensurate with risk; and ensuring that controls, once implemented, continue to operate effectively.

For access controls, we found weaknesses for 22 of 24 agencies (92 percent) in 2002 (no significant weaknesses were found for one agency, and access controls were not reviewed for another). This compares to access control weaknesses found in all 24 agencies for both 2000 and 2001. Weak access controls for sensitive data and systems make it possible for an individual or group to inappropriately modify, destroy, or disclose sensitive data or computer programs for purposes such as personal gain or sabotage. In today's increasingly interconnected computing environment, poor access controls can expose an agency's information and operations to attacks from remote locations all over the world by individuals with only minimal computer and telecommunications resources and expertise.

Our analyses also showed service-continuity-related weaknesses at 20 of the 24 agencies (83 percent) with no significant weaknesses found for 3 agencies (service continuity controls were not reviewed for another). This compares to 19 agencies with service continuity weaknesses found in 2001 and 20 agencies found in 2000. Service continuity controls are important in that they help ensure that when unexpected events occur, critical operations will continue without undue interruption and that crucial, sensitive data are protected. If service continuity controls are inadequate, an agency can lose the capability to process, retrieve, and protect electronically maintained information, which can significantly affect an agency's ability to accomplish its mission. Further, such controls are particularly important in the wake of the terrorist attacks of September 11, 2001.

These analyses of information security at federal agencies also showed that the scope of audit work performed has continued to expand to more fully cover all six major areas of general controls at each agency. Not surprisingly, this has led to the identification of additional areas of weakness at some agencies. These increases in reported weaknesses do not necessarily mean that information security at federal agencies is getting worse. They more likely indicate that information security weaknesses are becoming more fully understood—an important step toward addressing the overall problem. Nevertheless, the results leave no doubt that serious, pervasive weaknesses persist. As auditors increase their proficiency and the body of audit evidence expands, it is probable that additional significant deficiencies will be identified.

Most of the audits represented in figure 2 were performed as part of financial statement audits. At some agencies with primarily financial missions, such as the Department of the Treasury and the Social Security Administration, these audits covered the bulk of mission-related operations. However, at agencies whose missions are primarily

nonfinancial, such as DOD and the Department of Justice, the audits may provide a less complete picture of the agency's overall security posture because the audit objectives focused on the financial statements and did not include evaluations of individual systems supporting nonfinancial operations. However, in response to congressional interest, beginning in fiscal year 1999, we expanded our audit focus to cover a wider range of nonfinancial operations—a trend we expect to continue. Audit coverage for nonfinancial systems has also increased as agencies and their IGs reviewed and evaluated their information security programs as required by GISRA.

To fully understand the significance of the weaknesses we identified, it is necessary to link them to the risks they present to federal operations and assets. Virtually all federal operations are supported by automated systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Hence, the degree of risk caused by security weaknesses is extremely high.

The weaknesses identified place a broad array of federal operations and assets at risk. For example,

- resources, such as federal payments and collections, could be lost or stolen;
- computer resources could be used for unauthorized purposes or to launch attacks on others;
- sensitive information, such as taxpayer data, social security records, medical records, and proprietary business information, could be inappropriately disclosed, browsed, or copied for purposes of espionage or other types of crime;
- critical operations, such as those supporting national defense and emergency services, could be disrupted;
- data could be modified or destroyed for purposes of fraud or disruption; and
- agency missions could be undermined by embarrassing incidents that result in diminished confidence in their ability to conduct operations and fulfill their fiduciary responsibilities.

Congress Consolidates and Strengthens Federal Information Security Requirements

Concerned with accounts of attacks on commercial systems via the Internet and reports of significant weaknesses in federal computer systems that make them vulnerable to attack, on October 30, 2000, Congress enacted GISRA, which was signed into law and became effective November 29, 2000, for a period of 2 years. GISRA supplemented information security requirements established in the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, and the Clinger-Cohen Act of 1996 and was consistent with existing information security guidance issued by OMB[19] and the National Institute of Standards and Technology (NIST),[20] as well as audit and best practice guidance issued by GAO.[21]

Most importantly, however, GISRA consolidated these separate requirements and guidance into an overall framework for managing information security and established new annual review, independent evaluation, and reporting requirements to help ensure agency implementation and both OMB and congressional oversight. GISRA assigned specific responsibilities to OMB, agency heads and CIOs, and IGs. OMB was responsible for establishing and overseeing policies, standards, and guidelines for information security. This included the authority to approve agency information security programs, but delegated OMB's responsibilities regarding national security systems to national security agencies. OMB was also required to submit an annual report to the Congress summarizing results of agencies' independent evaluations of their information security programs. OMB released its fiscal year 2001 report in February 2002 and its fiscal year 2002 report in May 2003.

GISRA required each agency, including national security agencies, to establish an agencywide risk-based information security program to be overseen by the agency CIO and ensure that information security is practiced throughout the life cycle of each agency system. Specifically, this program was to include

[19]Primarily OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," February 1996.
[20]Numerous publications made available at http://www.itl.nist.gov/ including National Institute of Standards and Technology, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, NIST Special Publication 800-14, September 1996.
[21]U.S. General Accounting Office, *Federal Information System Controls Manual, Volume I—Financial Statement Audits*, GAO/AIMD-12.19.6 (Washington, D.C.: January 1999); *Information Security Management: Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

- periodic risk assessments that consider internal and external threats to the integrity, confidentiality, and availability of systems, and to data supporting critical operations and assets;
- the development and implementation of risk-based, cost-effective policies and procedures to provide security protections for information collected or maintained by or for the agency;
- training on security responsibilities for information security personnel and on security awareness for agency personnel;
- periodic management testing and evaluation of the effectiveness of policies, procedures, controls, and techniques;
- a process for identifying and remediating any significant deficiencies;
- procedures for detecting, reporting, and responding to security incidents; and
- an annual program review by agency program officials.

In addition to the responsibilities listed above, GISRA required each agency to have an annual independent evaluation of its information security program and practices, including control testing and compliance assessment. The evaluations of non-national-security systems were to be performed by the agency IG or an independent evaluator, and the results of these evaluations were to be reported to OMB. For the evaluation of national security systems, special provisions included having national security agencies designate evaluators, restricting the reporting of evaluation results, and having the IG or an independent evaluator perform an audit of the independent evaluation. For national security systems, only the results of each audit of an evaluation are to be reported to OMB.

With GISRA expiring on November 29, 2002, on December 17, 2002, FISMA was enacted as title III of the E-Government Act of 2002 to permanently authorize and strengthen the information security program, evaluation, and reporting requirements established by GISRA. Among other things, FISMA also requires NIST to develop, for systems other than national security systems, (1) standards to be used by all agencies to categorize all their information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels; (2) guidelines recommending the types of information and information systems to be included in each category; and (3) minimum information security requirements for information and information systems in each category. In addition, FISMA requires each agency to

develop, maintain, and annually update an inventory of major information systems (including major national security systems) operated by the agency or under its control. This inventory is also to include an identification of the interfaces between each system and all other systems or networks, including those not operated by or under the control of the agency.

DOD Highlights Initiatives, But Also Reports Weaknesses

DOD has undertaken several initiatives to improve its information security, including the development of an overall IA strategy and the issuance of information security policy and guidance.[2] However, information that DOD's CIO and IG submitted for fiscal year 2002 GISRA reporting showed that a number of challenges remain for the department in implementing both its policies and procedures and the statutory information security requirements. These challenges are indicated by the material weaknesses DOD reported related to its IA capabilities and its performance data, which showed that further efforts are needed to implement key requirements.

DOD Efforts to Improve Information Security

Overall, the DOD CIO reported in its fiscal year 2002 GISRA report that the department has an aggressive IA posture and highlighted several initiatives to improve its IA program. In particular, DOD has developed an overall IA strategic plan to define the department's goals and objectives and to provide a consistent departmentwide approach to information assurance. Further, according to a DOD official, DOD is aligning its strategic initiatives to objectives in this plan and is developing milestones and performance measures to gauge success.

Specific plan goals include:

- protecting information to ensure that all information has a level of trust commensurate with mission needs;
- defending systems and networks to ensure that no access is uncontrolled and that all systems and networks are capable of self-defense; and

[2]IA refers to the range of information security activities and functions needed to protect DOD's information and systems.

- creating an IA-empowered workforce that is trained, highly skilled, knowledgeable, and aware of its role in assuring information.

The plan also identified specific objectives for each goal. For example, to meet the goal of protecting information to ensure that all information has a level of trust commensurate with mission needs, DOD identified objectives including defining data protection requirements, applying protection mechanisms across the enterprise, and developing robust mechanisms that protect information. In addition, DOD has developed a complementary implementation mechanism for IA known as Defense in Depth that uses a multilayered approach with defense mechanisms on successive layers at multiple locations.

Other initiatives highlighted in the DOD CIO's fiscal year 2002 GISRA report included establishing a number of senior-level bodies that discuss, brief, and shape the future of IA efforts—such as the CIO Executive Board and the Military Communications-Electronics Board—and issuing information security policy directives, instructions, manuals, and policy memorandums.

During fiscal year 2003, DOD has continued its efforts to implement IA departmentwide by issuing additional policy and guidance. Specifically, in October 2002, it issued DOD Directive 8500.1 to establish policy and assign responsibility for IA management.[23] Further, in February 2003, DOD issued DOD Instruction 8500.2, which prescribes a framework for implementing the department's IA program and establishes baseline levels of assurance for information systems.[24]

Material Weaknesses Identified By DOD

DOD reported eight material weaknesses in fiscal year 2002 for which it said it is undertaking aggressive action to improve and expand its IA capabilities. The actions DOD identified to address the eight deficiencies are:

- completing the implementation of the Information Assurance Vulnerability Alert process to all services and agencies;

[23]Department of Defense Directive Number 8500.1, *Information Assurance (IA)* (Oct. 24, 2002).
[24]Department of Defense Instruction Number 8500.2, *Information Assurance (IA) Implementation* (Feb. 6, 2003).

- ensuring that effective computer security policies and procedures are distributed in a timely manner;
- improving DOD business processes to ensure that all systems are protected;
- decreasing the time necessary for correction of reported weaknesses;
- ensuring that computer security policies are enforced and security capabilities are tested regularly;
- ensuring that training is conducted for all network personnel (this includes awareness training for all personnel to specific network defense training for system and network administrators);
- increasing access security through the use of electronic tokens; and
- increasing security through certificates (for authentication and nonrepudiation).

DOD Reports Show Further Efforts Needed to Implement Key Information Security Requirements

OMB's fiscal year 2002 reporting instructions included new high-level management performance measures that the agencies and IGs were required to use to report on agency officials' performance, such as the number and percentage of systems that have been assessed for risk and that have an up-to-date security plan. In addition, OMB's reporting instructions for fiscal year 2002 stated that agencies were expected to review all systems annually.[25] OMB explained that GISRA requires senior agency program officials to review each security program for effectiveness at least annually, and that the purpose of the security programs discussed in GISRA is to ensure the protection of the systems and data covered by the program. Thus, a review of each system is essential to determine the program's effectiveness, and only the depth and breadth of such system reviews are flexible.

DOD reported data for most performance measures as required. However, as agreed with OMB, DOD reported these data for only a sample of its systems and networks rather than for all systems. As a result, DOD cannot ensure that these performance measures accurately reflect the information

[25]Office of Management and Budget, "Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Action and Milestones," Memorandum for Heads of Executive Departments and Agencies, Mitchell E. Daniels, Jr., M-02-09, July 2, 2002.

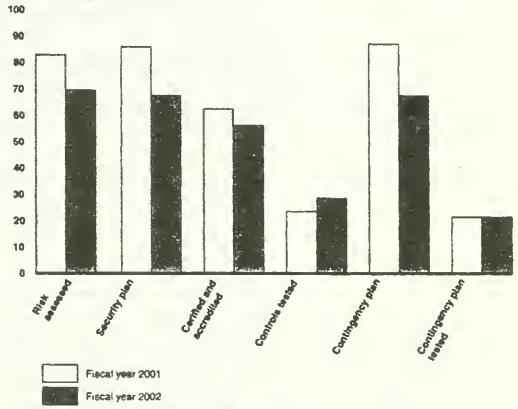
security status of its thousands of systems or that potential weaknesses for all systems have been identified for correction. Further, reporting on only a sample of systems limited the usefulness of OMB's analysis of the governmentwide status of IT security reported in its fiscal year 2002 report to the Congress, which considered data for only DOD's sample of systems in measuring the overall progress by 24 large agencies.

DOD indicated in its report that because of its size and complexity, the collection of specific metrics required sizable lead time to allow for the collection and approval process by each military service and agency. For this reason, DOD focused its fiscal year 2002 GISRA efforts on (1) a sample of 366 of its networks (241 unclassified and 125 classified) and (2) a sample of 155 systems that were selected from the sample of systems used for DOD's fiscal year 2001 GISRA review. Although DOD reported performance measure data for both the sample of networks and the sample of systems, OMB's provided comparative results in its report to Congress primarily for the sample of 155 systems. However, as discussed later in this statement, DOD did report that 96 percent of its sample of networks was certified and accredited.

OMB's fiscal year 2002 GISRA report to the Congress summarized both agency and overall results for certain key measures for 24 large federal agencies. Subject to the limitation of DOD's data, figure 3 summarizes DOD results for six of these measures for the 155 systems and shows that most of these measures actually decreased from fiscal year 2001 to fiscal year 2002. DOD attributed the decreases to inaccuracies in the fiscal year 2001 data. Discussion of these and other measures follow figure 3 and include a comparison of DOD results to results for other agencies as presented in our recent testimonies before a subcommittee of the House Government Reform Committee.[8]

[8]U.S. General Accounting Office, *Information Security: Progress Made, But Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures*, GAO-03-564T (Washington, D.C.: Apr. 8, 2003), and *Information Security: Continued Efforts Needed to Fully Implement Statutory Requirements*, GAO-03-852T (Washington, D.C.: Jun. 24, 2003).

Figure 3: Reported Results for Selected DOD Information Security Performance Measures



Source: OMB FY 2002 Report to Congress on Federal Information Security Reform, and GAO (analysis).

Systems Assessed for Risk

Agencies are required to perform periodic threat-based risk assessments for systems and data. Risk assessments are an essential element of risk management and overall security program management and, as our best practice work has shown, are an integral part of the management processes of leading organizations.[27] Risk assessments help ensure that the greatest risks have been identified and addressed, increase the understanding of risk, and provide support for needed controls. Our reviews of federal agencies, however, frequently show deficiencies related to assessing risk, such as security plans for major systems that are not

[27]GAO/AIMD-98-68.

developed on the basis of risk. As a result, the agencies had accepted an unknown level of risk by default rather than consciously deciding what level of risk was tolerable.

OMB's performance measure for this requirement mandated that agencies report the number and percentage of their systems that have been assessed for risk during fiscal year 2001 and fiscal year 2002. DOD reported that for its sample of 155 systems, 68 percent (106) had risk assessments for fiscal year 2002 as compared to 81 percent (125) for fiscal year 2001—a decrease of 13 percentage points. In comparison, our overall analyses of reporting for this measure for all 24 agencies (including DOD) showed that for fiscal year 2002, 11 agencies reported that they had assessed risk for 90 to 100 percent of their systems, and of the remaining 13, 8 reported less than 50 percent.

Systems With Up-to-Date Security Plans

An agency head is required to ensure that the agency's information security plans are practiced throughout the life cycle of each agency system. In its reporting instructions, OMB required agencies to report whether the agency head had taken specific and direct actions to oversee that program officials and the CIO are ensuring that security plans are up to date and practiced throughout the life cycle of each system. Agencies also had to report the number and percentage of systems that had an up-to-date security plan.

Regarding the status of agencies' security plans, DOD reported that for its sample of 155 systems, 66 percent (103) had up-to-date security plans for fiscal year 2002—a decrease from the 84 percent (130) reported for fiscal year 2001. In comparison, our overall analysis for all 24 agencies showed that for fiscal year 2002, 7 agencies reported that they up-to-date security plans for 90 to 100 percent of their systems, and of the remaining 17 agencies, 9 reported up-to-date security plans for less than 50 percent of their systems.

Systems Certified and Accredited

As one of its performance measures for agency program official responsibilities, OMB required agencies to report the number and percentage of systems that have been authorized for processing following certification and accreditation. *Certification* is the comprehensive evaluation of the technical and nontechnical security controls of an IT system to support the accreditation process that establishes the extent to

which a particular design and implementation meets a set of specified security requirements. Certification provides the necessary information to a management official to formally declare that an IT system is approved to operate at an acceptable level of risk. *Accreditation* is the authorization of an IT system to process, store, or transmit information, granted by a management official that provides a form of quality control and challenges managers and technical staff to find the best fit for security, given technical constraints, operational constraints, and mission requirements. The accreditation decision is based on the implementation of an agreed upon set of management, operational, and technical controls, and by accrediting the system, the management office accepts the risk associated with it.

DOD has established a standard departmentwide process, set of activities, general tasks, and a management structure to certify and accredit information systems and maintain the IA and security posture throughout the life cycle of the system. A companion manual, the *DOD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual*, provides implementation guidance to standardize the certification and accreditation process throughout DOD.[25] The DOD CIO reported that the department is implementing the DITSCAP process, but realizes the actual process is complex, lengthy, and costly; and several internal agencies are exploring efforts to streamline DITSCAP.

DOD reported that for fiscal year 2002, 55 percent (85) of its sample of 155 systems was authorized for processing following certification and accreditation—a decrease from the 61 percent (95) reported for fiscal year 2001. For this particular measure, DOD also reported that in fiscal year 2002, 96 percent (352) of its 366-network sample was certified and accredited to operate. In comparison, our overall analysis for all 24 agencies showed that for fiscal year 2002, only 3 agencies reported that 90 to 100 percent of their systems were authorized for processing following certification and accreditation, and of the remaining 21 agencies, 13 reported that less than 50 percent of their systems were authorized, including 3 that reported that none were authorized.

According to the DOD IG's fiscal year 2002 GISRA report, the certification and accreditation data reported by the department for fiscal year 2001 included systems that were certified and accredited either under the DITSCAP or another process. In addition, in analyzing a sample of the

[25]Department of Defense, *DOD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual*, DOD 8510.1-M (July 31, 2000).

systems used for the department's fiscal year 2001 GISRA reporting, the IG found the certification and accreditation status for some systems was incorrectly reported.

Security Control Testing and Evaluation

An agency head is responsible for ensuring that the appropriate agency officials evaluate the effectiveness of the information security program, including testing controls. Further, the agencywide information security program is to include periodic management testing and evaluation of the effectiveness of information security policies and procedures. Periodically evaluating the effectiveness of security policies and controls and acting to address any identified weaknesses are fundamental activities that allow an organization to manage its information security risks cost-effectively, rather than reacting to individual problems ad hoc only after a violation has been detected or an audit finding has been reported. Further, management control testing and evaluation as part of the program reviews can supplement control testing and evaluation in IG and our audits to help provide a more complete picture of the agencies' security postures.

As a performance measure for this requirement, OMB required agencies to report the number and percentage of systems for which security controls have been tested and evaluated during fiscal years 2001 and 2002. DOD reported that for fiscal year 2002, it had tested and evaluated controls for only 28 percent (43) of the 155-system sample—a slight increase from the 23 percent (35) reported for fiscal year 2001. In comparison, our overall analysis for all 24 agencies showed that for fiscal year 2002, only 4 agencies reported they had tested and evaluated controls for 90 to 100 percent of their systems, and of the remaining 20 agencies, 10 reported less than 50 percent.

System Contingency Plans

Contingency plans provide specific instructions for restoring critical systems, including such items as arrangements for alternative processing facilities, in case the usual facilities are significantly damaged or cannot be accessed. These plans and procedures help to ensure that critical operations can continue when unexpected events occur, such as temporary power failure, accidental loss of files, or major disaster. Contingency plans should also identify which operations and supporting resources are critical and need to be restored first and should be tested to identify their weaknesses. Without such plans, agencies have inadequate

assurance that they can recover operational capability in a timely, orderly manner after a disruptive attack.

As another of its performance measures, OMB required agencies to report the number and percentage of systems for which contingency plans had been prepared and had been tested in the past year. DOD reported that of its 155-system sample, 66 percent (103) of its systems had contingency plans for fiscal year 2002—a decrease from the 85 percent (131) reported for fiscal year 2001. However, more significantly, DOD also reported that for fiscal year 2002, only 21 percent (32) of its sample of systems had contingency plans that had been tested within the past year. In comparison, our overall analysis for all 24 agencies showed that for fiscal year 2002, only 2 agencies reported they had tested contingency plans for 90 to 100 percent of their systems, and of the remaining 22 agencies, 20 reported less than 50 percent, including 1 that reported none had been tested.

Incident-Handling Capabilities

Agencies are required to implement procedures for detecting, reporting, and responding to security incidents. Although even strong controls may not block all intrusions and misuse, organizations can reduce the risks associated with such events if they promptly take steps to detect intrusions and misuse before significant damage can be done. In addition, accounting for and analyzing security problems and incidents are effective ways for an organization to gain a better understanding of threats to its information and of the cost of its security-related problems. Such analyses can also pinpoint vulnerabilities that need to be addressed to help ensure that they will not be exploited again. In this regard, problem and incident reports can provide valuable input for risk assessments, help in prioritizing security improvement efforts, and be used to illustrate risks and related trends in reports to senior management.

In March 2001, we reported that over the past several years, DOD had established incident response capabilities for the military services and enhanced computer defensive capabilities across the department.[28] However, we also identified six areas in which DOD faced challenges in improving its incident response capabilities, including (1) coordinating resource planning and priorities for incident response across the

[28]U.S. General Accounting Office, *Information Security: Challenges to Improving DOD's Incident Response Capabilities*, GAO-01-341 (Washington, D.C.: Mar. 29, 2001).

department; (2) integrating critical data from systems, sensors, and other devices to better monitor cyber events and attacks; (3) establishing a departmentwide process to periodically and systematically review systems and networks on a priority basis for security weaknesses; (4) ensuring that components across the department consistently and fully report compliance with vulnerability alerts; (5) improving the coordination and suitability of component-level incident response actions; and (6) developing departmentwide performance measures to assess incident response capabilities and thus better ensure mission readiness. Although DOD was aware of these challenges and had undertaken some initiatives to address them, the initiatives were not complete at the time of our review. We recommended that DOD act to address these challenges to better protect its systems and networks from cyber threats and attacks. Currently, DOD reports that it has made progress in addressing many of these challenges.

For fiscal year 2002 GISRA reporting, OMB required agencies to report several performance measures related to detecting, reporting, and responding to security incidents. These included the number of agency components with an incident-handling and response capability, whether the agency and its major components share incident information with the Federal Computer Incident Response Center (FedCIRC)[26] in a timely manner, and the numbers of incidents reported. OMB also required that agencies report on how they confirmed that patches have been tested and installed in a timely manner.

In its fiscal year 2002 GISRA report, the DOD CIO reported that essentially all its components have an incident handling and response capability and that DOD has made significant progress in developing its computer network defense capabilities, including the January 2001 issuance of DOD Directive O-8530.1, "Computer Network Defense," which established computer network defense policy, definition, and department responsibilities. The CIO also reported that through its computer network defense capabilities, DOD could monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks. In addition, the CIO reported that each of the major military services has a robust computer emergency response team (CERT) and integrated network operations centers. Further, the report states that the DOD CERT works closely with FedCIRC on all incidents within the .gov

[26]FedCIRC, formerly within the General Services Administration and now part of the Department of Homeland Security, was established to provide a central focal point for incident reporting, handling, prevention and recognition for the federal government.

Internet domain and, along with other service and agency CERTs, shares incident information with FedCIRC within 10 minutes to 48 hours depending on the seriousness of the incident. The Joint Task Force for Computer Network Operations and the DOD CERT take responsibility for incidents within the .mil Internet domain.

In comparison to DOD, our analyses of agencies' fiscal year 2002 GISRA reports showed that most agencies reported that they have established incident-response capabilities. For example, 12 agencies reported that for fiscal year 2002, 90 percent or more of their components had incident handling and response capabilities, and 8 others reported that they provided these capabilities to components through a central point within the agency.

Security Training for Employees and Contractors

Agencies are required to provide training on security awareness for agency personnel and on security responsibilities for information security personnel. Our studies of best practices at leading organizations have shown that such organizations took steps to ensure that personnel involved in various aspects of their information security programs had the skills and knowledge they needed. They also recognized that staff expertise had to be frequently updated to keep abreast of ongoing changes in threats, vulnerabilities, software, security techniques, and security monitoring tools.

Among the performance measures for these requirements, OMB mandated that agencies report the number and percentage of employees—including contractors—who received security training during fiscal years 2001 and 2002, and the number of employees with significant security responsibilities who received specialized training. In response to these measures, the DOD CIO reported that it provides departmentwide, component-level security training and periodic updates for all employees, but that actual numbers and the percentage of agency employees who received security training in fiscal year 2002 were not available at the time of its report. For employees with significant security responsibilities, the CIO reported that specialized security and technical training is provided to persons empowered to audit, alter, or affect the intended behavior or content of an IT system, such as system/network administrators and information systems security officers. Additional training is also provided for others, such as CERT members, computer crime investigators, and Web masters/site managers. However, performance measure data reported for employees with significant security responsibilities showed that of

39,783 such employees, 42 percent (16,812) received specialized training in fiscal year 2002—a decrease of 9 percentage points from the 51 percent reported for fiscal year 2001.

In comparison with other major federal agencies, for specialized training for employees with significant security responsibilities, our analyses showed that 12 agencies reported 50 percent or more of their employees with significant security responsibilities had received specialized training for fiscal year 2002, with 5 of these reporting 90 percent or more. Of the remaining 12 agencies, 9 including DOD reported that less than half of such employees received specialized training, 1 reported that none had received such training, and 2 did not provide sufficient data for this measure.

Security of Contractor-Provided Services

Agencies are required to develop and implement risk-based, cost-effective policies and procedures to provide security protection for information collected or maintained by or for the agency. In its fiscal year 2001 GISRA report to the Congress, OMB identified poor security for contractor-provided services as a common weakness, and for fiscal year 2002 reporting, included performance measures to help indicate whether the agency program officials and CIO used appropriate methods, such as audits and inspections, to ensure that service provided by a contractor are adequately secure and meet security requirements.

For fiscal year 2002 GISRA, the DOD CIO reported that there was insufficient time and resources to accurately collect requested performance measure data. The CIO also reported that execution and verification of contractor services and facilities are managed at the subagency levels, and that agency program officials use audits or inspections to ensure that contractor-provided services are adequately secure and meet statutory information security requirements, OMB policy, and NIST guidance. The DOD IG did not review the status of contractor-provided services for compliance with GISRA, but did identify several reports issued from August 2001 to July 2002 by military service audit agencies that discussed weaknesses in background investigations. Screening of contractor or subcontractor employees as a condition for physical or computer systems access is a recommended safeguard, and depending on the program or system criticality or information sensitivity, can range from minimal checks to complete background investigations.

Challenges to Implementing an Effective Information Security Management Program

As previously discussed, our past analyses of audit results for 24 of the largest federal agencies showed that all 24 had significant weaknesses in security program management, which covers a range of activities related to understanding information security risks; selecting and implementing controls commensurate with risk; and ensuring that controls, once implemented, continue to operate effectively.[31] Establishing a strong security management program requires that agencies take a comprehensive approach that involves both (1) senior agency program managers who understand which aspects of their missions are the most critical and sensitive and (2) technical experts who know the agencies' systems and can suggest appropriate technical security control techniques. We studied the practices of organizations with superior security programs and summarized our findings in a May 1998 executive guide entitled *Information Security Management: Learning From Leading Organizations.*[32] Our study found that these organizations managed their information security risks through a cycle of risk management activities. These activities, which are now among the federal government's statutory information security requirements, included

- assessing risks and determining protection needs, selecting and implementing cost-effective policies and controls to meet those needs,
- promoting awareness of policies and controls and of the risks that prompted their adoption among those responsible for complying with them, and
- implementing a program of routine tests and examinations for evaluating the effectiveness of policies and related controls and reporting the resulting conclusions to those who can take appropriate corrective action.

Although GISRA reporting provided performance information on these areas, it is important for agencies to ensure that they have the appropriate management structures and processes in place to strategically manage information security, as well as ensure the reliability of performance information. For example, disciplined processes can routinely provide the agency with timely, useful information for day-to-day management of

[31]GAO-02-231T and GAO-03-303T.

[32]GAO/AIMD-98-68.

information security. Also, developing management strategies that identify specific actions, time frames, and required resources may help to significantly improve performance.

In January 1998, DOD announced its plans for DIAP—a program intended to promote integrated, comprehensive, and consistent IA practices across the department. In February 1999, the department issued an approved implementation plan, which described, at a high level, the program's goals, objectives, and organizational structure, and confirmed its responsibility for the planning, coordination, integration, and oversight of Defense-wide computer security initiatives.

In March 2001, we reported that DIAP had made progress in addressing IA, but that the department had not yet met its goals for promoting integrated, comprehensive, and consistent practices across DOD.[5] The program's progress was limited by weaknesses in its management framework and unmet staffing expectations. DOD had not established a performance-based management framework for IA improvement at the department level. As a result, DOD was unable to accurately determine the status of IA across the department, the progress of its improvement efforts, or the effectiveness of its initiatives. Also, understaffing kept the program from fulfilling its central role in planning, monitoring, coordinating, and integrating Defense-wide IA activities, and changes in the composition and authority of other key organizations interacting with DIAP left it without a consistent and fully supportive environment for its operations. We concluded that achieving this program's vision for information superiority would require the commitment of DOD to proven IA management practices. To improve progress toward the department's goals, we made recommendations to the Secretary of Defense in the areas of component commitments to DIAP and executive-level monitoring of the program. We also recommended that the DOD CIO institute performance-based management of DIAP through a defined budget and performance objectives, and that the program manager take steps to address the program's unmet goals.

DOD has made some progress in addressing our previous recommendations and, as discussed previously, during fiscal year 2003, DOD issued guidance to establish policy and assign responsibility for IA management and to prescribe a framework for implementing the department's IA program and establish baseline levels of assurance for

[5]U.S. General Accounting Office, *Information Security: Progress and Challenges to an Effective Defense-wide Information Assurance Program*, GAO-01-307 (Washington, D.C.: Mar. 30, 2001).

information systems. Despite such steps, OMB reported in its fiscal year 2002 report to the Congress that the overall results of the Defense audit community's assessment of the DOD fiscal year 2001 GISRA reporting reinforced the position that DOD does not have mechanisms in place for comprehensively measuring compliance with federal and Defense information security policies and ensuring that those policies are consistently practiced throughout the department.

In summary, DOD has taken positive steps through its policy and guidance to establish information security as a priority for the department. However, as its fiscal year 2002 GISRA reporting showed, further effort is needed to fully implement statutory information security requirements departmentwide and to expand future FISMA reporting to all systems. Significant improvement will likely require DOD to establish departmentwide processes that routinely provide information for day-to-day management of information security and to develop management strategies that identify specific actions, time frames, and required resources. With the first agency reporting under FISMA due in September 2003, updated information on the status of DOD's efforts will be available for continued congressional oversight.

Mr. Chairman, this concludes my written testimony. I would be pleased to answer any questions that you or other members of the Subcommittee may have at this time. If you should have any questions about this testimony, please contact me at (202) 512-3317. I can also be reached by E-mail at daceyr@gao.gov.

(310505)

Statement of Scott Charney

Chief Security Strategist, Microsoft Corporation

Testimony Before the
Subcommittee on Terrorism, Unconventional Threats, and Capabilities
House Armed Services Committee
U.S. House of Representatives

Hearing on "Cyber Terrorism: The New Asymmetric Threat"

July 24, 2003

Statement of Scott Charney
Chief Security Strategist
Microsoft Corporation

Before the
Subcommittee on Terrorism, Unconventional Threats, and Capabilities
House Armed Services Committee
U.S. House of Representatives

Hearing on "Cyber Terrorism: The New Asymmetric Threat"

July 24, 2003

Chairman Saxton, Ranking Member Meehan, and Members of the Subcommittee: My name is Scott Charney, and I am Microsoft's Chief Security Strategist. I want to thank you for the opportunity to appear today to provide our views on cybersecurity and cyberterrorism. I oversee the development of strategies to implement our long-term Trustworthy Computing initiative and to create more secure software, services, and infrastructures. My goal is to reduce the number of successful computer attacks and increase the confidence of all IT users. Not only do I work on our products and services, but I also collaborate with others in the computer industry, the U.S. Department of Defense (DoD), and across the government to make computing more secure for all users.

Earlier in my career, I served as chief of the Computer Crime and Intellectual Property Section (CCIPS) in the Criminal Division of the U.S. Department of Justice, where I helped prosecute nearly every major hacker case in the United States from 1991 to 1999.

At Microsoft, we are deeply committed to cybersecurity, and we recognize our responsibility to make our products ever more secure. We are at the forefront of industry efforts to enhance the security of computer programs, products and networks, and to

better protect our critical information infrastructures. We also work closely with our partners in industry, government agencies, and law enforcement around the world to identify security threats to computer networks, share best practices, improve our coordinated responses to security breaches, and prevent computer attacks from happening in the first place. These efforts accelerated after September 11th and crystallized when Bill Gates launched our Trustworthy Computing initiative in January 2002.

Today, I want to describe the ways in which we believe industry and government are working in partnership to promote cybersecurity. First, I will discuss our commitment to Trustworthy Computing and how it is reflected in our software, our development processes, and our research and development efforts. Second, I will discuss our efforts to join forces with others within the industry to help guard against cyber threats and enhance security for governments, businesses, and consumers. Third, I will address our engagement on cyberterrorism and other cybersecurity issues with DoD. Fourth, I will describe some of my personal experiences with DoD's efforts to protect against and to respond to cyberattacks, and how these experiences may inform my work in support of DoD missions. Finally, I will offer a few recommendations; steps the government can take to enhance cybersecurity.

The work of this Subcommittee on cybersecurity, terrorism, and unconventional threats is crucial to protecting and enhancing DoD's abilities to prevent and respond to cyberattacks that may impair DoD's capabilities and readiness. We deeply appreciate the Subcommittee's interest in protecting the Defense Department's civilian and uniformed personnel, and the computer systems upon which they rely, from the determined and unceasing efforts of cybercriminals to inflict substantial damage and disruption. We are

committed to working with DoD, the Congress, and industry partners to reduce DoD's vulnerabilities to cyberattacks, including cyberterrorism, and to strengthen DoD's capabilities to prevent, identify, characterize, respond to, and deter attacks.

I. Trustworthy Computing Overview

Trustworthy Computing is our top priority and involves every aspect of the company. The focus of Trustworthy Computing is on four key pillars: security, privacy, reliability, and business integrity. The goals of each pillar are not hard to define. Security involves designing programs and systems that are resilient to attack so that the confidentiality, integrity, and availability of data and systems is protected. As for privacy, the goal is to give individuals greater control over their personal data and ensure, as with the efforts against spam, their right to be left alone. Reliability means creating software and systems that are dependable, available when needed, and perform at expected levels. Finally business integrity means acting with honesty and integrity at all times, and engaging openly and transparently with customers.

The security pillar of Trustworthy Computing is most relevant for today's hearing. Under this pillar, we are working to create products and services for DoD and all of its customers that are Secure by Design, Secure by Default, and Secure in Deployment, and to communicate openly about our efforts.

- "Secure by Design" means two things: writing more secure code and architecting more secure software and services. Writing more secure code means using a redesigned software development process that includes training for developers, code reviews, automated testing of code, threat modeling, and penetration testing. Architecting more secure software and services means

designing software with built-in and aware security, so that security imposes less of a burden on users and security features are actually used.

- "Secure by Default" means that computer software is secure out of the box, whether it is in a home environment or an IT department. It means shipping software to customers in a locked-down configuration with many features turned off, allowing customers to configure their systems appropriately, in a more secure way, for their unique environment.
- "Secure in Deployment" means making it easier for consumers, commercial and government users, and IT professionals to maintain the security of their systems. We have a role in helping computer users help themselves by creating easy-to-use security technology. Due to the complexity of software and the different environments in which it may be placed, software will never be perfectly secure while also being functional. Accordingly, "secure in deployment" means providing training on threats and how to manage them; offering guidance on how to deploy, configure, and maintain software securely; and providing better security tools for users, so that when a vulnerability is discovered, the process of patching that vulnerability is simple and effective.
- "Communications" means sharing what we learn both within and outside of Microsoft, providing clear channels for people to talk to us about security issues, and addressing those issues with governments, our industry counterparts, and the public.

To see all of these principles in action, one need only look at our most recently released software: Windows Server 2003. In February 2002, we had all 8,500 developers on the Windows Server team stop developing new code to focus on security. First, they received training on writing secure code. Next, the software went through a three-phase "security push" that involved extensive code reviews, developing threat models to understand where attacks might occur, and, finally, extensive penetration testing by both Microsoft and contract personnel. This effort, which cost over $200 million dollars and delayed the shipment of Windows Server 2003, was a critical step forward and represents significant change in our development process. It is also significant that we are communicating our methodology to others; for example, software developers can use some of the same techniques by reading *Writing Secure Code* from Microsoft Press.

Last week a vulnerability was discovered and patched for Windows Server 2003. While disappointing, such occurrences are part of major operating system development. These systems – in all platforms, including Windows, Linux, and Unix – will always suffer vulnerabilities. Where we distinguish ourselves is in the processes and systems used to remediate such events, and part of Trustworthy Computing is ensuring that our state of the art security response center provides customers with the solutions and updates they need as quickly and rigorously as possible.

As you can see, the Trustworthy Computing goals are real and specific, and this effort is now ingrained in our culture and is part of the way we value our work. It is demonstrated by our enhanced software development process. It is demonstrated by our continued development of more sophisticated security tools, including threat models and

risk assessments, to better identify potential security flaws in our software. It is demonstrated by our formation of what we believe to be the industry's best security response center to investigate immediately any reported vulnerability and to build and disseminate the needed security fix. It is demonstrated by the tools, templates, and prescriptive guidance, such as configuration guidelines, that we post on our website to help system administrators secure our software in many different environments. And perhaps more clearly than anything else, it is demonstrated by our delay in releasing software for months to continue to improve its security. In short, security is – as it should be – a fundamental corporate value. We make every effort to address software security in the initial design, during development, and before a release, and we remain committed to the security of the software once it has gone to market.

At times, of course, people worry that increased security may lead to an erosion of privacy. It is important to note that while there may at times be tension between the two, in most cases security and privacy are not inevitably in conflict. In fact, we think technology can help protect both simultaneously, especially if companies continue to innovate. For example, customers have long said that they need new ways to control how digital information – such as e-mails and word processing documents – is distributed. In response, we are working on a number of emerging rights management technologies that will help protect many kinds of digital content and open new avenues for its secure and controlled use. For example, we are on the verge of releasing Microsoft Windows Rights Management Services (RMS), a premium service for Windows Server 2003 that works with applications to help customers protect sensitive web content, documents, and email. The rights protection persists in the data regardless of where the information goes,

whether online or offline. In this way it allows ordinary users and enterprises to take full advantage of the functionality and flexibility offered by the digital network environment — from sharing information and entertainment to transacting business — while providing greater privacy and better distribution control through persistent protections.

Although we have made major strides, much work on Trustworthy Computing remains ahead of us. One key piece of that work is the Next-Generation Secure Computing Base (NGSCB). This is an on-going research and development effort to help create a safer computing environment for users by giving them access to four core hardware-based features missing in today's PCs: strong process isolation, sealed storage, a secure path to and from the user, and strong assurances of software identity. These changes, which require new PC hardware and software, can provide protection against malicious software and enhance user privacy, computer security, data protection and system integrity. We believe these evolutionary changes ultimately will help provide individuals, government agencies, and enterprises with greater system integrity, information security and personal privacy, and will help transform the PC into a platform that can perform trusted operations to the benefit of consumers, other computer users, and society as a whole.

II. Inter-Industry Security Efforts

Notwithstanding the robust nature of our own efforts, we recognize that Trustworthy Computing and improved cybersecurity will not result from the efforts of one company alone. And so, we are working in partnership with industry and government leaders to make this Trustworthy Computing goal something that is embraced by the entire industry. To get there, we need stronger standards, as well as a

better articulation and implementation of security best practices. Such efforts can help us get out of our historically reactive mode and get into a mode where we prevent, detect, deter and, when necessary, respond by using technology as a tool against cybercrime and potential cyberterrorism.

In April of this year, we joined four other industry partners (AMD, Intel, IBM and Hewlett-Packard) in establishing the Trusted Computing Group (TCG), a not-for-profit organization formed to develop, define, and promote open standards for hardware-enabled trusted computing and security technologies. The primary goal is to help users protect their information assets (data, passwords, keys, etc.) from external software attack and physical theft and to provide these protections across multiple platforms, such as servers, personal computers, PDAs, and digital phones. With regard to best practices, we have worked with private and public partners when establishing configuration guides for systems administrators.

We also helped found the Information Technology – Information Sharing and Analysis Center (IT–ISAC) and provided its first president. The IT-ISAC coordinates information-sharing on cyber-events among information technology companies and the government. Working with other members, we continue to support the IT-ISAC's efforts to coordinate among members, with the government, and with ISACs for other critical infrastructures. Such efforts are critical because this nation's infrastructures were and are designed, deployed, and maintained primarily by the private sector. The interdependencies among infrastructure sectors mean that damage caused by an attack on one sector may have disruptive, unpredictable, and perhaps devastating effects on other sectors. Voluntary information sharing and industry-led initiatives, supported by

government cybersecurity initiatives, comprise an essential first line of defense against such threats. DoD has a direct and immediate stake in the success of these efforts because of DoD's reliance upon privately-operated infrastructures.

We believe that the information sharing engendered to date by the IT-ISAC and other ISACs is an important step in enhancing public-private cooperation in combating cybersecurity threats. Yet, there remains room for progress, and we believe that government and industry should continue to examine and reduce barriers to appropriate exchanges of information, and to build mechanisms and interfaces for such exchanges. This effort must involve moving away from ad hoc exchanges and toward exchanges that are built into business and governmental processes. This will require working toward a common understanding of the information that is valuable to share; when, how, and to what extent such information should be shared; how shared information will be used; and the means by which shared information will be protected. The keystones are trust and value — if an information sharing "network" provides value and the participants trust it, then information will be shared. While the appropriate structure and form of this network are still evolving for both industry and government, we are eager to contribute to a robust and enduring exchange of information on cybersecurity threats and will continue to work with government, our industry partners, and the ISAC community toward that goal.

In addition to efforts to coordinate and facilitate information sharing on cyber-events, we are also working with other industry leaders to propose and institutionalize industry best practices for handling security vulnerabilities in ways that more effectively protect Internet users. We are a founding member of the Organization for Internet Safety (OIS), an alliance of leading technology vendors, security researchers, and consultancies,

that is dedicated to the principle that security researchers and vendors should follow common processes and best practices to efficiently resolve security issues and to ensure that Internet users are protected. Last month, OIS issued for public comment a preliminary draft of best practices for reporting and responding to security vulnerabilities. These draft guidelines provide specific, prescriptive guidance that establishes a framework in which researchers and vendors can work together to improve the speed and quality of security investigations into security vulnerabilities, then jointly provide guidance to help users protect themselves and their infrastructures. OIS will release a revised set of best practices shortly. We view these best practices as an important step in elevating standards for accountability on all fronts and among all audiences in managing security vulnerabilities.

III. DoD-Specific Security Efforts

As I noted earlier, we are committed to working closely with DoD to support its information technology and research. We are keenly aware that any cyberattack against the computer systems of DoD, its allies, or the infrastructures upon which DoD relies may have significant and potentially devastating consequences for our nation. I would like to highlight briefly a few of the areas in which we are partnering with DoD to enhance the security, reliability, and functionality of DoD networks.

We are supporting our DoD customers in keeping their computer systems up to date and in compliance with the Department of Defense Computer Emergency Response Team (DoD CERT) Information Assurance Vulnerability Assessment (IAVA) process. The IAVA process provides positive control of vulnerability notification and corresponding corrective actions within DoD. For example, as United States Air Force Chief Information Officer John Gilligan recently testified before this Subcommittee, the

Air Force is fielding state-of-the art computer network and systems management tools, much of whose core capabilities are powered by Microsoft software. The Air Force uses these tools to control and update their systems rigorously and remotely. These capabilities improve the protection of information and enhance the efficiency of software distribution and asset management, as well as network and system troubleshooting. Although patching is a well-recognized problem, we have enabled the Air Force to realize command-wide implementation of patches and updates for anti-virus software fixes within hours or a day instead of the days and weeks it used to require. This includes massive time-savings in complex enterprises such as the Air Education and Training Command, which consists of 42,000 systems across 13 Air Force bases. Additionally, the United States Army Medical Command, with our support, reached 100% security-patch coverage in over 500 Systems in less than one month. We are also engaged with the Defense Information Services Agency (DISA) on a project that will mirror and make immediately available to its DoD customers the patches that we make available on the Internet.

In addition to supporting DoD's IAVA process, we have outlined a framework that defines the steps necessary to make Microsoft Exchange Server 2003 more secure. That framework also includes the measures that help our government and DOD customers deploy and maintain a secure messaging environment. These efforts help to protect the confidentiality, integrity, and availability of data and systems at every phase of the software lifecycle. For example, an Exchange Server 2003 implementation for the Army Knowledge Online Portal enables the Army to provide a platform that supports its U.S. Defense Message System (DMS). It also supports digitally signing and encrypting

e-mail in applications such as Outlook and the web-based Outlook Web Access. Our technology is providing the U.S. Army with an opportunity to consolidate servers, and the U.S. Army expects to use Exchange Server 2003 as one of the center-point technologies supporting its global messaging and information environment.

We are privileged to be a major contributor to the DMS, the designated messaging system created by the Defense Information Systems Agency (DISA) for DoD and supporting agencies. It is a flexible, commercial off-the-shelf (COTS) application using Microsoft Exchange and Outlook, and it provides messaging and directory services using the underlying Defense Information Infrastructure (DII) network and security services. DMS is installed and operational at 270 military installations worldwide and is integral to today's frontline warfighters. During Operation Iraqi Freedom, for example, DMS won praise for its enhanced capabilities to send attachments such as photos, images and other documents.

DMS provides a message service to all DoD users (including deployed tactical users) and interfaces to other U.S. government agencies, Allied/Coalition forces and defense contractors. We have contributed to DMS over the past eight years, streamlining and hardening the code required to perform unclassified and classified messaging in support of the DoD and others.

We are also helping DoD meet the unique challenges presented by the number of DoD networks, the requirements and trust levels of users, and the sensitivity of information on those networks. Many of today's enterprise customers manage user access to at least three separate networks: an Intranet, an Extranet, and the Internet. Together, these multiple networks enable users to share information with those inside and

outside of their enterprises. The trustworthiness of each of these networks varies according to the level of trust extended to the networks' users.

For the typical enterprise, trusted hosts – such as firewalls and application proxies – are responsible for controlling the access among these different networks. The trusted host model, when correctly configured and maintained, allows enterprises to secure a small number of network connections and, if necessary, to isolate a network under attack.

Particularly within the agencies responsible for protecting national security, the government has elected to keep certain networks completely isolated. These so-called "air-gapped" networks remain so because it was determined that access to them by an unauthorized user could result in loss of life or grave damage to national security. Users of air-gapped networks, who must also access other networks, are typically required to work at multiple workstations, which impedes their effectiveness.

In addition, the importance and number of these "air-gapped" networks supporting information sharing for both the war on terror and coalition warfighting continues to grow. The need for faster, more efficient information sharing, as well as the need to reduce the hardware footprint, power requirements, and ambient cooling demands on the user's desktop, is contributing toward the trend of reducing the number of workstations. For these reasons, there is a growing demand within the U.S. Government, particularly within the DoD and the U.S. intelligence community, to provide access to multiple networks through a reduced number of workstations. One possible solution is to provide increased functionality and usability through multiple windows on a workstation that would securely access multiple networks in a compartmentalized fashion.

We are actively engaged with the government on this important security topic and are currently reviewing technical approaches. We are also in discussions with the government on future technical capabilities that will provide rigorous security mechanisms to protect sensitive information while enabling greater information sharing. Our industry colleagues are also working with the government in this field. In the years ahead, these industry-government collaborations will increase the level of the government's cybersecurity while enhancing the government's overall effectiveness.

IV. Reflections on DoD's Efforts to Protect against Cyberterrorism

My experiences at the Justice Department suggest that the government generally, and the Department of Defense in particular, have great bureaucratic challenges ahead. Throughout our history, citizens have relied upon government to protect public safety and national security. But all threats are not the same, and we have created different organizations and mechanisms for addressing different threats. To protect citizens against crime, we hire, train and equip law enforcement personnel. To protect us against those who would steal our military secrets or attack our vital national interests, we rely upon the intelligence community, both affirmatively to collect foreign intelligence, and defensively to engage in counterintelligence techniques. Finally, to address the military threat posed by another state, we fund a military, supporting personnel, equipment and weapons. In short, depending upon the threat, we deploy a different resource, and each resource plays by its own set of rules.

This traditional model works, however, only when one can identify the nature of the attack; specifically, who is attacking and for what reason. This traditional model fails in the Information Age because when computers come under attack, the "who" and "why" are, and may remain, unknown.

The notion that only states have access to weapons of war is no longer correct, at least not if information warfare is considered. Simply put, we have distributed a technology that is far more powerful than most that are placed in the public domain. Traditional vigilance regarding states that support terrorism or political unrest, or are otherwise considered "rogue" (i.e., "nations of concern") is now supplemented by threats from "individuals of concern," a far larger pool, and one that is harder to identify and police. As a result, an attack upon DoD may come not only from a foreign nation conducting information warfare, but also from juveniles on the West Coast, as it did in Solar Sunrise, the case name for a widespread attack against DoD that appeared, at least initially, to come from the Middle East. To the extent the nation detects a cyberattack but does not know who is attacking – a juvenile, a criminal, a spy, or a nation-state or terrorist group bent on committing information warfare – the role of the Department of Defense may not be entirely clear.

V. Policy Prescriptions

In the face of this challenge, it remains clear that, in cyberspace, "an ounce of prevention is worth a ton of cure." But while the efforts outlined above can address many of the security challenges that DoD faces, technology, process, and people alone cannot provide a complete answer. A comprehensive response to the challenges of cybersecurity depends on technology, process, people *and* appropriate public policy and how these four elements interact with, complement, and reinforce one another. I want to outline a few specific areas where government policy can be particularly helpful in promoting cybersecurity within the government and throughout our infrastructures.

First, the government can lead by example by securing its own systems through the use of reasonable security practices and buying products that are engineered for

security. Where appropriate — such as for national security agencies and other agencies, issues, and services for which security is of the utmost importance — the government's acquisition policies should include purchasing products whose security has been evaluated and certified under the internationally-recognized (and U.S.-supported) Common Criteria for Information Technology Security. We believe that policies requiring the acquisition of software that has received appropriate Common Criteria certifications should be developed and applied consistently and evenhandedly, and we applaud DoD's recent efforts to make clear that its security policies apply to software that has been developed under all business, development, and licensing models. Such efforts to procure only security-engineered products, and specifically such clear support for the Common Criteria, will help strengthen the government infrastructure. In doing so, the government also will help establish appropriate security practices, which ultimately are necessary to enhance the protection of critical infrastructures.

Second, sustained public support of research and development can play a vital role in advancing the IT industry's security efforts. Accordingly, we support additional federal funding for cybersecurity research and development (R&D), including university-driven research. The public sector should increase its support for basic research in technology and should maintain its traditional support for transferring the results of federally-funded R&D under permissive licenses to the private sector so that all industry participants can further develop the technology and commercialize it to help make all software more secure.

Third, government has a critical role to play in facilitating information sharing. Government sharing its own information with industry is essential to improve the security

of software, to protect critical infrastructures, and to build the value for all participants of the information sharing network. In short, the government must be an active provider as well as an avid consumer of valuable threat and vulnerability information.

Conclusion

We are committed to strengthening the security of our software and services, and are equally committed to working with Congress, DoD, other government agencies, and our industry peers on security issues, whether by offering our views on proposed regulatory and policy measures or by participating in joint public and private security initiatives. In the end, a coordinated response to cybersecurity risks – one that is based on dialogue and cooperation between the public and private sectors – offers the greatest hope for promoting security against cyberattacks and for fostering the growth of information networks that sustain and enhance government's capabilities and effectiveness.

Thank you.

Testimony before the House Armed Services Committee
Subcommittee on
Terrorism, Unconventional Threats and Capabilities

"Cyber Terrorism: The New Asymmetric Threat"

24 July 2003

Statement of
Eugene H. Spafford
Professor and Director
Purdue University Center For Education and Research in Information Assurance and Security (CERIAS)

Co-Chair of The U.S. Public Policy Committee
of The Association For Computing Machinery (USACM)

Member of the Board of Directors
of the Computing Research Association (CRA)

Table of Contents

Introduction

Thank you Chairman Saxton and Ranking Member Meehan for the opportunity to testify at this hearing. Threats from malicious software have been steadily growing over the last 15 years and currently present a substantial danger to information systems used by the U.S. military, the civilian government, industry, academia, and the general public. So many of those systems are interconnected and dependent on each other that threats to one segment often spread to all the others. Because malicious software uses victim computers to perpetuate the attack, it presents an asymmetric threat to which U.S. computer systems are particularly vulnerable. In this testimony I will present a short primer on various types of malicious software, their history, their operation and threat, and some of the defenses we can deploy. I wish to stress at the outset, however, that the threat is significant, and the major strategies being taken by government to address this threat are palliative rather than truly preventative.

By way of introduction, I am a professor of Computer Sciences at Purdue University, a professor of Philosophy (courtesy), a professor of Communication (courtesy) and the Director of the Center for Education and Research in Information Assurance and Security. CERIAS is a campus-wide multidisciplinary Center, with a mission to explore important issues related to protecting computing and information resources. We conduct advanced research in several major thrust areas, we educate students at every level, and we have an active community outreach program. CERIAS is the largest such center in the United States, and we have a series of affiliate university programs working with us in Illinois, Iowa, North Carolina, the District of Columbia, Ohio, Virginia, and New York State. CERIAS also has a close working relationship with a dozen major commercial firms and government laboratories.

In addition to my role as an academic faculty member, I also serve on several boards of technical advisors, including those of Tripwire, Arxan, Microsoft, DigitalDoors, Unisys, and Open Channel Software; and I have served as an advisor to Federal law enforcement and defense agencies, including the FBI, the Air Force and the NSA. I am currently a member of the Air Force Scientific Advisory Board, and I have been nominated for membership on the President's Information Technology Advisory Committee. I have been working in information security issues for 25 years, and working with malicious software for over 15 years.

I began this document by listing my affiliations with ACM and CRA. This testimony is not an official statement by either organization, but is consistent with their overall goals and aims. ACM is a nonprofit educational and scientific computing society of about 75,000 computer scientists, educators, and other computer professionals committed to the open interchange of information concerning computing and related disciplines. USACM, of which I serve as the co-chair, acts as the focal point for ACM's interaction with the U.S. Congress and government organizations. USACM seeks to educate and assist policy-makers on legislative and regulatory matters of concern to the computing community. The Computing Research Association is an association of more than 180 North American academic departments of computer science and computer engineering, industry and academic laboratories, and affiliated professional societies. The CRA is

particularly interested in issues that affect the conduct of computing research in the USA. Both organizations stand ready to provide expertise and advice upon request.

Definitions and History[1]

Computers are designed to execute instructions one after another. Those instructions usually do something useful — calculate values, maintain databases, and communicate with users and with other systems. Sometimes, however, the instructions executed can be damaging and malicious in nature. When that happens by accident, we call the code involved a software *fault* or *bug* — perhaps the most common cause of unexpected program behavior. If the source of the instructions was an individual who intended that some abnormal behavior occur, then we consider this malicious coding; various authorities have sometimes referred to this code as *malware* and *vandalware*. These names relate to the usual intent of such software.

There are many distinct programmed threats that are characterized by the way they behave, how they are triggered, and how they spread. Coupled with these characteristics are a number of different methods of deployment and behavior. In recent years, occurrences of malware have been described almost uniformly by the media as *computer viruses*. In some environments, people have been quick to report almost every problem as being caused by a virus. This is unfortunate, as most problems are from other causes (including, most often, operator error or coding faults). Viruses are widespread, but they are not responsible for many of the problems attributed to them.

The term computer virus is derived from and is analogous to a biological virus. The word *virus* itself is Latin for *poison*. Biological viral infections are spread by the virus (a small shell containing genetic material) inserting its contents into a far larger host cell. The cell then is infected and converted into a biological factory producing replicants of the virus.

Similarly, a computer virus is typically a segment of computer code or a macro that will copy itself (or a modified version of itself) into one or more larger "host" programs when it is activated. When these infected programs are run, the viral code is executed and the virus spreads further. Sometimes, what constitutes a "program" is more than a simple application: startup code, word processing document macros, spreadsheets, and window systems also can be infected.

Viruses cannot spread by infecting pure data; pure data files are not executed. However, some data, such as files with spreadsheet input or text files for editing, may be interpreted by application programs. For instance, text files may contain special sequences of characters that are executed as word processor commands when the file is first read into the program. Under these circumstances, the data files are "executed" and may spread a virus. Data files may also contain "hidden" macros that are executed when the file is used by an application, and this too may be infected. Technically speaking, however, pure data itself cannot be infected.

[1] Portions of this text are derived from my article *Virus* in Internet Besieged: Countering Cyberspace Scofflaws, Dorothy and Peter Denning, eds.; Addison-Wesley, 1997.

The first use of the term *virus* to refer to unwanted computer code was by Gregory Benford. As related by Dr. Benford in correspondence with me[2], he published the idea of a virus in 1970 in the May issue of Venture Magazine. His article specifically termed the idea "computer virus" and described a program named *Virus* — and tied this to the sale of a program named *Vaccine* to defeat it. All this came from his experience as a programmer and research physicist at the (then) Lawrence Radiation Lab in Livermore. He and the other scientists noticed that "bad code" could self-reproduce among lab computers, and eventually get onto the ARPANet. He tried writing and launching some "viruses" and they succeeded with surprising ease. Professor Benford's friend, the science fiction author David Gerrold, later incorporated this idea into a series of short stories in the early 1970s that were later merged into a novel in 1972: When Harlie Was One.

Fred Cohen more formally defined the term *computer virus* in 1983. At that time, Dr. Cohen was a graduate student at the University of Southern California attending a security seminar. Something discussed in class inspired him to think about self-reproducing code. He put together a simple example that he demonstrated to the class. His advisor, Professor Len Adleman, suggested that he call his creation a *computer virus*. Dr. Cohen's Ph.D. thesis and later years of research were devoted to computer viruses.

Actual computer viruses were being written by individuals before Cohen, although not named such, as early as 1980 on Apple II computers. The first few viruses were not circulated outside of a small population, with the notable exception of the "Elk Cloner" virus released in 1981 on Apple II systems.

Although Cohen (and others, including Len Adleman) have attempted formal definitions of a computer virus, none have gained widespread acceptance or use. This is a result of the difficulty in defining precisely the characteristics of what a virus is and is not. Cohen's formal definition includes any programs capable of self-reproduction. Thus, by his definition, programs to copy files would be classed as "viruses" because it is possible to use them to copy themselves! This also has led to confusion when Cohen (and others) have referred to "good viruses" — something that most others involved in the field believe to be an oxymoron.

Other forms of self-reproducing or malicious software have also been written. Although no formal definitions have been accepted by the entire community to describe this software, there are some informal definitions that seem to be commonly accepted:

> [*Back doors, Trapdoors*] Back doors, often called trapdoors, consist of code written into applications to grant special access by circumventing the normal methods of access authentication. They have been used for many years, and are generally written by application programmers who are seeking a method of debugging or monitoring code that they are developing. This usually occurs when a programmer is developing an application that

[2] Later reiterated in a letter to the editor of the New York Times, published in December of 1994.

has an authentication procedure, or a long setup requiring a user to enter many different values to run the application. To debug the program, the developer may wish to gain special privileges, or to avoid all the necessary setup and authentication. The programmer also may want to ensure that there is a method of activating the program should something go wrong with the authentication procedure that is being built into the application. The back door is code that either recognizes some special sequence of input, or is triggered by being run from a certain user ID. It then grants special access.

Back doors become threats when they are used by unscrupulous programmers to gain unauthorized access, or when the initial application developer forgets to remove the back door after the system has been debugged, and some other individual discovers its existence.

[*Logic Bombs*] Logic bombs are one of the oldest forms of malicious code. They usually are embedded in programs by software developers who have access to the code. A logic bomb is code that checks for a certain set of conditions to be present on the system. If those conditions are met, it executes some special function that is not an intended function of the code in which the logic bomb is embedded, and is not desired by the operator of the code.

Conditions that might trigger a logic bomb include the presence or absence of certain files, a particular day of the week, or a particular user running the application. It might examine to see which users are logged in, or which programs are currently in use on the system. Once triggered, a logic bomb may destroy or alter data, cause machine halts, or otherwise damage the system. In one classic example, a logic bomb checked for a certain employee ID number and then triggered if the ID failed to appear in two consecutive payroll calculations. A logic bomb embedded in a military system could be designed to disable to disrupt operations on a certain date, or if the code was being used in a particular country.

Of significant concern today is the significant use of commercial, off-the-shelf (COTS) software that has been produced, wholly or in part, outside the U.S. and/or using untrustworthy personnel. Many software vendors have notoriously poor source code control and testing procedures (viz., the large number of bugs and attacks against their products). Thus, logic bombs or hidden trapdoors included in their products are unlikely to be noticed or found. ***Software is regularly being used in mission-critical military and law enforcement tasks that has been produced under the control of individuals who would be prohibited from personally participating in those tasks. We do not adequately screen that software for unwanted, dangerous code. Many of us who work in information security see this as a major threat to U.S. national security.***

[*Worms*] Worms are another form of software that is often referred to by the term virus, especially by the uninformed. "So-called "cyberpunk" novels such as Neuromancer by

William Gibson refer to worms by the term "virus." The media has also often referred incorrectly to worms as viruses. The recent Slammer, CodeRed and ILoveYou incidents were all caused by software that is more correctly described as a worm.

Unlike viruses, worms are programs that can run independently and travel from machine to machine across network connections; worms may have portions of themselves running on many different machines. Worms do not necessarily change other programs, although they may carry other code that does, such as a true virus. It is this replication behavior that leads some people to believe that worms are a form of virus, especially those people using Cohen's formal definition of virus (which also would classify automated network patch programs as viruses).

In 1982, John Shoch and Jon Hupp of Xerox PARC (Palo Alto Research Center) described the first computer worms. They were working with an experimental, networked environment using one of the first local area networks. While searching for something that would use their networked environment, one of them remembered reading The Shockwave Rider by John Brunner, written in 1975. This science fiction novel described programs that traversed networks, carrying information with them. Those programs were called *tapeworms* in the novel. Drs. Shoch and Hupp named their own programs worms, because they saw a parallel to Brunner's tapeworms. The PARC worms were actually useful — they would travel from workstation to workstation, reclaiming file space, shutting off idle workstations, delivering mail, and doing other useful tasks.

The Morris Internet Worm of November 1988 is often cited as the canonical example of a damaging worm program. That worm clogged machines and networks as it spread out of control, replicating on thousands of machines around the Internet.

Few computer worms were written between 1988 and 1998, especially worms that have caused damage, because they were not easy to write by those inclined to want to write them for malicious purposes. Worms required a network environment and an author who was familiar not only with the network services and facilities, but also with the operating facilities required to support them once they reached a target. However, that dynamic began to change as vendors, particularly Microsoft, began to supply network applications with high-level macro interfaces. a could then use high-level macro constructs to write worms and viruses, and the network particulars were handled by the underlying applications (e.g., Outlook and Word).

[*Trojan Horses*] Trojan horses are named after the Trojan horse of myth and legend. Analogous to their namesake, they resemble a program that the user wishes to run — a game, a spreadsheet, or an editor. While the program appears to be doing what the user wants, it actually is doing something else entirely. For instance, the user may think that the program is a game. While it is printing messages about initializing databases and ask-

ing questions about "What do you want to name your player?" and "What level of difficulty do you want to play?" the program can actually be deleting files, reformatting a disk, or otherwise altering information. All the user sees, until it's too late, is the interface of a program that the user thinks he wants to run.

Trojan horses have been, unfortunately, common as jokes within some programming environments. They are often planted as cruel tricks on web sites and circulated among individuals as shared software. Note that the activity of a trojan is not necessarily damaging, but usually is unwanted.

[*Spyware*] Advertisers are continually seeking new ways to get their ads in front of potential buyers, and to collect information that could be used in marketing. One of the more annoying methods of doing this is to insert software into a user's operating system or browser that continually presents the user with pop-up ads. A quieter, but potentially more dangerous form of such software is *spyware* – software that records information about WWW sites visited and sometimes even as much as keystrokes typed. This information is then sent to a central monitoring site for analysis.

Most users are unaware that they have downloaded and installed spyware as part of the software they may be obtaining for other purposes. Usually, the purveyors of spyware include generic legal permission statements in the online license agreements that are presented to users when downloading software. Users seldom read these, or understand the full impact of what they mean.

Note that spyware used on sensitive systems may indeed be operated by actual spies, but disguised as commercial spyware!

[*Rootkits, exploit scripts*] When new faults ("bugs") are discovered in widely-deployed software, some individuals race to develop tools to exploit those flaws. These tools often contain sophisticated interfaces and documentation so as to enable unsophisticated users to employ them. These tools are then posted on newsgroups and WWW sites for open download. What results are widespread break-ins to sites where the patches for the affected flaws have not yet been applied.

The name *rootkit* derives from the goal of hacking into most Unix systems: obtaining access to the *root* account[1]. As some of these tools are written in simple scripting languages, the untrained people who employ them are known as *script kiddies*.

These kits and scripts are written by a variety of individuals. Some are well-meaning individuals who believe they are producing tools to help others determine vulnerabilities in

[1] The Unix root account is the superuser account. It is so named because the superuser owns the root of the file system rather than owning a particular named account

their own systems. Some are simply antisocial individuals with ill-specified agendas, such as to cause embarrassment to particular software vendors. Often these exploits are an attempt to gain some form of notoriety in the marketplace.

[*DDOS, bots*] Systems that are designed to flood sites with more network traffic than they can handle are known as *denial of service* attacks, or DOS systems (not to be confused with MS-DOS or PC-DOS, the early PC programs). These first became a problem in late 1996. To heighten the effectiveness of these attacks, and to further obscure their origin, software has been constructed to create slave programs (robots, or *bots*) on compromised systems around the Internet. These bots maintain contact with a control channel, usually an Internet Relay Chat connection[4]. When the controller of the bots issues a command, all of the bots participate in a distributed denial of service attack, or *DDOS*.

There are a number of automated tools that scan large numbers of systems for vulnerabilities, compromise those systems, and then install bots for DDOS attacks. It is not unusual for thousands of machines to participate in DDOS attacks. The attacking hosts are difficult to trace, and the resulting network traffic can flood (or crash) multiple systems for hours or days at a time. One figure derived in 2001 using statistical methods suggests that thousands of these are occurring each week, although not all are severe enough to be noticed by victims.

Threats and Risks

The malware threat to U.S. systems, and the military in particular, is significant. Software is at the heart of most advanced weapon systems, command and control, communications, mission planning, and platform guidance. Intelligence, surveillance, and logistics all depend on massive computational resources. Less known but equally critical are the embedded processors and SCADA (system control and data acquisition) controllers that are used to adjust everything from flood control gates to utility distribution to building A/C controls. Disruption or compromise of any of these systems can significantly damage our national defense and public safety.

The U.S. military is highly trained and equipped. We have outstanding personnel and equipment. However, those personnel and their equipment are more dependent on correctly-functioning computational resources and communication than any military force in history. That we have equipped them with a computational infrastructure — in hardware and software — that is largely the same as anyone can buy from a major supermarket or mail-order house means that the core of their technical superiority is available for hands-on study by our opponents. ***Worse, a large hobbyist and civilian population is actively seeking weaknesses and attacks against exactly the same platforms used by our military, and they are sharing their findings on global mailing lists and WWW sites. Antagonists from lone fanatics to nation-states large and small have access to detailed information enabling them to construct effective weapons that target our IT systems.***

[4] Internet Relay Chat, or IRC, is form of distributed conferencing that allows users to exchange messages and files without any centralized control. It is similar to instant messaging.

The traditional model of security holds that three qualities need to be protected: confidentiality of information, integrity of data and software, and availability of service and data. The threats are counter to these, namely observation or disclosure of sensitive information, alteration or destruction of data or software, and denial or degradation of service. Traditional viruses target primarily integrity. DDOS tools target availability. Spyware accesses data and compromises confidentiality. Rootkits and backdoors provide access to privileged data and software on the system, thus compromising both confidentiality and integrity.

Currently, threats occur from a spectrum of antagonists. At some level, there are undoubtedly agents of foreign intelligence services and criminal organizations seeking information and mapping weaknesses. The level of this threat may not be accurately known because of the level of "noise" generated by the script kiddies and widespread DDOS attacks. Repeated experiments by groups such as the Honeynet Project have revealed widespread, automated scanning for target systems. Often a new, unpatched system will be compromised and a bot or backdoor installed within 15 minutes of it being placed online in the United States. I have heard of attack intervals as low as 90 seconds.

In addition to ongoing probes, marketing activities generate significant background noise. Unsolicited e-mail ("spam") accounts for as much as 70% of all network traffic in some environments. Some WWW-based probes are the consequence of visiting commercial sites. Some pop-up advertisements are permanently installed on systems through the installation of new run-time software, added without the user's permission. We are also seeing instances of advertisements that are actually worm programs. These worms install themselves on end-user machines and then proceed to send out spam e-mail using the new host, including copies of themselves.

The majority of these attacks are undoubtedly not directed against the U.S. as an entity, but the sheer volume of such traffic makes it difficult to distinguish actual hostile traffic from more benign activity. At the least, the volume of probes and spam is a significant degradation of service, thus meeting the definition of one form of "attack." It is well within the realm of possibility that this traffic is being used as camouflage by hostile actors.

There is a significant threat from simple failure that must not be overlooked. The complexity of our systems is increasing, and software (particularly commercial off-the-shelf or COTS products) are not developed to be robust in the face of active attacks and degraded environments. These factors may combine to cause unanticipated failures, with consequences beyond the ken of the operators. As more of this technology gets pushed into the hands of the individual warfighters, the likelihood of unanticipated and uncompensated failure will increase unless care is taken to simplify and harden the platforms. Use of COTS products optimized for running games and surfing the WWW is *not* likely to provide the necessary protection.

The insider threat is not being given enough consideration. At sites where strong network border

guards are in place and software is generally protected, a trusted insider can introduce dangerous malware that is designed to degrade or halt critical systems, silently corrupt data (e.g., change targeting and mapping information used in precision weapons), or disclose classified information. By being introduced on the inside, the software does not need to be written to overcome specialized protections, but only needs to establish itself on critical systems. This introduction can occur as a result of compromised software from a vendor or contractor, from a visitor or contract worker, from a disaffected or compromised employee or serviceman, or from coalition personnel with interests not in complete alignment with the US.

Enablers

Where malware has flourished is in the weaker security environment of the "personal computer." Personal computers were originally designed for a single dedicated user — little, if any, thought was given to the difficulties that might arise should others have even indirect access to the machine. The systems contained no security facilities beyond an optional key switch, and there was a minimal amount of security-related software available to safeguard data.

Today, however, personal computers are being used for tasks far different from those originally envisioned, including managing defense databases and participating in networks of computer systems. Unfortunately, their hardware and older operating systems are still affected by the assumption of single trusted user access, and this allows computer viruses to spread and flourish on those machines. The population of users of PCs further adds to the problem, as many are unsophisticated and unaware of the potential problems involved with lax security and uncontrolled sharing of media.

Over time, the problem of viruses has grown to significant proportions. In the 17 years after the first infection by the Brain virus in January 1986, the number of known viruses has grown to around 90,000 different viruses affecting Intel/Microsoft platforms. At any one time, approximately 500-1000 of those viruses are actually "in the wild" and posing a threat. The problem has not been restricted to the Intel/Windows PC, and now affects all popular personal computers. However, there are under 60 viruses that have ever been found for the Macintosh platform, and about a dozen for Unix-based platforms. This disparity reflects a number of factors, not least of which is the underlying software architecture of the operating systems in use.

Viruses may be written for any operating system that supports sharing of data and executable software, but all mainframe viruses reported to date have been experimental in nature, written by serious academic researchers in controlled environments. This is probably a result, in part, of the greater restrictions built into the software and hardware of those machines, and of the way they are usually used. It may also be a reflection on the more technical nature of the user population of these machines.

Eight years ago we saw the emergence of the macro virus. This is a virus written in a high-level macro language and attached to word-processing documents or spreadsheets. When an infected

document is opened on any computer platform supporting the software the macro is activated and spreads itself to other, similar documents on the system As these documents are shared across networks, the macro viruses spread widely.

Originally discussed as a theoretical issue[5], the first "in the wild" version appeared in late 1995. Microsoft distributed a CD-ROM to developers with the first virus for the Word program included by an unknown party. No public account has ever been given by Microsoft of how the virus came to be on the CD-ROM, or what they might have done to trace the author. The virus, since named the CONCEPT virus, quickly established itself and began to spread. Within 18 months, over 700 macro viruses had been circulated, and several vendors were indicating that macro viruses were the most commonly reported virus problem at customer sites. Macro and high-level viruses have become the most prevalent in the years since that time.

Unfortunately, macro viruses are here to stay. Users are loathe to do without their custom macros. Multimedia mail makes enclosure of infected documents simple and distribution even simpler. Increasing use of active content in WWW pages and automated downloads suggests that the problem will get worse as time goes on.

One of the biggest enablers of malware is the homogeneous nature of computing environments, especially in the military and government. Systems have been purchased with cost or compatibility as the defining criteria, and this has often included reuse of old software, hardware, and training. Thus, there has been a steady tendency to obtain systems from a limited set of vendor families. Because cost is an issue, COTS software is almost always at the base of these choices, despite the fact that COTS is not written for high reliability or security. Furthermore, the installed systems have their defenses set to lower than optimal to accommodate legacy software and peripherals that were designed for less-protected predecessor systems. The result is an infrastructure that has widespread vulnerabilities — a monoculture — and that is susceptible to widespread attack. If a vulnerability is discovered against one of these systems, there is an extremely high probability that it can be spread to many other systems in the same enterprise.

Consider this quote from a study[6] released by the Air Force Scientific Advisory Board in April 2000: "COTS software is not secure. ... It is strongly recommended that COTS products, particularly software, not be used for critical applications."

The poor quality of most software is perhaps the biggest enabler of attacks against IT systems. Major, widespread attacks are enabled by the presence of significant flaws in deployed software. Those flaws are often the result of poor design and improper coding. Our studies have shown that over 70% of all published flaws in the last few years were caused by faulty coding practices that have been known for years, and often decades. Consider that the CERT/CC reported slightly under 2000 new vulnerabilities in the first half of 2003: that suggests that perhaps 1400 reported

[5] The late Dr. Harold Highland and I each made presentations on macro viruses at security conferences in 1991. Unfortunately, those conferences were never attended by representatives of the major software firms.
[6] Ensuring Successful Implementation of Commercial Items in Air Force Systems.

vulnerabilities (and all associated attacks) in that time were preventable by using known good methods of development.

Traditionally, code has been shipped without adequate testing or care taken in the design. Vendors have felt compelled to ship software with known flaws so as to compete "in Internet time" where time to market has been the most important criterion for success. Customers have largely accepted poor quality software rather than buy competing products that may cost more (and thus reflect the cost of producing higher quality code); the U.S. government is a prime example of this practice. The continual focus on lowest cost rather than ultimate fitness for use has discouraged companies from investing in better software engineering methods, and has also contributed to the increasing use of off-shore development and maintenance operations. Meanwhile, vendors have largely been immune from liability lawsuits despite negligent behavior. In fact, the software vendor community has sought to immunize itself from liability through mechanisms such as the UCITA[7] legislation put forward at the state level.

The result is that vendors of higher quality, safer software have found themselves serving a shrinking market – they face a significant penalty for spending extra resources to make their code reliable. Meanwhile, the typical system administrator may be faced with the prospect of installing and configuring as many as five critical security patches *per week* to the systems under her control. Each of these patches has the potential to disable 3rd-party software that is mission critical. However, the consequence of not installing a patch may well be a system break-in, or contamination of the system from a network worm, thus requiring a complete system scrub and rebuild. All of this is at the expense of the system operator. Unfortunately, this increased cost of operation is not included in the evaluation of price when the original purchase is made. Nor are the costs of of virus protections, firewalls, scanners, and other security tools that are not part of the base system but required to safely operate these complex systems.

To be fair, the vendors with a poor reputation for software quality simply have been reacting to the market. They are in business and must be competitive in the marketplace. As such, meeting customer pressure for low-cost, high-complexity code is what enables them to succeed. The fault for code quality problems lies with the consumers as well as the developers. Some companies have become quite sensitive to these problems and have initiated extensive programs to effect a change in quality control and security awareness. Microsoft's initiative in this respect is particularly notable.

Increased connectivity is also to blame for the magnitude of the current threat. Systems are configured so that every machine has network access. This is needed to provide for remote backups, access to patches, and user access to WWW browsing and e-mail. Unfortunately, that same access allows users without training to import and execute software and documents with macros. Once "inside" the security perimeter, malicious software can spread widely.

[7] UCITA is the Uniform Computer Information Transactions Act, an update of the Uniform Commercial Code that has been opposed by consumer advocates, professional associations, state attorney generals, the ABA and ALA, and many others. Its primary champions are large software firms.

Defenses and Outlook

There are several methods of defense against viruses. Unfortunately, no defense is perfect. It has been shown that any sharing of writable memory or communications with any other entity introduces the possibility of virus transmission. Furthermore, Cohen, Adleman, and others have shown proofs that the problem of writing a program to exactly detect all viruses is formally undecidable: it is not possible to write a program that will detect every virus without any error.

Defense against malware generally takes one of four forms, or as is more often the case, some combination of these four:

[*Activity monitors*] Activity monitors are usually programs that are resident on the system. More general monitoring is now called *intrusion detection*, although it actually detects more than intrusions. These systems monitor activity, and either raise a warning or take special action in the event of suspicious activity. Thus, attempts to alter the interrupt tables in memory, send out many e-mail messages in a short amount of time, or to rewrite special portions of the disk would be intercepted by such monitors. This form of defense can be circumvented by malware that activates earlier in the boot sequence than the monitor code. Many rootkits and viruses contain code that is designed to alter the operating system so as to hide from activity monitors.

[*Scanners*] Scanners have been the most popular and widespread form of malware defense. A scanner operates by reading data from disk and applying pattern matching operations against a list of known virus patterns. If a match is found for a pattern, a virus instance is announced. Other forms of scanners look for known signs of rootkits or intrusions, and also may look for known vulnerabilities that might be exploited by such software. It is usually the case that virus scanners are separate programs from the more general form of security scanners.

Scanners are fast and easy to use, but they suffer from many disadvantages. Foremost among the disadvantages is that the list of patterns must be kept up-to-date. New viruses are appearing by as many as several dozen each day. Keeping a pattern file up-to-date in this rapidly changing environment is difficult. Although it is unlikely that any given user will encounter any particular virus, a single activation by a machine in a critical environment can be devastating.

A second disadvantage to scanners is one of false positive reports. As more patterns are added to the list, it becomes more likely that one of them will match some otherwise legitimate code. A further disadvantage is that some self-altering viruses cannot easily be detected with scanners.

To the advantage of scanners, however, is their speed. Scanning can be made to work rea-

sonably quickly. Scanning can also be done portably and across platforms, and pattern files are easy to distribute and update. Furthermore, of the new viruses reported each week, few will ever become widespread. Thus, somewhat out-of-date pattern files are still adequate for most environments. It is for these reasons that scanners are the most widely-used form of antivirus software.

A variation on scanners that is used by some vendors is heuristic scanning. In this case, new code is examined instruction by instruction to determine if it matches any known pattern of behavior that is common to viruses or other malicious software. This technique can be effective against previously unseen virus code, but it also tends to have a high false positive rate, thus requiring manual intervention.

[*Integrity checkers/monitors*] Integrity checkers are programs that generate checkcodes (e.g., checksums, cyclic redundancy codes (CRCs), secure hashes, message digests, or cryptographic checksums) for monitored files. Periodically, these checkcodes are recomputed and compared against the saved versions. If the comparison fails, a change is known to have occurred to the file, and it is flagged for further investigation. Integrity monitors run continuously and check the integrity of files on a regular basis. Integrity shells recheck the checkcode prior to every execution.

Integrity checking is an almost certain way to discover alterations to files, including data files. As viruses must alter files to implant themselves, integrity checking will find those changes. Furthermore, it does not matter if the virus is known or not — the integrity check will discover the change no matter what causes it. Integrity checking also may find other changes caused by buggy software, problems in hardware, and operator error.

Integrity checking also has drawbacks. On some systems, executable files change whenever the user runs the file, or when a new set of preferences is recorded. Repeated false positive reports may lead the user to ignore future reports, or disable the utility. It is also the case that a change may not be noticed until after an altered file has been run and a virus spread. More importantly, the initial calculation of the checkcode must be performed on a known-unaltered version of each file. Otherwise, the monitor will never report the presence of a virus, probably leading the user to believe the system is uninfected.

Several vendors build self-checking into their products. This is a form of integrity check that is performed by the program at various times as it runs. If the self-check reveals some unexpected change in memory or on disk, the program will terminate or warn the user. This helps to signal the presence of a new virus quickly so that further action may be taken.

[*Border guards, firewalls, proxies*] These are software/hardware combinations that are placed at gateways and borders of networks to examine all traffic into a network. These

systems look for known attacks, viruses, and other dangerous content. Some also scan for prohibited items such as pornographic pictures. When content is found, it is interdicted.

Border scanners are a help in many environments, but they fail when scanning encrypted contents, such as in encrypted e-mail and VPNs (virtual private networks, or tunnels). They also fail against previously unseen content, or when users actively seek to circumvent them. This often happens when a user is seeking to obtain prohibited material, and unknowingly brings in a trojan horse artifact.

There are some experimental systems that seek to measure untoward network behavior and isolate machines that are behaving in an anomalous manner. Automated measures at a larger scale may be necessary to cope with the increasing virulence and speed of malware. Consider:

- The Brain virus, introduced in 1986, required 5 years to reach its maximum level of spread. This was to approximately 50,000 machines, and resulted in perhaps $5 million in damages according to some estimates.
- The Melissa macro worm, released 13 years later, spread to approximately 150,000 systems over a period of four days. Damage was estimated to be in the vicinity of $300 million.
- The ILOVEYOU macro worm, released in May 2000 spread to as many as 500,000 systems in a little over 24 hours. Damage was estimated to be as much as $10 billion.
- The Code Red and Nimda worms in October/November 2001 exploited flaws with published fixes but still managed to compromise 500,000 systems in 14–16 hours. Several billion dollars in damages were estimated.
- The Sapphire/Slammer worm at the beginning of this year, also exploiting flaws with known patches, reached its maximum spread of 75,000 systems in 10 minutes. It was doubling every 8 seconds. It caused over a billion dollars in damages (approximately $13,000 per machine; $1.7 million per second).

Faster propagation of malicious software is possible, especially if some preplanning is done, and it is started by multiple entities. Greater damage is also possible.

If no more computer viruses were written from now on, there would still be a computer virus problem for many years to come. Of the thousands of reported computer viruses, several hundred are well-established on various types of computers around the world. The population of machines and archived media is such that these viruses would continue to propagate from a rather large population of contaminated machines.

In addition to the virus problem is the ongoing problem with DDOS, rootkits, trojan horses, and other attacks. The CERT/CC recorded over 82,000 major attack reports for 2002. In the first half of 2003 they have reported over 76,000. Analysts at Symantec Corporation have esti-

mated that worldwide there were over 80,000 network intrusion attempts in 2002, and over 800 million attempted virus infections. At the current rate of growth, these are expected to reach 100,000 and 120 million, respectively, this year. These are not salutary trends.

Defense against Trojan horse programs, rootkits, and logic bombs is generally limited to intrusion detection systems, firewalls and code inspection. Intrusion detection systems examine log files and/or network traffic to detect known patterns belonging to known attacks or suspicious activity. New attacks, or gradual attacks are often not detected. Firewalls then provide the next level of protection by denying access to certain network services and ports based on policy and need. Unfortunately, users often circumvent these protections with "tunnels" or "proxies" because the firewalls prevent access to desired services. Additionally, tuning of the firewall policies is not simple, and small mistakes or oversights often lead to problems. And finally, if there are flaws in services that are supposed to be exposed to the outside network, the firewalls provide no protection.

Code scanning is a class of techniques used to ensure that software imported to a machine is free of malicious code. This may constitute scanning with automated tools to look for known flaws, or it may involve a more formal procedure of examination such as is done with the Common Criteria. Unfortunately, these examinations are often limited in scope, require some cooperation of the software vendor, require significant time and expense to complete, and are not designed to search for all possible flaws. As the examinations are not carried out after each upgrade and patch, it is still possible to insert malicious code into otherwise protected systems. With some commercial operating systems with applications and database systems installed comprising close to 100 million lines of source code, any examination process using current technology is bound to be incomplete.

Unfortunately, there appears to be no lessening of computer virus and hacking activity. Many new viruses are appearing every day. Major flaws and corresponding attacks are reported every few days. Some of these are undoubtedly being written out of curiosity and without thought for the potential damage. Others are being written with great purpose, and with particular goals in mind — both political and criminal.

Legal Issues

It is very difficult to track computer viruses once they have established themselves. Some luck may be had with tracking a computer virus to its authors if it is found very early after its release. To date, there have been only about seven publicized cases of authors being arrested, tried, and convicted for releasing viruses or similar malware. In most cases, the convictions carried only a fine and a suspended sentence. *For this to be the only visible punishment for over 20 years of virus-writing and almost 100,000 viruses written speaks to the difficulty of coping with the problem within established legal structures.* The little experience we have had with these cases also suggests that the convictions did little to dissuade others from writing viruses.

The same problem occurs with the variety of software break-ins that occur. Each case currently requires investigators with training beyond the norm, access to specialized forensic labs, and (often) cooperation of agencies in foreign jurisdictions. Investigation and then prosecution of computer crimes is vastly underfunded and understaffed in the U.S. today. Each case is expensive to pursue, and often the damages do not justify it. When juveniles are involved, or transnational jurisdictions, there is even less incentive to pursue such cases. The result is a lack of deterrence, and this leads to a continuing high level of attack against critical systems. These attacks draw away resources, and help mask more sinister activities that may be occurring.

The writing of computer malware is not a crime in most places. It is arguable whether writing a virus or attack tool should be a crime, exactly as constructing a bow and arrow is not innately a crime in most jurisdictions. It is the use of the item, and the state of mind of the user that determine the criminality. As such, it is probably the case that the deliberate release of a computer virus should be considered criminal and not simply the writing of the virus. Laws should reflect that difference. However, lawmakers have discovered the same difficulty in clearly defining a virus that researchers have encountered. An overbroad definition such as Cohen's would make the authoring and release of almost any software illegal; the presence of bad laws hurt the situation more than help it, especially when some of the same techniques are used in writing protective software and building test platforms.

The difficulties posed by laws against writing any kind of software is best illustrated with what has happened with regards to copyright. As more content has been developed for use with computers and networks, there has been a greater concern for protecting intellectual property represented by that content. Content owners have stridently lobbied for greater and greater protections for their on-line property. Unfortunately, the evolution of the law has led to unintended consequences for those of us working in security. In particular, I have heard of several instances where research into novel forms of information security have been curtailed because patent holders have threatened researchers. University faculty members do not have the resources to fight such threats.

More recently, provisions of the Digital Millennium Copyright Act (DMCA) have led to faculty being threatened with lawsuits for publishing their security research, and some faculty (Fred Cohen and myself included) have decided to curtail or stop our research in some areas of security because of the potential for us to be arrested or sued. This is particularly true in the area of software threats — the very same tools and techniques necessary to reverse-engineer and protect against malicious software are seen as a threat by many in the entertainment and content provision industries. ***Legislation against technology instead of against infringing behavior can only hurt our progress in securing the infrastructure.***

Some Recommendations

There are several actions that can be taken to reduce the threat of computer malware in the government and military. All of these can be derived by examining the problems that confront us. Among those that have the highest likelihood of making a difference, I would include:

1. Explicitly seek to creating heterogeneous environments so that common avenues of attack are not present. This *may* require some extra expense *at first*, but eventually it may lead to increased compliance with standards, increased innovation, and increased choice in the marketplace, thus lowering costs while increasing security. If real standards (rather than de facto standards) are developed and followed, interoperability should not be a concern.
2. Complementary to the previous recommendation is giving thought to different architectures. Rather than a computer on each desktop, thin-client technologies based on a mid-size computer in a centralized location can provide all the same mission-critical services, but remove many of the dangerous aspects of distributed PCs. For instance, patches need only be applied in one location, and there is a greatly reduced possibility of untrained users loading untested media or software.
3. Rethink the use of COTS software in mission-critical circumstances — the lowest cost is not necessarily the most fit for use. At the least, investigate better methods of screening and testing such software to ensure that it does not contain hidden, unwanted code. At the same time, hold the vendors to a higher standard of care and responsibility for what is in their code.
4. Rethink the need to have all systems connected to the network. Standalone systems may not receive all of the latest patches as soon as they come out. However, that alacrity may not be needed as those systems can no longer be attacked over the network.
5. Require greater efforts to educate personnel on the dangers of using unauthorized code, or of changing the settings on the computers they use. It is still often the case that personnel will turn off security features because they feel it slows them down or gets in their way. Unfortunately, this can lead to significant vulnerabilities.
6. Revisit laws, such as the DMCA, that criminalize technology instead of behavior. It is extremely counterproductive in the long run to prohibit the technologists and educators from building tools and studying threats when the "bad guys" will not feel compelled to respect such prohibitions.
7. Provide increased support to law enforcement for tools to track malware, and to support the investigation and prosecution of those who write malicious software and attack systems. This includes support for additional R&D for forensic tools and technologies.
8. Do not be fooled by the "open source is more secure" advocates. Whether source is open or proprietary is not what makes software reliable. Rather, it is the care used to design and build it, the tools used to construct and test it, and the education of the people deploying it. In fact, some Linux distributions have had more security flaws announced for them in the last 18 months than several proprietary systems. However, some open source software, such as OpenBSD and Apache, appear to be far more reliable than most proprietary counterparts. There is no silver bullet for problems of quality and security.

9. Initiate research into the development of metrics for security and risk. Acquiring systems based on cost as the primary criterion is not reasonable for mission-critical applications. We need to be able to differentiate among different vendor solutions, and set standards of performance.
10. Establish research into methods of better, more affordable software engineering, and how to build reliable systems from untrusted components. 15-20 years ago the decision was made to cede research in this arena to the commercial sector, believing the market would drive innovation. That has not happened. The military needs to reengage in this domain to ensure that their unique and their critical needs are met.
11. Emphasize the need for a systems-level view of information security. Assuring individual components does little to assure overall implementation and use. This requires trained personnel with an understanding of the "big picture" of IT security. Too often those who design and specify the systems do not understand how they are actually used....or misused.
12. Establish better incentives for security. The current climate in many military commands and government agencies is to penalize operators for flaws, thus leading many of them to dread enhancement and exploration of better security.
13. Increase the priority and funding for basic scientific research into issues of security and protection of software. Too much money is being spent on upgrading patches and not enough is being spent on fundamental research by qualified personnel. There are too few researchers in the country who understand the issues of information security, and too many of them are unable to find funding to support fundamental research. This is the case at our military research labs, commercial labs, and at our university research centers.
14. ***Most importantly***, reexamine the issues of the insider threat to mission critical systems – from obtaining software produced by uncleared personnel offshore and in this country, from using COTS products that are not designed for security and reliability, and from access and operation by untrained or unsupervised personnel.

Conclusion

It is clear that we have deficiencies in our cyber defenses. Malicious and incorrect software pose particular threats because of their asymmetric potential — small operators can exercise large and devastating attacks on our defenses. The situation cannot be remedied simply by continuing to spend more on newer models of the same systems and defenses that are currently deficient. It will require vision and willingness to make hard choices to equip our military with the defensible IT systems they deserve.

I will be happy to expand on any of these points, now or in the future.

Thank you again for the opportunity to testify.

Acknowledgments

I received many suggestions from colleagues when composing this testimony. I wish to acknowledge the people listed for their assistance. However, the content and opinions expressed are my own, and the presence of these names should not be construed as endorsement of any of the statements herein.

Rebecca Bace, John Reel, Paul Barry, Terry Kelly, John Davis, Robin Roberts, Kenneth Olthoff, David Isacoff, Paul Williams, Sarah Gordon, Annie Antón, Dwayne Melancon, and Mark Bruhn. I also received statistical information from Symantec Corporation, and from Tripwire Corporation.

QUESTIONS AND ANSWERS SUBMITTED FOR THE RECORD

JULY 24, 2003

QUESTIONS SUBMITTED BY MR. MEEHAN

Mr. MEEHAN. Is there an analysis of terrorist organizations' plan to grow their cyber terrorism capabilities? Are there "terrorist training camps" for computer geeks designed to raise the skill level of the cyber terrorists?

Mr. LENTZ. [The information referred to is classified and is retained in the subcommittee files.]

Mr. MEEHAN. As the Department of Defense is growing increasingly dependent upon commercially based information technology, I believe the Department will be left exposed and vulnerable to internal and external attacks. I would like to hear from each of you, what specifically is being done to ensure a secure system using commercial technologies?

Mr. LENTZ. As DOD's dependence on information networks increases, it creates new vulnerabilities, as adversaries develop new ways of attacking and disrupting U.S. Forces. In recognition of this challenge, the Secretary of Defense identified protection of U.S. information networks from attack as one of his key transformational goals. No one technology, operation, or person is capable of assuring or protecting the Department's vast networks and information. In combination, however, they are parts of an integrated DOD IA strategy, Defense-in-Depth, in which layers of defense are used to achieve a balanced overall Information Assurance posture. To take advantage of rapid advances of rapid advances in information technology the Department maximizes the use of COTS and balances this with layered security.

Even with a solid Defense-in-Depth strategy in place, a fundamental precept is our maintenance of confidence in the security and trustworthiness of the products we use to implement that strategy. New vulnerabilities in the equipment we use, both government and COTS, are identified daily. Operationally, through the Department's IA Vulnerability Alert (IAVA) process and attendant alerts, bulletins, and technical advisories, users are made aware of the vulnerabilities and associated fixes. The IAVA process serves us well, minimizing the disruption of DOD networks during recent cyber incidents that caused widespread disruption elsewhere. Other operational constructs like our tiered Computer Network Defense system enables us to respond to incidents and limit potential damage.

Reactive measures must be balanced with proactive measures. New IT products and systems must be 'born secure'; designed, tested, and validated against specific security requirements. The concept of 'born secure' combined with an aggressive vulnerability management program incorporating the IAVA process, gives us the ability to proactively reduce our exposure to known vulnerabilities and maintain the capacity to respond to evolving vulnerabilities. To help DOD consumers select commercial off-the-shelf IT products that meet their security requirements and to help manufacturers of those products gain acceptance in the global marketplace, the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) established a program under the NIAP to evaluate IT product conformance to international standards. Although no product will ever be totally secure, we can incorporate security into their design and through comprehensive security test and evaluation gain a reasonable sense of the risk we assume when we use them.

A significant cybersecurity improvement over the next decade will be found in enhancing our ability to find and eliminate malicious code in large software applications. Beyond the matter of simply eliminating coding errors, this capability must find malicious software routines that are designed to morph and burrow into critical applications in an attempt to hide. In partnership with the Department of Homeland Security (DHS) we are initiating an effort to develop tools and techniques to examine effectively and efficiently either source or executable software. One goal is to examine the potential benefit of a truly National Software Assurance Center. This center would have representatives from academia, industry, Federal Government, national laboratories and the national security community all working together and sharing techniques to solve this growing threat.

We also need the ability to trust the hardware platforms we use for critical applications. Most microelectronics fabrication in the USA is rapidly moving offshore. DOD and NSA are working on a Trusted Microelectronics Capability to ensure that state-of-the-art hardware devices will always be available for our most critical sys-

tems. The most critical element in any Defense-in-Depth is the human factor. DOD, again in partnership with DHS, is working with government, industry and academia to develop exacting, nationally recognized security standards and certifications for IA/IT professionals as well as staffing standards to support our critical systems and networks.

Mr. MEEHAN. Earlier this year, news reports stated that North Korea had a program to train in attacking information systems—specifically, cyber terrorism. Yet, some sources have stated that cyber terrorism is over stated and the threat is not as great as a physical destruction. Could you please tell the committee what the threat really is?

Mr. LENTZ. [The information referred to is classified and is retained in the subcommittee files.]

Mr. MEEHAN. Mr. Lentz (of DOD), and I would appreciate if all the witnesses could comment on this question. It is my understanding that large portions of commercial off the shelf (COTS) software may actually be produced outside the U.S. The media has reported that software production is moving offshore to India due to cheaper labor costs. How can we ensure that COTS software is not corrupted by unscrupulous persons or even our allies? How can DOD create secure computing capabilities using COTS software that may have been produced outside the United States?

Mr. LENTZ. Ensuring that COTS software is not corrupted by unscrupulous people is a difficult task that warrants considerable effort by all federal agencies. Both foreign and domestic produced software products are vulnerable to having malicious code. Several existing Department of Defense initiatives address these concerns: Software Protection Initiative, Software Producible Initiative, Anti-Tamper Initiative, and the recently established Software Assurance program.

Through the Software Assurance program, DOD in conjunction with DHS will focus on identifying and specifying organizational software assurance processes and software-enabled technologies that are required to ensure systems and network capabilities are secure through a spectrum of threats ranging from vulnerabilities to cyber attacks. The program is initially analyzing software assurance problems and is organized into sub-working groups with representation from many DOD organizations, including the National Security Agency. The four working groups are: Security Process Capability Evaluation (process focused), Counterintelligence (CI) Support, Technical Security Evaluation (product focused), and User Identification of Protected Assets.

A significant cybersecurity improvement over the next decade will be found in enhancing our national capabilities for finding and eliminating malicious code in large software applications. There is little coordinated effort today to develop tools and techniques to examine effectively and efficiently either source or executable software. We believe that this problem is significant enough to warrant a considerable effort coordinated by a National Software Assurance Center. This center should have representatives from academia, industry, Federal Government, national laboratories and the national security community all working together and sharing techniques to solve this growing threat.

QUESTIONS SUBMITTED BY MR. THORNBERRY

Mr. THORNBERRY. Specifically, how is DOD working with the Department of Homeland Security (DHS) to share cyber vulnerability, threat, warning and recovery information? How many DOD personnel are currently assigned to DHS in support of the cyber security mission?

Mr. LENTZ. The Department of Defense (DOD) works with the Department of Homeland Security (U.S. DHS) to share cyber vulnerability, threat, warning and recovery information through the United States Strategic Command's (USSTRATCOM's) Joint Task Force-Computer Network Operations (JTF–CNO). The JTF–CNO, as the operational component of USSTRATCOM, is responsible for coordinating and directing the defense of the DOD computers and computer networks. The JTF–CNO represents the DOD's present operational relationship with DHS on cyber issues. The JTF–CNO communicates with the Information Analysis and Infrastructure Protection Directorate, National Cyber Security Division (formally the National Infrastructure Protection Center) of the U.S. DHS on explicit cyber issues that threaten or may perhaps impact adversely United States national security interests and objectives. Currently, the JTF–CNO is able to share cyber vulnerability, threat, warning and recovery information with U.S. DHS in a secure and rapid method. JTF–CNO maintains a 24/7-watch desk that monitors the cyber environment with the ability to respond swiftly and collaborate with U.S. DHS on a broad

range of cyber issues. This close collaboration includes the watch officers and analysts between the CERT–CC, DOD CERT, and Federal CERT to share threat and vulnerability information.

DOD continues to cooperatively support DHS stand-up, particularly in cyber related efforts through the National Infrastructure Protection Center (NIPC) and National Communication System (NCS) program. The DOD element of the NIPC, funded by Congress for FY03, consisted of up to 53 positions. DOD and DHS are currently developing a Memorandum of Agreement to address long-term DOD personnel working with DHS.

Mr. THORNBERRY. What is the relationship between DOD cyber research, development, and cyber research and development efforts in DHS and other parts of government?

Mr. LENTZ. DOD participates in the Information Security (INFOSEC) Research Council (IRC) that is a collaborative effort between the DOD, the Intelligence Community, and other Federal Civil Agencies to include DHS. The IRC serves as the principal forum to deconflict and focus INFOSEC research issues on common 'hard problems.' The 'hard problems' list was last published in 'draft' format 21 Sept 1999, is scheduled for review beginning in October 2003 and will publish a new list in April of 2004.

Mr. THORNBERRY. It appears that DOD is extremely dependent on commercial products and infrastructure on their own communications. Some estimates say that about 90 percent of DOD communications ride the public backbone—to include data and voice. How is DOD working with the private sector to improve physical and cyber security? How is DOD working with the Department of Homeland Security—who has broader infrastructure responsibilities? What processes and coordination mechanisms are in place or being developed to share threat and warning information that DOD may have with private industry and the DHS?

Mr. LENTZ. Extensive relationships have been developed with the private sector over the years to address the collection, handling, processing, and dissemination of industry data within the DOD. Many of these relationships were accelerated during the Y2K effort. One such group, the Network Security Information Exchange (NSIE), was established in 1991 to provide a confidential environment to share information on network intrusions. Once critical supporting infrastructure assets are identified, vulnerability assessments are then conducted to provide the warfighter, and their supporting Service or agency, measures of operational risk. These assessments include partnerships with industry to understand the specific commercial service networks "outside the fence" of DOD facilities and installations that DOD depends on to accomplish its missions. In many cases, the remediation activities necessary to reduce vulnerabilities and risk involve close partnerships between DOD and industry to mutually assure availability of required infrastructure commodities and services.

One of the key roles and responsibilities of the OASD(HD) is to serve as the central point of coordination between DOD and the Department of Homeland Security (DHS), of which CIP is a major effort. The DOD has actively supported the stand up of DHS with a small contingent of personnel working in the National Infrastructure Protection Center (NIPC). Additional DOD personnel have also been temporarily assigned to the Information Analysis & Infrastructure Protection section. The National Communications System (NCS), which manages the infrastructure, has recently been moved from DOD to DHS and DOD maintains an extensive, cooperative relationship with the NCS.

Additionally, DOD and DHS are collaborating on a first time ever CIP strategy. This strategy will provide guidance on addressing the CIP program, and will be used as the baseline for the development of a Counterintelligence (CI) strategy. There also exists a partnership with DHS on developing a common operational picture capability to mutually work towards supporting the event analysis and determining the effects of an action on other critical infrastructure assets from a regional and national perspective. With a better operational picture of critical assets and their relationships, better decisions can be made.

With respect to sharing threat and warning information, the CERT CC through the Carnegie Mellon has become the primary mechanism for sharing between industry, DOD, and DHS. The CERT CC maintains a knowledgebase, accessible via the Internet, which is a proprietary collection of security information compiled by network and computer security analysts. Sensitive threat and warning information within the CERT CC knowledgebase is available to the DOD CERT via authorized digital certificate access. DOD CERT and CERT CC have been sharing threat and warning information since March 1998, through both classified and nonclassified channels.

Mr. THORNBERRY. What is the role of the National Security Agency in supporting Information Assurance? Are they only permitted to support DOD? Should they have a broader responsibility within the Federal Government to include DHS? What expertise and skills could NSA bring to the broader national cyber security problem?

Mr. LENTZ. The NSA's Information Assurance Directorate (IAD) is responsible for providing information assurance products, services, processes, and policies that protect national security information systems.

NSA's IAD has technical and policymaking responsibility regarding the protection of national security telecommunications and information processing systems across the broad spectrum of departments and agencies within the Executive Branch.

NSA has a 50-year history of developing and deploying communications and now cyber security products and services. NSA has gained a deep understanding of and respect for the challenges the nation faces and must overcome to secure cyberspace. There is little difference between the cybersecurity that is required for a system processing classified information and one that controls a segment of the nation's critical infrastructure. Both systems require the element of assurance or trust. Information must be protected across the entire spectrum. It is vitally important that the Homeland Security and National Security communities continue to build linkages as both communities work to protect our nation's information and infrastructure.

NSA has broad responsibilities in providing for the security of national security telecommunications and for information systems processing national security information. These responsibilities include: evaluating systems vulnerabilities; acting as a focal point for cryptography and Information Systems Security; conducting Research and Development; reviewing and approving security standards and policies; conducting foreign liaison; assessing overall security posture; prescribing minimum security standards; contracting for information security products provided to other Departments and Agencies; coordinating with the National Institute of Standards and Technology (NIST); and providing NIST with technical advice and assistance.

Mr. THORNBERRY. What is the amount of the DOD's R&D budget for cyber security—classified and unclassified? What percentage of the total R&D budget (including percentage of information technology and total R&D budgets) does it represent? Is it sufficient? Does each of the services conduct cyber security R&D? How is this coordinated within DOD and how is technology transferred from research to operational use?

Mr. LENTZ. DOD's R&D budget for cyber security or Information Assurance (IA) in FY03 is $647 million. That amount is 14.9% of the total IT R&D budget and 1.4% of the overall DOD R&D budget. Additional resources can always be used but must be balanced with computing requirements that are both urgent and compelling. We believe we have achieved that for this fiscal budget.

Services and agencies conduct IA R&D to satisfy enterprise requirements and those peculiar to their environment. Their collective efforts are coordinated through the Department's INFOSEC Research Council (IRC). Members, including the Office of Undersecretary of Defense for Acquisition, Technology, and Logistics, each Service, the Defense Advanced Research Projects Agency (DARPA), and the National Security Agency meet bi-monthly to discuss and coordinate security (IA) related efforts. The Defense-wide Information Assurance Program (DIAP), charged with coordination and oversight of IA activities within DOD, meets with IRC regularly with member organizations independently providing a bridge between the research organizations and DOD elements requiring cyber security products and services.

There are several mechanisms in place to determine a developed technology's suitability for DOD use. These include Advanced Concept Technology Demonstrations (ACTD), Small Business Innovation Research/Small Business Technology Transfer (SBIR/STTR), DOD Pilots, and DOD Joint Operational Tests. Once a technology is proven operationally sound, the technology can be transitioned into the department via one of several established procurement channels including development of a DOD acquisition program, establishment of the technology as an Enterprise Solution Initiative (ESI), or transference of the technology to the commercial sector for development of a DOD-procurable Commercial-Off-The-Shelf product.

Mr. THORNBERRY. How is DOD's threat warning information shared with the rest of government? How are various watch centers coordinating their efforts? How does DOD obtain threat and warning information from the rest of government? Does DOD receive vulnerability and threat information from industry? How is this information flow coordinated?

Mr. LENTZ. DOD has solid relationships with industry partners and external agencies through USSTRATCOM and the JTF-CNO. These industry partners and external agencies comprise groups from the intelligence community (IC), federal law enforcement agencies, and the Information Analysis and Infrastructure Protection

Directorate of the U.S. DHS. The JTF-CNO also coordinates with the Federal Computer Incident Response Center (FEDCIRC), through U.S. DHS. The National Communications System (NCS) located in the DISA headquarters' compound, is the principal conduit for information sharing with private sector and Internet service providers. The Computer Emergency Response Team-Coordination Center located at Carnegie Mellon University has the responsibility of supporting the users on the Internet other than the DOD. By coordinating with the Infrastructure Coordination Division, also through U.S. DHS, DOD has the means to receive and pass information with the Information Sharing and Analysis Centers (ISAC). These are industry-run centers, chartered by Presidential Decision Directive 63 (PDD 63), that coordinate information on vulnerability and remediation within specific critical infrastructure sectors.

The CERT CC has emerged as the world's premier clearinghouse for vulnerability information. DHS has just announced an expanded role for the CERT CC with the creation of a US CERT to provide a national-level center to coordinate the cyber responses of the national, state, and local governments.

Mr. THORNBERRY. What are the missions and functions of the DOD Joint Task Force Computer Network Operations? What is their chain of command? What is their relationship with the Strategic Operations Command, the Joint Staff, the Assistant Secretary for Homeland Security and others? Are they coordinating their national security mission with homeland security?

Mr. LENTZ. The mission of DOD's Joint Task Force - Computer Network Operations (JTF-CNO) is: to coordinate and direct the defense of DOD computer systems and networks across the DOD. This includes working with all Combatant Commands, Military Services and Defense organizations. The JTF–CNO actively performs this mission 24 hours a day, seven days a week. The JTF is a subordinate command of the United States Strategic Command (USSTRATCOM), which was charged by the President with the DOD Computer Network Defense (CND) mission in the Unified Command Plan, dated Oct 02. JTF–CNO also has the complementary mission of Computer Network Attack (CNA).

The JTF–CND mission is to defend DOD computer networks and systems from any unauthorized event whether it be a probe, scan, virus incident, or intrusion. The CNA mission is to coordinate, support and conduct, at the direction of the President, computer network attack operations in support of regional and national objectives.

JTF–CNO maintains watch 24 hours per day, seven days a week, and is located in Arlington, VA. It is co-located with the Defense Information Systems Agency (DISA) Global Network Operations and Security Center (GNOSC) and DOD Computer Emergency Response Team (DOD CERT). This co-location helps optimize the commander, JTF–CNO's ability to monitor the status of DOD information networks and conduct operations across the defense information infrastructure.

With this correlated information, the JTF–CNO assesses the impact to network operations and military operations, identifies courses of action that will restore the network, coordinates the necessary actions with the appropriate DOD or non-DOD organizations, prepares a plan to execute and, with approval, executes that order. The JTF–CNO can direct appropriate actions through its four military service components and the DOD CERT.

In addition, the JTF–CNO through the DOD CERT is our primary point of contact with industry in responding to Internet incidents. JTF–CNO also works closely with a co-located Law Enforcement/Counter Intelligence Center. This Center, manned by representatives from all the service investigative agencies, ensures our technical and operational responses to cyber attacks are coordinated with the corresponding criminal investigations.

Mr. THORNBERRY. Within each of the services and for DOD, is there formal cyber security training for managers, users, and systems administrators? Who provides the training? How is it managed and updated? Is it standardized? Is it adequate?

Mr. LENTZ. Each service has formal cyber security training for their system administrators. The initial training is provided through service schools. Additional training is offered via on-line courses and distributive training products. At this time, training provided by the services is not standardized across the DOD but we are working toward that goal. We continue to develop the baseline DOD information assurance standards and requirements.

Training requirements are based on existing DOD policy guidance, service requirements and information systems in use. For example, DOD policy provides specific responsibilities for various levels of the IA Workforce including managers and technical support (privileged access). In addition to formal training, training is available via the Defense Information Systems Agency's (DISA) Information Assurance Support Environment website. Distributive training products, web based tools, videos and classroom training opportunities are available through DISA's program.

They are available to anyone with access to DOD information systems and the training programs address a variety of Information Assurance topics.

A policy memorandum has been published requiring all personnel with primary responsibilities for the security of systems and networks, Designated Approval Authorities (DAA), to certify completion of a DAA training package that is provided by DISA. This DOD training standard meets existing requirements and is evaluated for adequacy on a regular basis. Current policy also establishes basic training requirements for managers, technical personnel (System Administrators), and users with access to DOD information Systems. Awareness training is provided annually for all DOD users.

Additional formal cyber security training requirements for all information assurance managers and technical (systems administrators) workers are drafted and pending formal staffing and publication. These training requirements will use commercial certifications to establish baseline requirements for each category and level of the DOD IA workforce including military, civilian (including foreign nationals), and contractors. Using "approved certifications" will standardize the training requirements for each IA Category, function and level. Analysis of the approved certifications and workforce effectiveness will allow continuous evaluation of the effectiveness of the certifications. In partnership with the Department of Homeland Security, DOD is working towards establishing national certification program standards that will ultimately be adopted not only by DOD and other federal agencies, but also by private industry.

Mr. THORNBERRY. There has been much discussion over whether cyber security standards are needed and should be developed. What is DOD's position? Is it possible to develop standards within DOD and would it make a difference if there were not broader national or international standards?

Mr. LENTZ. There cannot be a coordinated effort to address cyber security without standards. As no single technology, operation, or person is capable of assuring or protecting the Department's vast networks and information, we use all three in combination to form an integrated DOD Information Assurance strategy. One of the pivotal underpinnings of that strategy is the development, use and enforcement of standards in each of the three areas.

In October 2002, the Department published its capstone IA policy, DOD Directive 8500.1, "Information Assurance" followed in February the following year by amplifying policy in DOD Instruction 8500.2, "Information Assurance (IA) Implementation." The directive establishes basic policy and the instruction implements policy by further assigning responsibilities and prescribing procedures for applying integrated, layered protection of DOD information systems and networks. In addition to the capstone policy we have a comprehensive Computer Network Defense (CND) policy and amplifying instruction to guide operational issues. Other policies, or high level frameworks and standards, are scheduled for release within the next year to define Wireless Communications security, Certification and Accreditation of Systems and Networks, Vulnerability Management and Assessments, Interconnection and Data Transfer between Security Domains, Ports and Protocols Management and many others. These policies were developed with considerable government, industry, and academic involvement.

With respect to commercial-off the-shelf (COTS) Information Assurance products, we have developed standard security requirements or Protection Profiles to describe the security attributes of the products we need. Those requirements are written using the Common Criteria, an international security language, and products are tested in internationally certified laboratories to those criteria. We use standard security configuration guides developed by NSA and the Defense Information Systems Agency (DISA) to ensure software applications are used securely. Some of those guides are derived from commercial best practices.

In addition, DOD actively participates in standard groups with industry and our international partners to influence and support communications and network standards that have significant security implications. Examples include the recent decision to transition to IPv6 by fiscal year 2008 and the incorporation of a high-speed Internet Protocol encryption standard for GIG/BE requirements.

In the area of CND we have not only guiding policy but also specific standards for the Identification, Promulgation, Use, and Reporting of system vulnerability information; Computer Emergency Response Team (CERT) operations and certification; the Use of Penetration Testing during the conduct of exercises; and IA Readiness Metrics and Reporting Procedures. Working with the Department of Homeland Security (DHS) and industry we are developing standard staffing and personal IA/IT security certifications.

We co-exist in a global network environment with a heavy reliance on COTS products to create the infrastructure. Without standards we would not be able to lever-

age the efforts of the government and civil sectors both nationally and internationally.

Mr. THORNBERRY. Since DOD is so reliant on information technology and the infrastructure and with network centric concepts being more fully developed, which rely on a robust, survivable network, what is DOD doing to more fully protect its information and physical infrastructure?

Mr. LENTZ. The DOD Information Assurance Directorate has published Instruction 8500.2, "Information Assurance Implementation", that sets confidentiality, integrity and availability controls used in the protection of information. This policy also lays out the survivability of information that should be tied with the continuity of operation and continuity of government plans. Other recent policy issuance includes ports and protocol management and the wider use of public key encryption.

The DOD CIP Program under the ASD(HD) has led the DOD effort to identify and evaluate cyber and physical assets essential to the mobilization, deployment, and sustainment of U.S. military operations. Once the critical supporting infrastructure assets are identified, vulnerability assessments can then be conducted to provide the war fighter, and their supporting Service or agency, measures of operational risk. This information adds valuable input to the IA requirements generation process. The mission priorities, interdependencies, and vulnerability assessments can serve as a catalyst for vulnerability remediation or mitigation decisions, the implementation of mechanisms to reduce or minimize operational impacts, and the development of operational risk management protocols. In many cases, these remediation activities involve close partnerships between the military and industry to mutually assure availability of required infrastructure commodities and services.

Mr. THORNBERRY. Does DOD conduct cyber exercises in which its cyber operational posture has been degraded or wiped out? For example, during fleet training or exercises, do battle groups simulate loss of communications, and assess the mission impact if they are unable to send or receive targeting information within the battle group or from national authorities? If so, what have been the results of these exercises and how has that impacted force operations in both a service and joint context?

Mr. LENTZ. DOD conducts numerous exercises to simulate experimental and real world events to test the effects of cyber operational posture. Exercises such as Apollo CND (in 2000) and Millennium Challenge 2002 validate the operational methods used to protect and defend DOD networks from attacks. Command and control structure and procedures are specifically examined during these exercises, by testing cyber operations both real and simulated. U.S. Strategic Command (USSTRATCOM) is working closely with the other Combatant Commands to integrate CND capabilities into future exercises and real-world operations. Lessons learned from these exercises are used to develop and refine the planning, command and control, and communication processes for future joint operations.

QUESTIONS SUBMITTED BY MS. SUSAN DAVIS

Ms. DAVIS OF CALIFORNIA. Can you describe the security that the Navy Marine Corps Intranet provides? Is it a secure network? Should other services adopt a similar model?

Mr. LENTZ. Overall, the NMCI Information Assurance (IA) approach addresses the fundamental components of DOD's Global Information Grid (GIG) IA strategy (people, operations, and technology). This is done through the employment of a defense in depth strategy, mandatory requirements for Certification and Accreditation, DOD PKI, National Information Assurance Partnership (NIAP) approved products, security specific Service Level Agreements (SLAs), security assessment teams, and Commercial Off the Shelf (COTS) security products based on best commercial practices. The Department of the Navy (DON) has retained the right to exercise essential command authority over network operations for Defense Information Warfare (IW) activities. Also, the NMCI contract has retained DON approval authority of key components, to include security architecture, security critical product selections, network connectivity plan, and security procedures.

Although the use of commercial best practices is encouraged, there are certain mandatory security requirements defined in the NMCI contract that must be adhered to, such as:

- Use DOD Public Key Infrastructure (PKI) that is interoperable with DOD PKI.
- Implement strong Authentication: DOD PKI Certificates stored on a cryptographic smart card (the DOD Common Access Card) will be required for network access.

• Certify and accredit (C&A) in accordance with the DOD Information Technology Security Certification and Accreditation Process (DITSCAP)
• Map DITSCAP requirements into the NMCI implementation strategy to ensure that both are accomplished in a timely and cost-effective manner
• Use NIAP approved IA and IA-Enabled products
• Use Defense Information Systems Network (DISN) Security Accreditation Working Group (DSAWG)/Secret and Below Interoperability (SABI) approved products for interconnecting Secret and Below networks
• Implement a sensor grid based intrusion detection architecture for Computer Network Defense (CND) that is fully interoperable with the current DON CND infrastructure.
• Use Government-run Security Assessment Teams (Red Teams and Green Teams).
• Use Defense-in-Depth, which is multiple protection technologies installed in a layered system of defenses
• Incentives performance on IA: DON Teams will provide independent assessments of the security posture of the NMCI network. The NMCI vendor will receive a monetary reward based on their performance on these assessments.
• Train using on-line web based IA training, which is available to all NMCI users

NMCI implements a wide range of mechanisms (policies, documentation, processes, and tools) that fully support IA and interoperability of NMCI with the DOD GIG. NMCI enables secure, seamless, global end-to-end connectivity for Naval and Joint warfighting and business functions. We believe this approach lays the groundwork for significant improvement in secure interoperability with the Joint DOD community. In fact, NMCI has undergone an Operational Assessment to ensure that it is interoperable with the JCS, other Services, IT-21 and Marine Corps Enterprise Network. NMCI is designed to provide confidentiality, integrity, authenticity, identification, access control, non-repudiation, survivability, and availability of the information and information technology (IT) systems in a Joint network centric warfare environment. We believe other services have seen many benefits in the DON's approach to IA with respect to NMCI.

Ms. DAVIS OF CALIFORNIA. Secretary Lentz, I'd like to follow up on a line of questioning from one of my colleagues relating to NMCI. He seemed to infer that NMCI was not a secure network because sailors may possess and use their own electronic devices. Are sailors allowed to connect their own systems, such as a personal laptop or Blackberry, to NMCI? If so, what security precautions are taken? Does NMCI provide laptops and Blackberry hardware and services as part of the contract?

Mr. LENTZ. DON personnel are not allowed to connect personally owned equipment such as computers and portable digital assistants (PDAs) to NMCI, in accordance with DOD and DON policy. These policies are enforced by not allowing non-NMCI registered computers and PDAs to log on to NMCI, even if they are physically plugged into the NMCI network in violation of the policy. A NMCI user cannot load software on a NMCI computer.

The NMCI contract does provide a Contract Line Item Number (OLIN) for portable and Blackberry hardware and services.

Ms. DAVIS OF CALIFORNIA. You mentioned in your testimony today that DOD successfully defended against some 50,000 attacks. That's great work! Were there any successful attacks?

Mr. LENTZ. DOD has experienced some intrusions of limited success although none have had an impact on our operations. Almost all of the successful intrusions come during the period of risk between the time when vulnerability is first discovered and the time we can apply patches or anti-virus updates across the entire Department. Our network operators have extensive measures for detecting and containing the intrusions and our criminal investigation agencies are increasingly successful in finding and prosecuting intruders.

Ms. DAVIS OF CALIFORNIA. What is NORTHCOM doing to protect our critical infrastructure?

Mr. LENTZ. NORTHCOM began an effort earlier this year to identify and assess all the infrastructure assets used for NORTHCOM Command and Control (C2) missions, i.e., the connectivity to all of their supporting/subordinate commands in the areas of voice, VTC, data, and satellite communications, both secure and non-secure. There is also a pilot project to facilitate information sharing with civil authorities that, so far, connects DOD installation security personnel in the National Capital Region, allowing them to share data regionally about suspicious activities, bomb threats, etc. for purposes of Force Protection. In addition, the upcoming Joint Warrior Interoperability Demonstration (JWID) 2004-05 is focused on NORTHCOM and

the HLS missions. Plans are in full swing to demonstrate products and technologies that can support all facets, including CIP.

QUESTIONS SUBMITTED BY MR. BARTLETT

Mr. BARTLETT. Mr. Chairman, there may be some dispute as to what a large extra atmospheric nuclear detonation would do to our ground-based computers. But I think there is not dispute as to what it would do to the communications satellite. I think it was Mr. Dacey who mentioned how critical they were in our communications.

It is my understanding that they are the softest link of our communications net, that a large extra- atmospheric nuclear detonation, producing a surge of Compton electrons, would take out all of the satellites that were in line of sight. And those that were not would shortly die because of pumped Van Allen belts. So they would decay very quickly. I have only two or three or so hardened satellites, radiation-hardened satellites, and the Milstar satellites. They carry a tiny percentage of even our military communications, to say nothing of other communication. And by the way, you cannot launch a new satellite if this happens because Van Allen belts are still pumped up, will remain so for a year or so. So to get communications through satellites, you would have to build some radiation-hardened satellites and launch those. And clearly, by that time, the Van Allen belts would have receded and you could not launch conventional satellites.

And by the way, this could all happen with an "Oops, I am sorry," kind of an event, and accidental launch. And they detonate the missile high in space so that it is not going to hurt anybody on Earth. What would we do if that happened? This is the ultimate in asymmetric terrorist attack, of course. What will we do? And is there a COOP Plan for that?

Mr. LENTZ. The nuclear effects on satellites have been a concern of the Department of Defense for more than three decades. Throughout the Cold War, Department scientists and engineers studied the effects of atmospheric and exo-atmospheric nuclear detonations and provided recommendations to our operations and acquisition communities. Hardening satellites to ensure continued operations in a nuclear environment was a major Cold War effort and remains part of our space protection posture. Since the impact of nuclear detonations is highly scenario dependent, the Department continues to work with both the operations and acquisition communities to develop mitigation strategies as well as to field appropriate, cost effective measures for protecting space systems. The continued proliferation of missile technology has required the Department to constantly monitor emerging threats and reassess its mitigation strategies for the future.

QUESTIONS SUBMITTED BY MR. LANGEVIN

Mr. LANGEVIN. One of the most concerning problems in information security is the issue of patch management. Every plan to increase our cybersecurity puts this at the top of its priority list. How does the DOD handle patch management across the agency? Is in-house testing done to ensure they will not adversely affect systems? Do you have any requirements or standards vendors must comply with when they issue patches? How can we in general better deal with this issue?

Dr. SPATFORD. I am only familiar with some aspects of how DOD handles patch management, so I am not able to answer most of this question.

As a general issue, consideration should be given to purchasing and deploying systems that do not need such frequent patching. Systems that have single uses (such as running a WWW server) might be better hosted on a server appliance that does not need patches to email, DB, or word processing software. This will reduce the number of patches, as well as reduce the number of attack points. This is simple engineering: a component with 100 breakable parts is less likely to fail than a component with 5000 breakable parts.

Additionally, purchases should take into account the security history of platforms that could be used for various purposes. For instance, consider platform A and platform B (different OS's sold by different vendors, possibly on different hardware). Both support email, a WWW browser, and other common applications, and either could be used to support a set of DOD missions, given some inital custornization and training. But suppose platform A has had 100 serious security flaws with patches over the last 3 years, and platform B has had only 30. Additionally, platform A has 50,000 potential viruses and worm programs that can attack it, but platform B has only 20. If so, then serious thought should be given to purchase of platform B even if the up-front purchase cost is more than platform A. Buying platform B

should result in reduced expenses in maintenance, reduced security vulnerabilities, and increased productivity over the lifespan of the platform. It should also apply market feedback to both of the vendors. Currently, vendors are rewarded for offering a cheaper product even if it is less safe.

Mr. LENTZ. The Department of Defense (DOD) established the Information Assurance Vulnerability Management (IAVM) program in 1998. IAVM is a comprehensive distribution process for notifying Combatant Command, Military Service's and Defense Agencies about vulnerability alerts and countermeasures information. The IAVM provides positive control of vulnerability notification and corresponding corrective action for DOD networks. The IAVM program is one of the key means of ensuring the security of DOD computers and consequently isan area to which we devote considerable attention. The DOD Computer Emergency Response Team (CERT) at Defense Information Security Agency (DISA) assesses all announced vulnerability and determines specific actions required to address the vulnerability. Based on various factors such as the number of vulnerable systems in DOD, the likelihood that the vulnerability will be exploited, and the availability of a patch, the DOD CERT will recommend mandatory patching, optional patching, or issue a situational awareness alert. The Joint Task Force - Computer Network Operations makes the ultimate decision to order mandatory patching within a given time period after balancing the risk against any operational impact of devoting manpower and resources to the patch. DOD has established extensive policy and guidance for these processes in information assurance and computer network defense directives and instructions.

So far in 2003, DOD has issued 12 orders for mandatory vulnerability patching from over 1583 identified vulnerabilities. These are patches that must be installed immediately and often cover multiple vulnerabilities. Additional bulletins and advisories have been issued for patches that should be considered for installation during the normal patch management. Vendors are responsible for the quality of their patches; however, DOD routinely advises Combatant Commands, Military Services and Defense Agencies to test patches to ensure compatibility with their particular fielded configurations. Patches installed to critical systems such as command and control systems and messaging systems are subject to rigorous testing by their program managers.

Fiscal year 2003 initiatives with DOD-wide cooperation in this area focus on improving the ability to automatically apply patches across large networks and automatically verify patch compliance. The complexity of our networks, with over 3 million computers and a wide variety of operational configurations, makes this important effort a tremendous technical challenge. Nonetheless this is a challenge to which we are committed to finding a solution.

Mr. DACEY. At the subject hearing, we discussed the status of efforts by the Department of Defense (DOD) to ensure the security of its information systems and to implement the statutory information security requirements of government information security reform law.[1] Our testimony and the responses to the questions considered performance data that DOD reported to the Office of Management and Budget (OMB) for fiscal year 2002 pursuant to this law. We did not validate the accuracy of the data reported by DOD. We have not specifically reviewed the patch management process for DOD, which would include such items as whether in-house testing is done and whether DOD has any requirements or standards that vendors must comply with when they issue patches. However, in its fiscal year 2002 report pursuant to government information security reform law, the department reported that it operates the Information Assurance Vulnerability Alert program to manage vulnerabilities in its operating systems and software and to take steps to alert users and to fix these weaknesses. This program notifies the services and agencies about identified software weaknesses and defines the proper patches to fix the problems. DOD also reported that this program has aided in mitigating some of the risk and problems associated with viruses and is a key ingredient to a successful information security program.

An update on DOD's patch management program should be provided in its upcoming fiscal year 2003 information security report, which the Federal Information Security Management Act now requires that federal agencies submit to OMB and the Congress[2] DOD's report, which OMB has requested be submitted by October 1,

---

[1] *Title X, Subtitle G—Government Information Security Reform, Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001, P.L. 106–398, October 30, 2000.*

[2] *Title III—Federal Information Security Management Act of 2002, E-Government Act of 2002,* P.L. 107–347, December 17, 2002. This act superseded an earlier version of FISMA that was enacted as Title X of the Homeland Security Act of 2002.

2003, is to specifically include information on how DOD confirms that patches have been tested and installed in a timely manner.

Agencies can implement effective patch management programs. As we reported in our recent testimony on patch management,[3] effective patch management practices have been identified in security-related literature from several groups, including the National Institute of Standards and Technology (NIST), Microsoft,[4] patch management software vendors, and other computer-security experts. Common elements identified include the following:

- **Senior executive support.** Management recognition of information security risk and interest in taking steps to manage and understand risks, including ensuring that appropriate patches are deployed, is important to successfully implementing any information security-related process and ensuring that appropriate resources are applied.
- **Standardized patch management policies, procedures, and tools.** Without standardized policies and procedures in place, patch management can remain an ad-hoc process—potentially allowing each subgroup within an entity to implement patch management differently or not at all. Policies provide the foundation for ensuring that requirements are communicated across an entity. In addition, selecting and implementing appropriate patch management tools is an important consideration for facilitating effective and efficient patch management.
- **Dedicated resources and clearly assigned responsibilities.** It is important that the organization assign clear responsibility for ensuring that the patch management process is effective. NIST recommends creating a designated group whose duties would include supporting administrators in finding and fixing vulnerabilities in the organization's software. It is also important that the individuals involved in patch management have the skills and knowledge needed to perform their responsibilities, and that systems administrators be trained regarding how to identify new patches and vulnerabilities.
- **Current technology inventory.** Creating and maintaining a current inventory of all hardware equipment, software packages, services, and other technologies installed and used by the organization is an essential element of successful patch management. This systems inventory assists in determining the number of systems that are vulnerable and require remediation, as well as in locating the systems and identifying their owners.
- **Identification of relevant vulnerabilities and patches.** It is important to proactively monitor for vulnerabilities and patches for all software identified in the systems inventory. Various tools and services are available to assist in identifying vulnerabilities and their respective patches. Using multiple sources can help to provide a more comprehensive view of vulnerabilities.
- **Risk assessment.** When a vulnerability is discovered and a related patch and/or alternative workaround is released, the entity should consider the importance of the system to operations, the criticality of the vulnerability, and the risk of applying the patch. Since some patches can cause unexpected disruption to entities' systems, organizations may choose not to apply every patch, at least not immediately, even though it may be deemed critical by the software vendor that created it. The likelihood that the patch will disrupt the system is a key factor to consider, as is the criticality of the system or process that the patch affects.
- **Testing.** Another critical step is to test each individual patch against various systems configurations in a test environment before installing it enterprisewide to determine any impact on the network. Such testing will help determine whether the patch functions as intended and its potential for adversely affecting the entity's systems. In addition, while patches are being tested, organizations should also be aware of workarounds, which can provide temporary relief until a patch is applied. Testing has been identified as a challenge by government and private-sector officials, since the urgency in remediating a security vulnerability can limit or delay comprehensive testing. Time pressures can also result in software vendors' issuing poorly written patches that can degrade system performance and require yet another patch to remediate the problem. For instance, Microsoft has admittedly issued security patches that have been recalled because they have caused systems to crash or are too large for a computer's capacity. Further, a complex, heterogeneous systems environment can lengthen this already time-consuming and time-sensitive process because it takes longer to test the patch in various systems configurations.

---

[3] U.S. General Accounting Office, *Information Security: Effective Patch Management is Critical to Mitigating Software Vulnerabilities,* GAO–03–1138T (Washington, D.C.: Sep. 10, 2003).

[4] Microsoft Corporation, *Solutions for Security, Solutions for Management: The Microsoft Guide to Security Patch Management* (Redmond, WA: 2003).

• **Distributing patches.** Organizations can deploy patches to systems manually or by using an automated tool One challenge to deploying patcles appropriately is that remote users may not be connected at the time of deployment, leaving the entity's networks vulnerable from the remote user's system because they have not yet been patched.

• **Monitoring through network and host vulnerability scanning.** Networks can be scanned on a regular basis to assess the network environment, and whether patches have been effectively applied. Systems administrators can take proactive steps to preempt computer security incidents within their entities by regularly monitoring the status of patches once they are deployed. This will help to ensure patch compliance with the network's configuration.

Mr. LANGEVIN. From what the panel can tell, is there sufficient information sharing taking place between researchers who discover most vulnerabilities, companies who created the products and DOD? Does the DOD actively work to foster an environment where researchers and companies could work together? How does CERT/CC (Computer Emergency Response Teams Coordination Center) fit into your strategy?

Dr. SPAFFORD. I cannot answer this question definitively because I do not have sufficient information of the amount of sharing that is performed. However, I can provide a subjective answer: I run the country's largest academic center for information security, and we have been unable to establish any meaningful connection with DOD in the last few years. Many of my peers at other academic institutions also report spotty or non-existant contact as well. To be fair, our work is largely more research-oriented than mission support that is needed by DOD. It is also true that without financial support for the universities involved it would be difficult or impossible for most academic centers to undertake new efforts. There is also the issue that many of our students are not US nationals. However, the lack of meaningful contact with relevant DOD entities does not allow those of us in academia to explore those areas where we might be of assistance.

Mr. LENTZ. Considerable information sharing occurs among DOD Agencies, Services, CERT/CC and many technology vendors. The DOD fosters relationships and works extensively with many of the nation's top IA technology researchers and commercial vendors. The DOD IA community is sought out for support and guidance on all areas of information assurance. This sharing exists at many levels and at varying degrees of intensity.

- The Information Assurance R&D community is particularly successful, through avenues such as the Information Security (INFOSEC) Research Council. This collaborative effort between the DOD, the Intelligence Community, and other Federal Civil Agencies serves as the principal forum to deconflict and focus INFOSEC research issues on common 'hard problems.' Research efforts can then be worked with academia and industry to solve the government's needs.
- The Information Assurance Technical Framework Forum (IATFF) is a National Security Agency (NSA) sponsored outreach activity created to foster dialog amongst U.S. Government agencies, U.S. Industry, and U.S. Academia seeking to provide their customers solutions for information assurance problems.
- The Center for Internet Security (CIS) is a not-for profit cooperative organization of government, industry and academia members who develop security benchmarks to improve the security of network products. The CIS has worked with DISA, NSA, and NIST to incorporate their security technical guidance in their benchmarks.
- Through work in standards forums, such as the Internet Engineering Task Force, DOD works with researchers to jointly address security concerns.
- DOD has significant efforts with NIST on commercial algorithm development, evaluation and certification of commercial IA products, and development of guidelines for securing Federal Government IT systems.

The CERT CC is the primary mechanism for sharing vulnerability information between industry and DOD. The CERT CC is a FFRDC funded by the DOD to provide this service to the DOD CERT and to industry. CERT/CC also works closely with NSA's National Security Incident Response Center during the identification, diagnosis and remediation of significant INTERNET security incidents.

Mr. DACEY. Although we have not specifically reviewed efforts by researchers who discover most vulnerabilities, companies who created the products, and DOD to share information and work together, our recent patch management testimony discussed two critical vulnerabilities in widely used commercial software products and

the steps taken by the Federal Government and the private sector security community to collaboratively respond to the threat of potential attacks against these vulnerabilities. First, in June 2003, Last Stage of delirium Research Group notified Microsoft about a security vulnerability in Microsoft's Windows Distributed Component Object Model Remote Procedure Call interface.[5] This vulnerability would allow an attacker to gain complete control over a remote computer and was exploited by both the Blaster and Welchia worms in August 2003. Within hours of being notified, Microsoft verified the vulnerability and issued a security bulletin in July that publicly announced the critical vulnerability and provided workaround instructions and a patch. In addition, the CERT® Coordination Center (CERT/CC),[6] the Federal Computer Incident Response Center (FedCIRC),[7] and the Department of Homeland Security (DHS) all issued advisories. Second, in July 2003, Cisco Systems, Inc., which controls approximately 82 percent of the worldwide share of the Internet routers[8] market, issued a security bulletin to publicly announce a critical vulnerability in its Internet operating system software, and provide workaround instructions and a patch. This vulnerability could allow an intruder to effectively shut down unpatched routers, blocking network traffic. Cisco had informed the Federal Government of the vulnerability prior to public disclosure, and worked with different security organizations and government organizations to encourage prompt patching.

A variety of resources is available to provide information related to vulnerabilities and their exploits, including the CERT/CC. This organization has a research program, one goal of which is to try to find ways to improve technical approaches for identifying and preventing security flaws, limiting the damage from attacks, and ensuring that systems continue to provide essential services in spite of compromises and failures. Other efforts include Microsoft's recently initiated Trustworthy Computing strategy to incorporate security focused software engineering practices throughout the design and deployment of its software. Microsoft is also reportedly considering the use of automated patching in future products.

Mr. LANGEVIN. I'd like the panel to give their opinion on how DOD might help DHS and other federal agencies improve their information security?

Dr. SPAFFORD. Sharing best practices is helpful. Sharing histories of vulnerabilities and defenses could be helpful. Sharing some training and awareness materials might be helpful. However, many of the same problems faced by the civilian agencies are still problems in the DOD. It is also the case that threats and operational parameters are often different, and this suggests that the proper solutions may also be different. Thus, it is not clear how much useful guidance can be given.

Mr. LENTZ. DOD is currently engaging on several information security initiatives with DHS. They include:

- DOD–DHS Partnership to lead expansion of the 'Consensus-based Security Benchmark Development' across the public & private sectors
- DOD–DHS Partnership to collaborate on identification of 'Information Assurance Hard Problems' and Partnering on Research & Development Investments
- DOD–DHS Partnership on development of International Agreements to Share Cyber-Warning Information
- DOD–DHS Partnership to develop national IA/IT Training and Certification Standards for IA/IT professionals
- DOD–DHS Partnership to develop and promote a Federal Software Assurance Initiative focused on state-of-the-art capabilities to discover the presence of mal-ware in commercial or government developmental software

[5] The Distributed Component Object Model allows direct communication over the network between software components. The Remote Procedure Call is a protocol of the Windows operating system that allows a program from one computer to request a service from a program on another computer in a network, thereby facilitating interoperability.

[6] The CERT® Coordination Center (CERT/CC) is a center of Internet security expertise at the Software Engineering institute, a federally funded research and development center operated by Carnegie Mellon University. CERT/CC is a major center for analyzing and reporting vulnerabilities, as well as for providing information on possible solutions.

[7] Formerly within the General Services Administration and now part of the Department of Homeland Security, FedCIRC was established to provide a central focal point for incident reporting, handling, prevention, and recognition for the Federal Government.

[8] Routers are hardware devices or software programs that forward Internet and network traffic between networks and are critical to their operation.

- DOD–DHS Partnership to conduct a comprehensive review of the National Information Assurance Partnership (NIAP) process to examine its efficacy and extensibility to the Federal and Civil environments
- DOD is also actively engaged with DHS on the Committee for National Security Systems (CNSS) and is working extensively on E-Gov initiatives such as E-Authentication.

Mr. DACEY. DOD should continue working with DHS to help respond to information security incidents and threats. For example, according to its fiscal year 2002 government information security reform report, the DOD CERT (computer emergency response team) works closely with FedCIRC on all incidents within the .gov domain. In addition, DOD's Joint Task Force for Computer Network Operations and the DOD CERT take responsibility for incidents within the .mil domain, but reportedly also work closely with FedCIRC on significant cyber incidents, sharing threat information and providing analytic support. As another example, elements of DHS, the Federal Bureau of Investigation's Counterterrorism Division, the Director of Central Intelligence's Counterterrorist Center, and DOD are participating in the recently established Terrorist Threat Integration Center, which is intended to fuse and analyze all-source information related to terrorism. Appropriate DOD intelligence elements are to participate fully in the center, providing information, and contributing to analytic efforts.

DOD can also assist DHS and other federal agencies in improving their information security by sharing information on practices and technologies successfully deployed by DOD, as well as the results of DOD research and development efforts. For example, the Federal Information Security Management Act requires NIST to develop federal information security standards and guidelines, including minimum information security requirements for information and information systems. In developing these standards and guidelines, NIST is required by the act to consult with other agencies, specifically including DOD, to assure use of appropriate information security policies, procedures, and techniques.

Mr. LANGEVIN. Mr. Lentz, do you foresee DOD and DHS working together on information security? Would that be advantageous? What does the rest of the panel believe?

Dr. SPAFFORD. Based on what I know and have observed, I believe we are only partially prepared. We have too many vulnerable systems being run by ill-trained personnel. We have some incident response capability, but it is not large enough in scope, nor sufficiently advanced technically.

If an attack were to occur, not only would it be directed at military and civilian parts of the government, but also at the civilian infrastructure. The success of Sapphire, Blaster, and other small bits of malware illustrate the patchwork responses that are currently in place and of mixed effectivness. A carefully-crafted attack using a previously undisclosed vulnerability could be quite severe in scope and effect.

I also do not believe we have the means to reliably find intruders or authors of malware, except in exceptional cases. There is too little in the way of forensic tools and technology available. There are too many systems with insufficient audit trails to determine what happened.

There is too much unknown code being run to be certain where an attack occurred. And the list goes on. There are hundreds, if not thousands, of attacks per year against Pentagon systems alone. How many are currently investigated and prosecuted? How many authors of malicious viruses that degrade military and civilian systems are tracked and prosecuted? If history is any guide, the majority of these people committing these acts are amateurs and thus should be easier to find than those who would perpetuate a major, malicious cyberattack.

Is it an issue of changing priorities? Yes, it is a matter of funding, technology, and will. In my original written testimony I provided a list of steps that should be taken to improve the security of DOD and government systems. Those are all issues of priorities.

Mr. LENTZ. DOD is currently engaging on several information security initiatives with DHS. They include:

- DOD–DHS Partnership to lead expansion of the 'Consensus-based Security Benchmark Development' across the public & private sectors
- DOD–DHS Partnership to collaborate on identification of 'Information Assurance Hard Problems' and Partnering on Research & Development Investments
- DOD–DHS Partnership on development of International Agreements to Share Cyber-Warning Information

- DOD–DHS Partnership to develop national IA/IT Training and Certification Standards for IA/IT professionals
- DOD–DHS Partnership to develop and promote a Federal Software Assurance Initiative focused on state-of-the-art capabilities to discover the presence of mal-ware in commercial or government developmental software
- DOD–DHS Partnership to conduct a comprehensive review of the National Information Assurance Partnership (NIAP) process to examine its efficacy and extensibility to the Federal and Civil environments
- DOD is also actively engaged with DHS on the Committee for National Security Systems (CNSS) and is working extensively on E-Gov initiatives such as E-Authentication.

Mr. DACEY. As emphasized in our written statement,[9] as greater amounts of money are transferred through computer systems, as more sensitive economic and commercial information is exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on commercially available information technology, the likelihood increases that cyber attacks will threaten vital national interests. Government officials remain concerned about attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence gathering, and acts of war. The disgruntled organization insider is also a significant threat, since these individuals often have knowledge that allows them to gain unrestricted access and inflict damage or steal assets without possessing a great deal of knowledge about computer intrusions. In addition, intrusion or "hacking" tools have become readily available and relatively easy to use. Also, the growing number of flaws discovered in software code increases the potential that these vulnerabilities may be exploited to launch attacks against specific targets or to distribute attacks widely through viruses and worms.

Over the last several years, we have made numerous recommendations concerning critical infrastructure protection (CIP), which involves activities that enhance the security of the cyber and physical public and private infrastructures that are essential to our national security, national economic security, and/or national public health and safety. Although improvements have been made, further efforts are needed to address the following critical CIP challenges:

- developing a comprehensive and coordinated national plan to facilitate CIP information sharing that clearly delineates the roles and responsibilities of federal and nonfederal CIP entities, defines interim objectives and milestones, sets timeframes for achieving objectives, and establishes performance measures;
- developing fully productive information sharing relationships within the Federal Government and between the Federal Government and state and local governments and the private sector,
- improving the Federal Government's capabilities to analyze incident, threat, and vulnerability information obtained from numerous sources and share appropriate, timely, useful warnings and other information concerning both cyber and physical threats to federal entities, state and local governments, and the private sector, and
- providing appropriate incentives for nonfederal entities to increase information sharing with the Federal Government and enhance other CIP efforts.

Finally, determining who is responsible for a cyber attack can be difficult because groups or individuals can attack remotely from anywhere in the world, over the Internet, other networks, or dial-up lines, and they can disguise their identity, location, and intent by launching attacks across a span of communications systems and computers. Among others who investigate such attacks, the FBI's Cyber Division coordinates, supervises, and facilitates the investigation of federal violations in which the Internet, computer systems, or networks are exploited as the principal instruments or targets of terrorist organizations, foreign government-sponsored intelligence operations, or criminal activity. These and other investigative activities have identified those thought responsible for some cyber attacks. For example, at the end of August 2003, an arrest was made of an individual for allegedly developing a variation of the Blaster worm.

Mr. LANGEVIN. Mr. Lentz, I understand that DOD is undertaking a program whereby all users must demonstrate knowledge of information security protocols be-

[9] U.S. General Accounting Office, *Information Security: Further Efforts Needed to Fully Implement Statutory Requirements in DOD,* GAO–03–1037T (Washington, D.C., Jul. 24, 2003).

fore they are given access to parts of the DOD network. Has this process begun yet? Can you tell us how it will work?

Mr. LENTZ. DOD policy requires all DOD employees and contractors with access to any DOD Information System to participate in annual Information Assurance user training. Policy also requires all personnel with primary responsibilities for the security of systems and networks, Designated Approval Authorities (DAA), to certify completion of a DAA training package.

We are in the process of establishing Information Assurance certification requirements for all DOD employees and contractors with "privileged access" to any DOD Information System (including out-sourced support systems). Policy memorandums, a Directive, and a Manual have been drafted and are in various stages of development or staffing. These provide detailed requirements to the Components, Services and Agencies to identify ail Information Assurance Workforce personnel by category, function, and level including full-time and part-time/embedded duty positions. After identifying each position requirement, they must then ensure the incumbent passes a commercial certification specifically approved for their IA category, function, and level. The implementation plan for these policies will require gradual compliance over a 4–5 year period.

In partnership with the Department of Homeland Security, DOD is working towards establishing national certification program standards that will ultimately be adopted not only by DOD and other federal agencies, but also by private industry.

Mr. LANGEVIN. I'd like to hear the panel's thoughts about whether or not we truly prepared for the possibility of large-scale cyber attacks? If not, what more needs to be done—is it a question of changing priorities? Do we currently have the means to physically find an intruder, whether it's a skilled individual or a rogue nation or terrorist group?

Mr. LENTZ. In the cyber world, DOD actively defends its networks everyday against probes, scans and intrusions. Our experience with defending our network against these frequent but generally small-scale attacks makes us well postured to deal with large-scale attacks. For example, the DOD has sustained and successfully defended against large Distributed Denial of Service attacks. These attacks have attempted to flood DOD networks and ultimately prevent network communications. However, the combination of predictive intelligence, defense-in-depth strategy and immediate, coordinated defensive action across the DOD has prevented these attacks from interfering with military operations. Our defense-in-depth concept employs technical and procedural means of defending our networks at every level from the desktop to major commercial Internet providers. By combining good security procedures with anti-virus software, patch management, network sensors to track malicious traffic and firewalls with router features to block malicious traffic, we have demonstrated that we can continue to react quickly and effectively to any scale of cyber attack. The widespread use of vulnerability assessments further enhances our understanding and sensitivities to potential attack points. STRATCOM, the newly assigned commander of network defense activities, has made network readiness a top DOD priority.

Determining the identity of intruders is one of the hardest problems the entire computer network industry faces. Intrusions are investigated as criminal offenses and we are becoming increasing successfully prosecute them. Because cyber crime is growing worldwide problem, there is increasing willingness on the part of law enforcement agencies throughout the world to assist us. While DOD does not have the resources to investigate and prosecute all intrusions, 188 cases were closed last year and 189 are currently under investigation.. Attributing intrusions to governments or terrorist groups has proven especially difficult. Once we trace back an intrusion to a country where we do not have close law enforcement or intelligence connections, finding the identity and affiliation of a person sitting behind an Internet address is extremely difficult.

C4I INTEROPERABILITY: NEW CHALLENGES IN 21ST CENTURY WARFARE

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES,
Washington, DC, Tuesday, October 21, 2003.

The subcommittee met, pursuant to call, at 11:17 a.m., in room 2212, Rayburn House Office Building, Hon. Jim Saxton (chairman of the subcommittee) presiding.

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

Mr. SAXTON. Good morning, ladies and gentlemen. Let me apologize. We just finished a vote. And so we are a little bit late getting started. But we will try to expedite the process here so we can move through this at a smart pace.

Good morning, ladies and gentlemen. The Subcommittee on Terrorism, Unconventional Threats and Capabilities meets this morning to assess command, control, communications, computer and intelligence systems—C4I—interoperability issues and lessons learned from Operation Iraqi Freedom (OIF). We are also interested to learn more about how these issues present new challenges in the 21st century.

Ensuring that systems work effectively together is a key issue for the Department of Defense as it transitions the military into a lighter, faster, more lethal force in the battlespace. Information technology plays a critical role in the department's transformation.

The objective is to decrease the decision making time process to effectively shorten the sensor-to-shooter time to deliver rounds on targets. Network centric warfare (NCW) is an essential element in the department's transformation.

The foundation of NCW is to use technology—computers, data links, networks—to connect members of the armed services, ground vehicles, aircraft and ships into a series of highly integrated local and wide-area networks capable of sharing critical data information on a rapid and continuous-time basis. NCW's components include: interoperability of various command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems.

NCW eliminates stove-pipe systems, parochial interests, redundant and non-interoperable systems, and optimizes capital planning investments for present and future IT systems. The sub-

committee supports the department's initiative to attain the goals of NCW by implementing network-centric activities and programs.

To provide our warfighters the most accurate real-time information, they must have the latest command, control, communications, computer and intelligence systems to receive and move that data over secure communication links. The key is to have this information move seamlessly within a chain of command and between the service commanders.

During OIF, the United States had over 170,000 military personnel in theater. With such a large number of people involved in operations that spanned several countries, it was imperative to have real-time C4I interoperability between the services at every level to coordinate missions, air-strikes, troop movements and to prevent fratricide.

Interoperability is more than just the individual C4I and weapon systems that move the information to leverage firepower. Interoperability also includes procedures and techniques.

But most importantly, interoperability is about people and how warfighters can obtain real-time access to intelligence and information to make informed decisions in battle. Information, access to it and how fast it can be delivered now determines combat power.

There are several C4I interoperability issues that should be addressed during today's hearing. These include Battle Command On the Move—the integration of command and control (C2), intelligence, logistics, force protection and weapon systems, bandwidth constraints and satellite communications and coalition interoperability.

These fundamental issues need to be addressed as the U.S. military transforms to meet and defeat conventional and asymmetric threats in the 21st century battlespace.

I would at this time like to yield to my friend, Mr. Meehan, for any comments he may wish to make.

[The prepared statement of Mr. Saxton can be found in the Appendix on page 183.]

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

Mr. MEEHAN. Thank you, Mr. Chairman. I am impressed by the success of our extensive military operations in Iraq. And I share your view that this success represents really the culmination of intensive investment in advanced command and control systems.

I returned recently from a trip to Iraq. And despite some misgivings about the way we are attempting to stabilize and rebuild, I can personally attest to the professional dedication of the men and women in uniform.

As for equipment and information systems, it is clear that the joint success of Operation Iraqi Freedom are the direct results of investments made 5 to 10 years ago. That said, I also recognize that many of the past and present shortcomings, as well as recognize the future challenges.

Information fusion is perhaps the greatest challenge, particularly in the intelligence collection and dissemination architecture. Yet,

the delivery of actual intelligence from the point of collection to the people who need to use it is a necessary and vital component of battlefield success.

There are many challenges as well. And I hope that this hearing serves, Mr. Chairman, the purpose of increasing our focus on the appropriate investments, whether they are financial or intellectual. And I look forward to the testimony of the panelists and thank the chairman.

[The prepared statement of Mr. Meehan can be found in the Appendix on page 186.]

Mr. SAXTON. Thank you, Mr. Meehan.

We only have one panel of witnesses for our proceedings this morning. I want to welcome our panel of witnesses who will testify on the importance of C4I interoperability following combat operations in Iraq.

They are: Lieutenant General William Wallace, commander of the U.S. Army's V Corps. He was responsible for the capture and occupation of Baghdad during Operation Iraqi Freedom.

His headquarters synchronized the decisive execution of the 3rd Infantry Division, the 101st Airborne Division, the 3rd Armored Calvary Regiment and the 82nd Airborne Division, the 2nd Cavalry Division, the 4th Infantry Division and the 1st Armored Division, along with the associated combat support and combat service support under the 3rd Corps Support Command. Presently, General Wallace is commanding general for Combined Arms Center, U.S. Army Training and Doctrine Command in Fort Leavenworth, Kansas.

Also, Lieutenant General Daniel Leaf, served as director of Air Component Coordination Element with the Coalition Land Forces Component commander in Kuwait and Iraq during Operation Iraqi Freedom. General Leaf served as the Joint Forces Air Component commander's representative to the land component commander. He worked with the Coalition Forces Air Component commander to develop the air and space strategy and coordinated close-air-support missions with the Army.

General Leaf acted as the coordinating authority between the land and air commanders. Presently, General Leaf is vice commander for U.S. Air Force Space Command.

Major General Keith Stalder served and continues to serve as the deputy commanding general of the 1st Marine Expeditionary Force (MEF), the command element for all Marine air, ground and combat service support operations during Operation Iraqi Freedom. During command operations, he was responsible for the MEF's rear headquarters.

From this vantage point, General Stalder was able to assess the effectiveness of the corps' C4I systems operating within the MEF and those networked to higher headquarters, sister services and coalition partners.

Brigadier General Dennis Moran, who served as U.S. Central Command (CENTCOM's), J–6 and was responsible for all programs that provide command, control and communications (C3), support to the commander of CENTCOM and his staff during OIF. In addition, he was responsible for the integration of all C3 support required by the ground, air and sea components of CENTCOM.

General Moran also provided the planning and execution of the communications architecture for Operation Enduring Freedom, as well as Operation Iraqi Freedom. Presently, General Moran is the director of Information Operations, Networks and Space for the U.S. Army.

Brigadier General Marc Rogers is the director, Joint Requirements and Integration Directorate, J–8 for the U.S. Joint Forces Command. He is responsible for integrating the national military strategy with the Department of Defense's (DOD) planning programming and budgeting system.

His directorate conducts reviews of future capabilities requirements outlined by the combatant commanders. The directorate focuses on the degree of interoperability among all force components and then validates emerging technology for testing through experimentation and demonstration.

At the outset, I ask unanimous consent that all members' and witnesses' written opening statements be included in the record. I also ask unanimous consent that articles, exhibits and extraneous or tabular material referred to be included in the record. Without objection, so ordered.

General Wallace, you may proceed, sir.

Thank you very much, all of you, for being here. And thank you for your patience.

STATEMENT OF LT. GEN. WILLIAM WALLACE, USA, COMMANDING GENERAL, UNITED STATES COMBINED ARMS CENTER AND FORT LEAVENWORTH

General WALLACE. Good morning, sir. Yes, sir. Good morning, Mr. Chairman and members of the committee.

My name is Lieutenant General William Wallace. I currently serve as the commander of the Combined Arms Center, where we support the Army Training through our four core missions of doctrine development, leader development, collective training and battle command.

I am pleased to be before the committee today. Your leadership of our country and support of our military are greatly appreciated. And I am honored by this opportunity to contribute to your endeavors.

I have submitted a full statement to the committee, which, as you have already said, will be made part of the record. I will now give a very brief opening statement.

I am the U.S. Army Training and Doctrine Command's proponent for battle command. I hope to be of assistance to you by sharing my Operation Iraqi Freedom experience and insights from the perspective of the former V Corps commander during our operations to liberate the country of Kuwait—or Iraq.

I would suggest to you that we enjoyed great success in C4I compatibilities and joint network enhanced fighting during the recent fight. But there is still some work to be done.

I believe we need to push the goodness gained by network enhanced operations down to the tactical level. I believe that we need to design and field tactical command posts capable of Battle Command On the Move. And finally, I think we need to put some effort into overcoming what I refer to as the "digital divide" that exists

between the combat soldier and the information that he needs to fight in complex terrain and against a determined enemy.

With regard to command post, I believe we are capable of fielding Battle Command On the Move capabilities. Stationary command posts, in my judgment, do not support large-scale maneuver warfare.

I believe commanders should be untethered from fixed command post structures. And I believe that our experience in Iraqi Freedom proved that Battle Command On the Move works.

My own command post, a small number of vehicles, a small number of soldiers, was linked to the battlefield by commercial narrow and wide band satellite connections that enabled me to observe the fight through the use of a system called C2PC, command and control personal computer. That computer and that network allowed us to see both my formations, those of the Marine Expeditionary Force and those of the coalition forces on the move during the course of the fight.

We also had the capability of a thing called Blue Force Tracking, which has received some accolades during the course of the fight, which gave us the granularity to see individual vehicles during the course of the battle. All of that linked together with a capability to provide long-range voice communications through wide band tactical satellite communications enabled us to maintain Battle Command On the Move capabilities from my command post.

I would suggest that that capability needs to be pushed down further in the chain of command in our command post structure, so that organizations from battalion all the way to corps could enjoy that kind of connectivity. I believe that mobile satellite network command posts can have a smaller footprint on the battlefield.

I believe it is feasible to give some traditional command post functions to distant sanctuary command posts or even home station operation centers and, in so doing, enhance the deployability of our formations, reduce the drain on strategic lift. I also believe that smaller command posts, because of the size of their footprint, would be more survivable based on the smaller physical presence on the battlefield.

My experience also suggests that terrestrial-based communications limit our warfighting capability under conditions of complex terrain. Near real-time satellite network connectivity, in my judgment, is the key to gaining enhanced situational awareness effectiveness in that kind of terrain.

In summary, Mr. Chairman, Operation Iraqi Freedom proved the effectiveness and potential of network enhanced warfare. We know it works. Applying lessons that we learned, we can improve our C4I capabilities by discarding technology and concepts that did not work and pursuing those that did.

The Battle Command On the Move concept works. We just need to build a command post structure that supports it.

I believe satellite-based communications work. But we need to enhance our ability to take advantage of the available bandwidth and better manage the bandwidth that is available to push the synergy of the network enhanced operations down to the tactical level.

I believe that once we overcome the digital divide, then we can push the synergy of the network and the enhanced operations that that holds to the heroic soldier in the dirt. I would also suggest to you that we also need to understand and always remember that, regardless of the improvements that we gain and the networks that we build, warfare in the 21st century will remain lethal, up close and personal and that the American soldier, sailor, airman and Marine, supported by family and nation, will continue to be our most treasured and lethal weapon. Their bravery, heroism, sacrifice and compassion will continue to be our impression.

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

[The prepared statement of General Wallace can be found in the Appendix on page 187.]

Mr. SAXTON. General Wallace, thank you very much.

We will move now to General Leaf.

STATEMENT OF LT. GEN. DANIEL P. LEAF, USAF, VICE COMMANDER, UNITED STATES AIR FORCE SPACE COMMAND

General LEAF. Thank you, Mr. Chairman, members of the subcommittee. I am also honored to be appearing before you today, especially with such a distinguished panel of friends and fellow joint warfighters.

I cannot improve much on the basic precepts of your statement, Mr. Chairman, and Mr. Meehan's or General Wallace's. I would like to offer a few amplifications of my thoughts, in addition to the written statement that you have already accepted into the record.

My experience in Operation Iraqi Freedom was from a unique perspective of an airman with a land component. It was also somewhat unique because I had worked for the previous 3-plus years as the director of operational requirements—later operational capability requirements—for the Air Force; and thus, was involved in the formulating of the requirements and the basis for interoperability for the Air Force side of capabilities.

That was further improved upon, that view was improved upon, by an opportunity to travel throughout Operation Enduring Freedom, at the behest of the chief of staff of the Air Force, General Jumper, and Secretary Roche, to look at our kill chain, improving the timeliness of our time-sensitive and other targeting actions and ensure that we had as much network centricity and machine-to-machine communication as possible, not to eliminate the warfighter, not to eliminate the human element of combat, but to enable it.

From that perspective and some Goldwater-Nichols-mandated joint service, I think I had a unique seat, working for General McKiernan. My statement stresses the importance of the human element of warfare, not just at the soldier, sailor, airman and Marine level, but at the operational level, where the component commanders executed the combatant commanders' plan, I would say, brilliantly.

They did it as true joint teammates. And that was fundamental to the success on the battlefield, General Wallace, your component, the Special Operations Component and our maritime forces.

That cannot be replaced by machines. It can only be improved upon. And I think it important to capture that, as we also capture the technical lessons learned and acknowledge the areas where we have room for improvement.

We have improved, as noted, because of investment. We have also improved because of innovation.

We have invested heavily in C4I systems. And we have innovated through joint experiment, joint exercises and taking what we have learned there and getting it to the field.

And specifically, we have transitioned 32 of 70 initiatives from Joint Expeditionary Force Experiment (JEFX) to the field in time for Iraqi freedom. That innovation and timely application of technology to the warfighters' problem is essential if we are going to succeed at the pace of change we face in the modern world.

We have a good structure now for examining interoperability. All of our acquisition programs at level two or higher require a key performance parameter for interoperability.

Those parameters have to include critical information exchange requirements. In the Air Force, in fact, while I was director of requirements, made it mandatory not just for Acquisition Category (ACAT) level two and higher, but for all acquisition programs.

That is a very good measure for setting a foundational level of interoperability. We must be careful not to over-legislate interoperability or we will reach paralysis. We will not be able to turn initiatives and equipment advances fast enough to get them to the field.

Additionally, we have to be aware that there is some danger in homogeneity. Our components—and they are not Air Force components, it is an air component; it is not an Army component, it is a land component; and I know you all are well aware of that—bring unique capabilities to the fight.

We need to make them conceptually and technically interoperable without making them totally alike. Because their differences in capability, their are differences in approaches bring a broad spectrum against the enemy and enable victory.

I believe we demonstrated that. We do have room for improvement, particularly in avoiding fratricide, blue on blue and improving the situational awareness of the warfighter.

In terms of fratricide, zero is the only good score. And we are not there yet. We will continue to work that. The Army-led Blue Force Tracker initiative is an example of potential advances we can make in that area.

Additionally, I think, when it comes to bandwidth and the use of the available spectrum, we do not just need to improve our user equipment, as General Wallace accurately noted, we have to improve our awareness of the utilization of the spectrum. Just like we need an operationalized picture of air activity and land activity and maritime activity and space activity, we must have a picture, that operational commanders can use, of bandwidth utilization, availability and, in some cases, waste, so that they can set and implement priorities that lead to the efficient use of what bandwidth is available.

I look forward to your questions. And again, I am honored here to represent our Air Force with these great joint warfighters. I look forward to your questions.

[The prepared statement of General Leaf can be found in the Appendix on page 196.]

Mr. SAXTON. Thank you very much, general.

General Stalder, we are going to move over to you now. Let me apologize for mispronouncing your name in my opening statement, sir.

STATEMENT OF MAJ. GEN. KEITH STALDER, USMC, COMMANDING GENERAL, FIRST MARINE EXPEDITIONARY BRIGADE AND DEPUTY COMMANDING GENERAL, FIRST MARINE EXPEDITIONARY FORCE

General STALDER. No problem, sir. It happens quite frequently, actually.

Thank you, Mr. Chairman and members of the subcommittee. I appreciate this opportunity to discuss the First Marine Expeditionary Force's experiences and observations from Operation Iraqi Freedom.

I served as the deputy commanding general throughout the operation. And I returned from Iraq last month.

Thank you very much for your support of our armed forces. Command and control systems generally were very effective and conveyed commanders' intent, reports, orders, intelligence and overlays well. They supported constant communications between and among the MEF commander, our subordinate commanders and the joint and combined units and headquarters that made up our force.

During Operation Iraqi Freedom, the MEF performed many of its tasks and missions in the time-proven tradition of the Navy-Marine Corps team. But the Marine Corps had never operated and conducted sustained operations in combat so far inland until now.

Our command and control facilities and equipment required tactical and operational flexibility and mobility greater than envisioned. The system performed remarkably well under the very harsh conditions we encountered.

The Marine Corps installed, operated and maintained the largest and most complex architecture in our history. It required 80 percent of the Marine Corps' communications assets and the augmentation of commercial satellite resources as well.

We supported both Marine and British coalition forces. And while there were challenges and there are needed improvements, the overall consensus from commanders at every level was that communications and interoperability worked well.

No amount of technology can eliminate the human dimension of war. Our best command and control system is still a well-trained Marine.

With me today is Colonel George Allen, who served as the MEF assistant chief of staff for communications during Operation Iraqi Freedom. I am honored to appear here before you today and look forward to your questions.

Thank you.

[The prepared statement of General Stalder can be found in the Appendix on page 199.]

Mr. SAXTON. Thank you very much, sir.

General Moran.

STATEMENT OF BRIG. GEN. DENNIS MORAN, USA, DIRECTOR OF INFORMATION OPERATIONS, NETWORKS AND SPACE, OFFICE OF THE CHIEF INFORMATION OFFICER/G–6, DEPARTMENT OF THE ARMY

General MORAN. Mr. Chairman, members of the subcommittee, thank you for the opportunity to provide testimony describing Operation Enduring Freedom and Operation Iraqi Freedom C4I lessons learned, based on my experiences as the director of command, control, communications and computers or what is better known as the CENTCOM J–6.

And I need to add, it is an absolute professional pleasure to be here, not only with these great warfighters, but in front of this committee, with the important work that you have to do.

Prior to 9/11, the US Central Command Area of Operation was an economy of forces theater that supported relatively small headquarters. The communications architecture to support the missions was austere, consisting of tactical satellite communications and a small amount of commercial satellite supporting widely dispersed sites.

During Operation Enduring Freedom, the communications architecture grew, literally and figuratively, in support of uncharted locations and C2 requirements. As the plan for Operation Iraqi Freedom came together, US CENTCOM leveraged lessons learned from Operation Enduring Freedom concerning force numbers and C4 requirements. And the architecture changed dramatically.

Lessons learned from operations in Southwest Asia centered on three main topics: Beyond Line-of-Sight Communications; Battle Command On the Move; and coalition information sharing.

The first lesson I will address is beyond line-of-sight communications. As General Wallace has already stated, the required distances between command posts greatly exceeded the capabilities of the current military multi-channel line-of-sight communications equipment.

Solutions developed or adapted were hybrid military-commercial systems that proved invaluable in providing required critical communications links.

The second lesson learned was that of the speed of maneuver that produced distances well beyond—distances between lower echelon units that exceeded the capabilities of today's tactical radio systems. The Army, in response to this, fielded Blue Force Tracking and Force XXI Battle Command Brigade and Below, FBCB2, systems that would allow V Corps to execute Battle Command On the Move and maintain better situational awareness.

The last lesson learned I will mention concerns coalition forces. The coalition forces require an unprecedented amount of information to maintain an adequate level of situational awareness. US CENTCOM, in coordination with the Office of the Secretary of Defense—Network and Information Integration, NII, developed a coalition information sharing system called CENTRIXS, Coalition Enterprise Regional Information Exchange System.

This system provided command and control computer applications to allow the British and Australian tactical headquarters to receive the information they required.

In conclusion, the Army continues to take an analytical look at the lessons learned from Operation Enduring Freedom and Operation Iraqi Freedom, to determine what adjustments will improve near-term combat capabilities, as well as to better position itself for future successes. What is clear is the need to invest in both emerging technology and emerging operational concepts that will make our forces more combat effective.

The warfighter requires a global, interoperable, integrated network, which supports distributed planning and decentralized execution. The services are working to ensure that improvements of the joint C4I architecture and the systems to support that vision.

Mr. Chairman, I look forward to your questions.

[The prepared statement of General Moran can be found in the Appendix on page 214.]

Mr. SAXTON. General, thank you very much.

And now we will go to General Rogers.

STATEMENT OF BRIG. GEN. MARC ROGERS, USAF, DIRECTOR, JOINT REQUIREMENTS AND INTEGRATION DIRECTORATE, J8, UNITED STATES JOINT FORCES COMMAND

General ROGERS. Mr. Chairman, distinguished members of the committee, good morning. I am pleased to appear before you today to discuss 21st century challenges to command and control for joint warfighting.

United States Joint Forces Command, under the command of Admiral Ed Giambastiani, continues to advance our Nation's joint capabilities through concept development and experimentation, advancing interoperability, integrating joint capabilities, providing joint force training, providing trained joint forces to combatant commanders.

My personal focus at Joint Forces Command is on improving joint command and control effectiveness by working to improve and resolve interoperability issues and to integrate service and joint command and control capabilities. Our battle management command and control efforts are aimed at providing an integrated, interoperable and networked joint force.

The primary goal is to give our people the best capabilities to plan, coordinate, control, direct and assess joint operations. And as you said in your opening remarks, Mr. Chairman, it is all about people, what real people have to do in real combat situations, sometimes under stress, at all levels of the operation.

I want to thank the committee for your continued support of our armed forces and specifically for the soldiers, sailors, airmen and Marines and their families who make sacrifices every day on behalf of this nation. They are the ones who deserve our best efforts. And I look forward to working with the committee toward that end.

I look forward to your questions, sir. Thank you.

[The prepared statement of General Rogers can be found in the Appendix on page 224.]

Mr. SAXTON. Thank you very much, General Rogers.

We will move at this point to see what kinds of questions we can drum up for you fine folks. And we will start with the ranking member, Mr. Meehan.

Mr. MEEHAN. Thank you, Mr. Chairman.

General Rogers, the Department of Defense has several planned information architectures, including the Global Information Grid (GIG), the Army's twin T, the Navy's FORCEnet and the Air Force's C2 constellation. One might expect various architectures to address functional issues. But the current split—it seems to me, along service boundaries—raises the question of parochialism that is inconsistent with today's joint cyber environment.

Is there an overall DOD information architecture? And are these various information architectures compatible? And will they convert?

General ROGERS. Sir, I would address that question two ways: one, in terms of parochialism or any perceived parochialism, I will tell you that, in my hat, trying to improve joint interoperability and integrating joint capabilities, I have received nothing but enthusiastic engagement from the services. I was pleasantly surprised when I went to Joint Forces Command and found that every service is far beyond what may have been perceived from a few decades ago.

And all are interested in ensuring that their future command and control architectures are joint from the beginning in terms of architectures that need to be net-centric and be able to operate in the GIG, within the GIG construct.

In terms of legacy systems, all are interested in one second facet, and that is the ability to maintain a capability while we transition to full net-centric capability. And to that end, Joint Forces Command has partnered with the Office of the Secretary of Defense, specifically the undersecretary for acquisition, test and logistics, to build a battled management command and control road map, which is specifically aimed at, over the next several years, attempting to migrate various service systems to an interoperable structure.

I hope that answers your question.

Mr. MEEHAN. So there is an overall DOD information architecture. And, over the next several years, if I understand the answer, these various information architectures will converge and become compatible?

General ROGERS. That is our hope, sir. It is a tremendous challenge, as you can imagine. But that is our hope, is that we will be able to bring together a number of integrated architecture—we call it integrated architectures—to achieve the net-centric capabilities in the future.

Mr. MEEHAN. Thank you, general.

General Moran, how did CENTCOM physically provide the infrastructure for information interoperability in Operation Iraqi Freedom? And was this task tantamount to building a DOD intranet in Iraq?

General MORAN. Sir, what we were focused on providing to the warfighting forces were a number of communications capabilities—secure voice, non-secure data, secure data and video teleconferencing. Those were the four services that we knew had to be delivered to almost every level of command and control.

And so what we did, in coordination with the Army, the Air Force, the Navy and the Marine Corps, is to develop a communications architecture, which used predominantly military and commercial satellites, that brought bandwidth to command post locations

throughout the theater, which delivered those services and created the secure and the non-secure internet that you just referred to in your question and also gave the commanders the capability to communicate, via voice, both within the theater and then back to the Continental United States or to Europe or to the Pacific, and also the capability to do secure video teleconferences from many places on the battlefield, either within the theater or back to the Continental United States, Europe or to the Pacific.

Mr. MEEHAN. General, what physical infrastructure was most successful?

General MORAN. First of all, the military infrastructure, the green boxes that we had invested in over time in the Air Force and the Army, the Marine Corps, was extremely successful. So the capabilities, which our soldiers, sailors, airmen and Marines train on every day provided the baseline of communications that the command posts needed.

But the commercial communications, the commercial satellite communications that we brought into the theater, were needed because our military communications did not have the full capacity necessary to meet all of the needs for secure voice, secure data, non-secure data and video teleconferencing for those command posts. So we made complete and very successful use of the military system that we had already been fielded.

And we were able to leverage commercial, state-of-the-shelf architecture—or state-of-the-shelf equipment, commercial equipment, to meet those needs that were beyond the capabilities of our military system.

Mr. MEEHAN. Let me ask the general, what IT investment did CENTCOM make into the region that provided for this robust networking capabilities during the conflict?

General MORAN. I am going to key on your word "investments." There were some operational things that we did—and let me speak to those first—that demonstrate that the department attempted and did, in fact, give Central Command all of the satellite capability that was possible with military satellites.

We, in fact, moved a number of military satellites so that they were in a better position to satisfy our forces, both within Afghanistan and Iraq. And we even, through agreements with Australia, leased a satellite, which also provided some communications specifically for Afghanistan, but gave us some capacity then that was available to us in Iraq.

From an investment perspective, we invested in Ku commercial satellite terminals that were transportable; in other words, they could be picked up and moved from location to location. And we invested in state-of-the-shelf data communications systems that are available from companies like SISCO or other commercial companies. And we invested in telephone switches and computers that gave us and created the capability for the services' data, voice and VTC that the commanders and the warfighters required.

Mr. MEEHAN. Thank you, general.

Last question, General Wallace and maybe General Stalder, how did Blue Force Tracking work, with respect to your troops and Marines? And what is the difference between Blue Force Tracking and

combat identification? And are we going to need both for a future operation?

General WALLACE. Sir, first let me explain to you my perspective on Blue Force Tracking. First of all, I think it was an extraordinarily successful fielding. But it was a relatively thin fielding to the formation.

On average, the U.S. Army divisions that received Blue Force Tracking only got about 150 systems per division. And that was based on limitations in satellite capability and just the physical capability to produce those numbers and get them in the field in a relatively rapid fashion.

The Blue Force Tracking systems were put primarily in commander's vehicles or vehicles that we assumed would be in close combat with the enemy, such as reconnaissance units. The system itself, the Blue Force Tracking system itself, worked very well.

It was satellite based. It provided to those folks that did have Blue Force Tracking visual signals as to where they were in relationship to the formation in which they were moving. It also gave them real-time view of other Blue Force Tracking-equipped vehicles and equipment, regardless of where they were in the formation.

What Blue Force Tracking did not do, because of the level of fielding, it does not give you individual vehicle views because of the thin fielding that I mentioned a moment ago, which leads to your second question with regard to situational awareness and potential for fratricide avoidance.

It is my judgment that Blue Force Tracking provides the ability to deny fires to occur. But it does not clear fires. And by that, I mean you do not have any guarantee that a Blue Force Tracking-equipped vehicle is, in fact, having a malfunction in that system.

So to answer the latter part of your question, in my judgment, there is going to have to be some kind of identification friend or foe system that complements Blue Force Tracking. But it, in and of itself, I do not believe is a solution.

General LEAF. May I, Representative Meehan? I would like to concur with General Wallace and add to that a little bit.

Blue Force Tracker is part of the overall combat identification matrix. But it does not, as he noted, give specific ID. And it is not of the fidelity or latency, at this point, to enable, for example, danger close expenditure of organs where friendly forces are at risk.

Because of its potential, however, the secretary of the Air Force and the chief of staff of the Air Force visited Air Force Space Command some weeks ago and gave us strong direction to look at how we can improve, enhance and expand the role of Blue Force Tracker, as part of our overall situational awareness.

There are ways to reduce the latency by using an atmospheric relay, as opposed to a satellite relay. There are ways—money, principally—to expand the fielding of systems that we can and should look at doing that, as we integrate it into an identification friend or foe and other means of combat identification that can technically identify enemy or friendly systems.

So we see, in the Air Force, while the Army continues its leadership of Blue Force Tracking initiatives, a great need for our serve to step up to it as part of combat identification and to expand its utilization.

Mr. MEEHAN. General Stalder.

General STALDER. Sir, I concur with General Wallace's comments on their experience in the use of Blue Force Tracker. We had two different systems. We used the MTS 2011, which is referred to generically as Blue Force Tracker.

And we also used the Marine Corps' program of record system, which is called MDAC. We fielded 319 MDAC, 177 Blue Force Trackers to Marine units and 47 Blue Force Trackers to UK units.

That coverage allowed us to function and operate much in the same manner as our colleagues in V Corps did, by pushing those systems to the most forward elements and those elements that might come in contact with the enemy in a situation where it required us to have as good a situational awareness as possible, as to the disposition. It was by no means complete coverage.

With respect to Blue Force Tracker, it is certainly useful and additive to the combat identification problem. But it is by no means a complete solution. It does not have the fidelity. And the shooter, who is ultimately the one who will make the decision on whether or not to engage a target, does not have the information they need from Blue Force Tracking system to do that with the precision that we would all like.

Mr. MEEHAN. Thank you very much. And thank you for your outstanding answers. And thank you for the great work that you do for the country.

Mr. SAXTON. Thank you, Mr. Meehan.

I move now to the gentleman from Minnesota, Mr. Kline.

Mr. KLINE. Thank you, Mr. Chairman. Thank you, gentlemen, for being here. And thank you for a terrific job in Iraq, just a terrific job.

We are all so proud. And I know you know that. And you are proud of your troops and your airmen and your Marines. But we are also.

In every operation that I ever participated in back in my days in uniform, whether it was real or training, there was always an after-action in which we stood up and concluded that command, indeed, was perfect—because obviously we were the commanders—but we did not have enough intelligence and the communications was terrible.

I am hearing a little bit different story from you today. We just heard that Blue Force Tracking was a little thin and needed to be improved.

I would like to hear, particularly from the ground force commanders in either order, what else was broken. What could you not do that you really felt that you needed to do, in the sense of communication of control and com?

General WALLACE. Sir, I will take a whack at it. Several things come to mind.

First of all, we realized early in the fight the importance of nonterrestrial communications, specially wideband technical satellite or SATCOM communications. There was insufficient frequencies allocated to provide that technical satellite communications to all the formations that needed it.

As I recall, the V Corps had allocated about eight frequencies, as I recall, several of which did not work because of what is referred

to as "low look angle;" that is that you cannot acquire the satellite with a high degree of efficiency, and therefore, the satellite communications channel is corrupted.

Second, we had problems with some of the frequencies themselves, with corrupted channels on the satellites. And as I recall, three or four of the frequencies that we were allocated were just not usable for the purposes that we needed them.

Has to do with the comment that I made during my opening statement, with regard to frequency and bandwidth management. I think we have to do a better job in that regard to provide to he who needs it the frequencies and the spectrum and the bandwidth that they need at the time that they need it.

Mr. KLINE. Excuse me, where does that management need to take place?

General WALLACE. I believe it takes place at the joint headquarters level, because they alone are responsible for the bandwidth within the theater. And they alone have the responsibility for providing the bandwidth to all the components.

Mr. KLINE. So in this case, CENTCOM itself?

General WALLACE. Central Command, with the recommendations from the component commanders, in my judgment.

The second thing that we made great inroads on but need to continue to work on is the notion of Battle Command On the Move. From my command post, we could move. And in fact, I could have real-time visualization of both the enemy and friendly locations, location of artillery, the fans of fire of those artillery systems.

What we could not get on the move, however, was real-time satellite imagery or real-time pictures from UAVs, for example. We had to stop, elevate our antennas for larger bandwidth to receive the streaming video from the GBS system in order to get those pictures.

Further, although I could get that at my command post by going to a short halt and erecting those antennas, it was very difficult to push those images down to lower levels of command. The brigade level command posts generally did not have that capability. And certainly, the battalion level command posts did not.

So I think one of the things that we need to work on in the future and one of the things we saw limitations in was being able to get information that was available to us at higher echelons of command down to the lower echelons of command, where it is most needed and where the most granularity is necessary to fight the fight.

Mr. KLINE. And that is, since time began, that is a problem. Is that an equipment issue?

General WALLACE. In my judgment, it is both an equipment issue. It is a bandwidth allocation and management issue. And it is also the design of the command posts, to make them smaller and more mobile, so they can accept the feeds that we are providing them. And the command posts can continue to move with the formations that they are a part of and still take advantage of the information that is available, but presently we are unable to push down to them.

Those would be my initial remarks, with regard to your question, sir.

Mr. KLINE. Thank you.

General Stalder.

General STALDER. Sir, I will make a couple of comments on things that I think need more work. I would not characterize these as irretrievably broken.

Mr. KLINE. Certainly, there were times when you just could not talk and it had to drive you crazy? It always has. I am just trying to find out if that is still there and what it is.

General STALDER. Sir, there were rarely times when we were absolutely and completely out of communications, either at the MEF headquarters level or down at the lower levels. Everything General Wallace told you with respect to Command On the Move was certainly true of our forces.

But in terms of creating any major friction points or rubs, we did not experience any major problems like that. We experienced one issue that gave us cause for concern.

A couple of nights into the war, misplaced our command post to Talil in Southern Iraq. And we had only one means of communicating with them. Ordinarily, we have two or three. That caused us some concern.

Command of the operation was passed back to me in Commando Camp at Kuwait very briefly. The cause of the concern was the weather. A sandstorm was occurring at that point that nobody had remembered anything the like of in all of Iraq's memory.

And at the MEF level, that was the only time when I was very concerned. But we maintained communication and we continued the battle.

So that is my perspective from our experience.

Mr. KLINE. I see my time has expired. But how did you maintain communications? What was the——

General STALDER. We did it with satellite communications.

Mr. KLINE. SATCOM. Okay.

Okay, I am allowed another minute or so here. If you have some more "it did not works."

General STALDER. Sir, these are the things that I think need work. I would characterize them that way. I will not spend a lot of time on each one.

Combat identification needs work. General Wallace spoke to the digital divide, communication on the move and beyond line-of-sight communication and bandwidth. The integration of our combat support.

By those applications, I mean Theater Battle Management Care Systems, Advanced Field Artillery Tactical Data System (AFATDS), Asset Tracking and Accountability Control System (ATACS), Airborne Seperation Assurance System (ASAS), IOC. I apologize for the alphabet soup. But all of those systems are only marginally interoperable.

They are legacy systems. And improvements certainly are in the offing. But in terms of capability for the warfighter, that would be very valuable.

The applications that we support coalition operations with, need work, centric-specifically. While well suited for higher levels of command, it is not as responsive at the tactical level, in terms of communicating the mass amounts of information and data that are

required to be shared with the coalition warfighting partner at the coalition level.

And finally, human intelligence is always something that will be extremely valuable. As the MEF, with the V Corps, began our attack on Baghdad and ultimately the capture occurred, our human sources in that portion of the battlespace were extremely limited.

Mr. KLINE. Right. Let me, just one more, if I might, Mr. Chairman, because we have talked about assignment of frequencies and bandwidth. General Moran, you were the J–6?

General MORAN. Yes, sir.

Mr. KLINE. Presumably, you were involved in that allocation?

General MORAN. Absolutely.

Mr. KLINE. I am not accusatory. I am just trying to——

General MORAN. The issue that General Wallace is talking about and if I had to say what was broken is there simply was not enough bandwidth at all levels of command to give the warfighters at the battalion—at the brigade level—the kinds of information they needed to be more effective. The current suite of satellites that we had and we utilized that did an extremely good job of providing adequate bandwidth down to the division level, when you went from the division level down the brigade, down to the battalion and then even further down to the companies, there just were not sufficient systems, as General Wallace alluded to, in a sufficient bandwidth, to provide them all of the information they needed to be effective.

So what are we doing to fix that? First of all—and again, I am speaking from my Army position, where I am in the Army staff now—as we look at the lessons learned that we have from Iraqi Freedom, the first thing that it is doing is validating the architectures—the communications architecture, the command and control architecture—that we have in our future combat system,; albeit that that system is not going to be delivered for a number of years. But it validates the technologies that we are trying to place down at the combat vehicle level, the lowest level, is going to give them the kind of information that they are going to require to be more effective.

If you tie the investments that we are making in the JTRS radio, the Joint Tactical Radio System, and if you tie that to the investments that we are making in the wide band gap filler satellite system, which will be coming on board in about 2 years, you look at the investments that we are making in the advanced DHF satellite system, with the ground terminals that will be in these formations, we are moving in the right direction to take that bandwidth starved formations and pushing bandwidth down to those organizations.

And the last step, which will be the least further out, is the need to continue in the investments in the transformational communications architecture, which is really going to give us, because of the kinds of technology we will get in that satellite constellation, give us the real capability that we will require, the objective capability, for Battle Command On the Move, where we will be able to move operational information, intelligence information, logistics information—I do not want to say freely, but certainly with much greater ease than we have now.

What we in the Army are doing right now is examining the programs that exist in the fiscal year 2005 budget. And we are making decisions that must be approved by the Army leadership, must be approved by the Department of Defense leadership and finally, will be presented to the Congress next year, which will show the changes that we would like to make in systems that will overcome the deficiencies that have been identified in Iraqi Freedom and our war in Afghanistan.

Mr. KLINE. Thank you. And I presume there is multi-service discussion and collaboration in that effort?

General MORAN. Sir, you are absolutely right. And General Rogers mentioned the joint battle management command and control road map, which is a Joint Forces Command and a DOD level effort to synchronize, across time and across domains, all of the command and control systems within the Joint Force. And they recognize the information that must be at the joint level.

But as General Leaf stated, it recognizes the unique requirements that the Air Force, the land component and the naval component has, so we can satisfy not only the needs of the Joint Force commander, but meet the needs of that specific commander that is in the air, on the land or in the sea.

Mr. KLINE. Thank you very much. And thank you, Mr. Chairman, for your indulgence.

Mr. SAXTON. Thank you, Mr. Kline.

Mr. Larsen, please.

Mr. LARSEN. Thank you, Mr. Chairman. Got a set of questions. I am not quite sure who to start with. But I may start with General Wallace.

We talked ahead of time a little bit about a few of these things. But I wanted to ask you about the question of digital divide. And I hope we do not—this committee—lose sight of the point you are making about the digital divide between operational level and tactical level.

But I would like you to discuss, if there is a digital divide between us and our coalition partners, our ability to share information on the ground, as is needed—and not that it is wrong for us to get too far ahead of any other country in terms of our technology, but what that might do for our ability to work in a coalition setting in the battlefield?

General WALLACE. Yes, sir. My judgment is that there will be a separation in capability between our forces and those of whatever coalition that we might operate as a part of. And I think the operative word is "any coalition."

We need to be prepared to operate to the same degree of efficiency with our British friends and Australian friends who may be more advanced than others in their command and control and IT technology. My judgment is that the only way to truly solve that problem is to recognize the importance of liaison teams that are sent out from our headquarters to become part of coalition headquarters and share with them the information that we have available to us.

I think it is probably unrealistic for us to expect those coalition allies, because of the level of spending that they have within their

own defense budgets, to buy the same capabilities that we ourselves enjoy.

Mr. LARSEN. I want to ask a question of maybe General Rogers. And maybe someone else can chime in as well.

In our background, an issues statement that was given to the committee, I want to just highlight a few statements that were made. We have to have the ability to move data over secure lines. We depend upon the security of our information technology infrastructure in order to move this data from command down to the tactical level.

The network itself, as a result, becomes a weapon. The fact that we have this network becomes a weapon.

Earlier this year, in our defense authorization debate, we cut about $2 billion out of the IT programs overall in DOD, largely just across the board. We did not really, I think, have a full consideration of the impacts of what that might mean on the security of our technology infrastructure within the department.

So that is sort of a context for the question for General Rogers and anybody else that wants to answer it. What if we faced a more technologically capable enemy than we did in Iraq?

What if our enemy perhaps certainly was not as far down the road as we are, in terms of our ability to integrate information technology into our warfighter, but they still had the ability to get inside our systems, get inside our—not past our front lines, but sort of get inside our fiber optic lines and inside our satellite communications?

What are we doing to prepare for that?

General ROGERS. Sir, I will tell you, you hit on a number of areas that we have been wrestling with at Joint Forces Command. And a couple of your observations I believe we would share, one being that the network can in some ways be viewed as a weapon system.

I will say that one thing we have learned about collaborative capability is that you build a collaborative information environment, it is more than just an application or an ability to communicate. It becomes an extension of the commander's operating environment.

And he needs to know how to control it, protect it, maintain unity of command within it, maintain unity of effort and hide it, so to speak. The network itself that he is going to have available needs to be one that is self-healing. We hope we can achieve that.

And he needs to know and his communications, his knowledge managers, need to know how to manage those things; damage control, if you will. And yet, subordinate units need to be enabled to continue operations.

All of these things point us down, as when we look to the future and know that we need to work with coalitions, share information, we need to attack aggressively the issue of multilevel security. There are some policy issues that would come to play there as well.

I will tell you that there is a lot we do not know about how to fight inside a fully networked or a net-centric environment, across the board, top to bottom, horizontal, in coalition. And I largely think it is just because we just now got here in the information age.

There is so much that we are learning every day about what it means to be able to communicate on that scale and to have that much data flowing around the battlefield—up, down, horizontally—and train people on what to do with all of that and how to function within all of that, keeping in mind that while our technology has surprised us all with what we have been able to achieve, the same human brains in it are the ones who marched on Moscow back in history, Napoleon. And about 50 years from now, I do not think our human brains are going to be much different.

The question is how you enable those human brains, different levels in command and control structure, with all of this IT capability, to execute those functions that I mentioned in my opening statement—that planning and coordinating, directing, controlling, assessing, keeping situation awareness, et cetera.

General LEAF. If I may, Representative Larsen, from an Air Force Space Command perspective, but based on my experience leading a wing in Operation Allied Force, observing Enduring Freedom and serving in Iraqi Freedom, the inter-weaving of space capabilities in everything we are discussing today is so apparent. Not so apparent, I think, is the subtle assumption we have begun to make of space superiority.

They are not invulnerable, our space capabilities. And we have to remember that.

We have come to assume, just as we in some ways assume there will be air superiority, that we will have space superiority. It is incumbent upon Air Force Space Command and all our other providers of space capabilities that we recognize the importance, the asymmetric—in a positive sense—nature of those space capabilities and ensure that we are prepared to guarantee their availability to the joint warfighter, sailor, airman, soldier or Marine.

Mr. LARSEN. General Stalder.

General STALDER. I would offer that security is at least somewhat a function of having multiple paths of communications. And that is very important as we build our architecture.

My anecdote about the opening days of the war and the bad weather illustrates that pretty effectively. So even legacy systems that provide that multiple path capability and flexibility are going to be important as a defense against security threats in the future.

The other thing that provides us with some security or measure of security are the tactics, techniques and procedures that make up our command and control process. These are integrated planning or rapid planning, mission orders, commander's intent, appreciation for the single battle, freedom of action of subordinates, LNOs and high tempo operations as well.

Mr. SAXTON. Thank you, Mr. Larsen. Good question.

Mr. Thornberry.

Mr. THORNBERRY. Thank you, Mr. Chairman.

General Rogers, I want to go back to where Mr. Meehan started. He asked you, as I understood it, if there is an overall IT architecture for the department. And as I understood your answer, you said everybody wants to work together and that there are several architectures that you are working to make sure are compatible.

I do not mean to play semantics, but I am trying to understand whether there is one overall architecture, department-wide, that

brings everything together, kind of like a master plan. So that when the services have various items that they are looking to purchase or obtain, then you can compare it with the master plan and see whether that fits together.

I am thinking a document that we could even see. Is there that sort of one, overall master plan that brings it all together?

General ROGERS. Sir, to my knowledge, we are not there yet. That is our vision.

And this is, as I mentioned earlier, we just now got here in the information age. It is not an excuse. It is just that discoveries happen every step of the way.

And I think the vision is we would love to have one, single, overarching architecture that everyone could fit in. It calls for a degree of standards that allows services to design to and field systems that would be seamlessly integrated into that architecture.

It calls for a data management strategy and data standardization. You can extend from that all of the other pieces to it.

At the current time, we are working hard on joint operating concepts that drive such architectures. And as you may be familiar, it is a cascading effect between the operational architectures, systems architectures, technical architectures—all driven by what you have to do from your concept of operations and above that, your operating concepts.

So I hope that answers your question.

Mr. THORNBERRY. No, it does. And I appreciate your candor. I think one of the concerns this subcommittee has had is that we have lots of things moving along, buying things, but without kind of an overall picture of how it all fits together. We may be going back and trying to find some sort of fixes to bring even these newer things back into the overall system in the future.

It does not mean that you stop everything until you have the plan. But I think it is something that we are concerned about and that we need to be aware of.

I want to ask about one other issue. All of you talk about the limits on bandwidth and certainly with satellite communications.

I suspect everybody agrees that we will need more—not less—in the future. Part of the problem General Leaf talked about is the importance of space and getting things up.

General Moran, let me ask you, Admiral Cebrowski's Office of Force Transformation is involved in an experiment where they are going to launch a fast, cheap, small satellite for tactical use by PACOM next year. And the hope is that this will be an example of what we can do to dramatically improve the assets—enhance the assets—in space quickly, cheaply.

The other side of it is it may be a threat to some of the more entrenched space-launched systems. My question is, number one, are you aware of what Force Transformation is doing? And second, are you aware of this project that they are funding?

General MORAN. Sir, I am aware of it. I know that there is a project, but I cannot speak too much to the details.

But I can tell you that there has always been discussion, particularly within the Department of the Army, of how do we get cheap satellites? How do you get either low-Earth orbit satellites or high

UAVs or other systems that can loiter over the battlefield to meet the information and the bandwidth requirements we have?

I can tell you that, as we look at the operational architecture, the systems architecture for the future combat system, within the Army, from a communications perspective, we are going to rely on UAVs of some form to do exactly what you are describing, which is an attempt at the part of the battlefield that we are talking about that is bandwidth-starved, to give them an airborne capability for that network that will give them the connectivity they require.

Mr. THORNBERRY. General Leaf, are you aware of Admiral Cebrowski's office and what they are trying to do?

General LEAF. Yes, sir, I am.

Mr. THORNBERRY. My concern is, if it works well, is it something that the services or Space Command will help make sure gets taken up and, you know, get the ball and run with it? Or is it going to, even if it works well, could it be starved because it threatens some other existing program?

General LEAF. Sir, from my perspective, the one word answer would be absolutely. We are very much aware of the need for responsive space capabilities, not just responsive space launch, but improving the affordability to make it more responsive, improving and thus decreasing the time it takes to integrate any payload with the launch vehicle, our mobility on orbit, the ability to move these capabilities around and provide them in a focused manner.

And given that we have discussed the need for space superiority, there may be a requirement to replenish on-orbit capabilities if they are somehow addressed by a threat. So we are taking a very open mind and have several initiatives within the command, including an operationally responsive space lift study that will turn into a full-blown initiative as we work through the 2006 bomb, if we gain department and congressional approval of that expenditure, of course.

But we understand the need to be responsive and to be more flexible. And we are working very hard to do that.

Mr. THORNBERRY. Well, I think there are some others who are working very hard to do that too. If we want to look——

General LEAF. Yes, sir, absolutely.

Mr. THORNBERRY [continuing]. For answers wherever we find them.

Mr. Chairman, thank you. I have some other questions I would like to submit for the record.

Mr. SAXTON. Absolutely. Thank you very much, Mr. Thornberry.

Mr. Cooper.

Mr. COOPER. Thank you, Mr. Chairman.

General Wallace, I appreciate your heroism, not only having commanded the V Corps, but also in your willingness to speak your mind during that conflict. I am worried that, as we discuss technology here today, the best communications system in the world will not work well if the speaker on one end is not willing to speak the truth.

I am worried that you are widely viewed as having been put out to pasture at TRADOC for having spoken the truth during your command. So to me, the message for our troops, young and old,

should be: the truth comes first, regardless of what your superiors may think of it.

I hope, as we discuss communication, truth will not be omitted from the discussion because, to me, it is supremely important.

My colleague, Mr. Larsen, mentioned what if we faced an enemy that was more sophisticated? As you well know, we spend more in a day than Iraq spent on its military in a year.

Are we hardening our systems so that they will meet threats from more technologically adept nations? I know it is something that people are willing to discuss. Are we hardening the systems? Are they robust? Can they defeat jamming or other electronic interference?

General MORAN. Sir, let me try to address that from an Army perspective. As we develop our operational requirements for communications systems, we look at the threat environment that they are going to exist in.

And we try to determine, based on our best military judgment, what is the appropriate technology to invest in to meet the operational requirement. And the requirement for Electromagnetic Pulse (EMP) hardening has always been one that has been addressed, for example, in the MILSTAR program, and the need for there to be, on the ground, a terminal, a voice terminal, a data terminal that will exist in a nuclear environment that can provide the last-ditch communications.

We also know that some of our communications will not exist in that kind of an EMP environment. But I think it is a judgment of risk that the Army leadership in specific makes as they are gauging the risk of that kind of an environment against the affordability of that.

Another risk that we are very much concerned about is the cyber threat. And we are very much concerned in all of our communications on how vulnerable our computer systems are, how vulnerable are our telephone switching systems? How vulnerable are those systems to hackers?

And we are finding from day to day that the threat is much more capable than we had anticipated. And so we continue to make and work with industry to do common sense-type of mitigation efforts to give our systems—computer systems, communications systems—protection from that type of threat.

General LEAF. Congressman Cooper, if I may, from the air perspective, I would like to echo General Moran's thoughts. We strike a balance in hardening because it is technically challenging. It is expensive. And it is weighty. It adds mass, especially to orbital systems.

So we try to take a broad-based approach to guaranteeing the capabilities are available. Some of that is simply situation awareness. We are working very hard to expand our situation awareness, the threats to communications, such as jamming and other actions an enemy might take.

And operationally, through establishing 8th Air Force under Lieutenant General Carlson as our IO focal point for the Air Force to give a good operational awareness of cyber threats. And that has become very important.

But we need to harden when able and when required. But also look at offensive and defensive measures that will guarantee our capabilities are available.

Mr. COOPER. I know it is a challenge because the technology in this area is moving so fast. In fact, I think if someone were watching this back home and hearing all this technical discussion, they would say, "Hey, our FedEx trucks are tracked."

I understand Blue Force Tracking used part of that system. And it may have been the most successful part of the technology. If FedEx can do it, I am glad that our military can catch up and keep up with commercial technology that is available.

Also, when they hear about the need for pushing pictures up or down, you know, now the youngest teenager seems to have a picture cell phone. It works pretty darn well, photographing all sorts of things. They are probably wondering why our military does not have something like that when it is ubiquitous in the regular commercial market here in this country.

And when people hear line-of-sight radio discussed, they probably wonder, "Why would anybody ever want that?" So I worry that we are perhaps behind the curve due to military procurement, time delays, things like that. Because the commercial market, it seems to me, is always going to be faster.

Are there ways that you can keep tabs on absolutely the latest developments in the commercial marketplace, so that we can get those promptly in the hands of our troops?

General LEAF. Mr. Cooper, I think we do, sir. We have a good awareness of what is occurring in the commercial market. We work hard to transition commercial off-the-shelf initiatives, recognizing that our requirements are more stringent.

FedEx does a great job of tracking their packages and their vehicles. But again, when we have the lives of our warriors on the line in danger close situations, that may not be of appropriate fidelity or latency to expend ordinance based on that situation awareness.

The need for sharing imagery is driven by what we do with that imagery, not the mere presence of a picture. If we are going to have an imagery that is usable for stereoscopic viewing and precise mensuration of coordinates to derive latitude, longitude and elevation in 3–D—and that requires stereoscopic viewing—so that we again can expend lethal force based on that imagery in part, that is a much bigger picture than what I might send to my daughter at the University of California to show her what her mom and dad are up to.

Sometimes those images are good enough. And sometimes, the timeliness is good enough.

We have to recognize that it is not always real time. It might be right time. It is not always the perfect picture. It might be the right picture.

That is not so much, I do not think, an awareness of the commercial marketplace, sir, as defining our requirements in genuine terms—what is needed versus wanted—and continuing to build our information age, discipline, the doctrine, tactics, techniques and procedures that General Wallace alluded to.

We have room for growth there. But we are aggressively pursuing it.

Mr. COOPER. I hear the phrase, "state-of-the-shelf" technology, I cannot help but think: you wait until it is on the shelf? Aren't you working with the investors and manufacturers long before it hits the shelf, so that the robust military variant can be available as soon as possible?

General LEAF. Absolutely. We have a very strong interface in a variety of venues with industry, through industrial associations at our development centers, our product centers and simply through our informal contacts with industry as well.

And American industry, by and large, has been very forthcoming with bringing their innovations to us, sometimes with purely a profit motive, but at least they are bringing us the initiatives.

General WALLACE. Sir, if I might add, during Iraqi Freedom, we were actually provided, in each of our headquarters, a number of commercially produced satellite telephones that were securable, that were off-the-shelf items, that helped maintain communications in times when other, more conventional communications systems were either not available or had failed us for one reason or another.

Mr. COOPER. You mean like INTELSAT?

General WALLACE. I forget the name of the gizmo, but it was a little black phone.

General MORAN. The Iridium, sir.

General WALLACE. The Iridium phones, yeah. And it gave us a secure capability.

General STALDER. Sir, over in I MEF, we worked in a partnership with our industry colleagues and the Marine Corps Systems Command to develop and deploy what became the Marine Expeditionary Force Command Operations Center. It worked very, very well.

And we sent it into Kuwait in about mid-January. And it represented some of the best thinking and the best technology that all those partners could put together. And it worked extremely well.

Mr. COOPER. Thank you, Mr. Chairman.

Mr. SAXTON. Thank you, Mr. Cooper. Great question.

Mr. Wilson.

Mr. WILSON. Thank you, Mr. Chairman. And thank you all for your service. It is really encouraging to find out the success of the developments, say, of the broad band capability, 42 times that which we had in 1991. And I am familiar, we have read articles today and it has been discussed, about problems.

But I am very hopeful. Additionally, I appreciate the attitude about fratricide. I retired 2 months ago as the JAG officer.

And that was one of my assignments, of course, fratricide investigation. And I agree that we should be working to zero.

Also, I was concerned though, during my service, the level of communication—as the JAG officer, obviously they do not expose us to everything. But I was really startled.

We used the SINCGARS system. And the people in communications loved it. But it seemed like, to me, General Wallace, as you identified the satellite telephones, to me a secure satellite phone, I was hoping would be ultimately universal.

And so I appreciate you raising that issue.

This afternoon, General Leaf, a question: how successful were our joint operations with coalition airborne assets? Did we have

C4I interoperability with coalition airborne assets during missions? Or did we merely stay out of each other's way?

General LEAF. In Operation Iraqi Freedom, we had coalition members integrated at the combined Air Operations Center. I had RAF officers on my staff of the air component coordination element, with coalition forces land component headquarters.

And the interoperability at the staff level was very good. Now we had the same interoperability when I was a wing commander in Operation Allied Force, with the combined mission planning cell at Aviano.

But there was this, to some degree, a separation of assets in the fight. And the major missions were predominantly U.S. only.

The integration of coalition assets, particularly the RAF and the Royal Australian Air Force, in the fight, I think was greater in this conflict than ever before. I believe we have made great strides in taking the planning together to actually fighting together.

Mr. WILSON. And it sure was appreciated, to have their support in the coalition.

General LEAF. Yes, sir.

Mr. WILSON. General Moran, will the proposed common operational picture allow a more efficient engagement of U.S. and coalition troops?

General MORAN. Oh, yes, sir. Let me give you an example. Because we had an integrated common operational picture, we were capable of knowing where our special operating forces were, where our ground forces were. And also overlaid on that was the capability to, based on analysis, to lay down where the enemy was suspected to be.

And using the command and control systems that we use for time-sensitive targeting, because we were enabled with a common operating picture, that we knew where people were on the ground, commanders were able to make rapid decisions when a target of opportunity presented itself, to be able to, using those command and control systems, determine if there was a risk for a blue-on-blue. And once they determined that there was no risk, they were able to very quickly pass the instructions to the Air Force or to another weapons system to engage that target.

That quick response of sensor-to-shooter was enabled because we knew where our forces were, where we were and where the enemy was. So it was certainly a combat multiplier.

Mr. WILSON. And it seemed so successful, I want to just congratulate all of you on that.

And General Rogers, are the services committed to the net-centric warfare and interoperability? Or are technical solutions taking a backseat to parochial interests?

General ROGERS. Sir, I am lucky to be in a central seat to get a view of that. And at General Forces Command, as we work towards battle command and control solutions, I work with flag officers from every service and with the more technical officers at lower levels.

All of them have a strong interest in being able to operate in an integrated manner and a net-centric environment. And my main problem is I cannot keep up with the demand from the services for involvement in their projects.

I am working to resolve that, using some of this very technology that was used in Operation Iraqi Freedom, to make us, in a peacetime environment, more effective at solving these problems by integrating us into collaborative environments, et cetera, with the services, so that as we attack these problems, we do them together.

But bottom line, sir, is I see zero pushback from the services. The main interest is that they have the capability to deliver their service-specific core competencies when they come to the battle.

And that is what we are aiming to help them do. They want to be on the team. That is my own personal problem, is keeping up with the demand to provide them the joint help.

General MORAN. Sir, let me, if you do not mind, let me just give you an example where the services have voted with their pocketbook. And it is the joint tactical radio system.

That is a program which is going to be fielded to the land force, both the Marines and to the Army. It is going to be in air frames, both in the Army, the Air Force and the Navy. And it is going to be aboard ships.

And it is a program which has got a joint program office and where all of the services have brought their requirements, their operational requirements. Those have been vetted. We have determined what the technical solutions are. And we are moving forward with an investment strategy to put that radio, that will be a common radio, but at the same time, meeting the unique communications requirements that each of those services have and will make interoperability much easier to achieve for the joint force commander.

General WALLACE. Sir, if I might, I think most of our discussion today just kind of demonstrates our commitment on the part of all the services. I can speak from my perspective. Not only are we committed to net-centric or net-enabled warfare, but we want more of it.

That is why we are talking about bandwidth and frequency management. That is why we are talking about increased situational awareness for Battle Command On the Move, as well as fratricide avoidance.

That is why we are talking about joint-capable systems and not going our own way. And I just think, specifically from the Army perspective, but I think on behalf of all the other services, we are into it.

We are interested in it. And we just want more of it.

Mr. WILSON. Well, again, I want to thank you for your service. I am excited for you to be in the service as technology is expanding exponentially and how this can help our troops be more effective and safe.

Thank you very much.

Mr. SAXTON. Thank you, Mr. Wilson.

General Wallace, you just gave me a great segue into the question that I wanted to ask. You said that what we have is great. We just need more of it. Or words to that effect.

And that is good. That is very encouraging.

My question, I guess, is this—it goes along the same line—as I look back to the last major conflict in the Gulf, 1990 and 1991, we had a level of capability with regard to systems and communica-

tions, et cetera. And now today, a little more than a decade later, we have evolved to something that few people could probably dream about in the 1990, 1991 theater.

And it gives me rise to question what we will look like some years ahead; five years ahead or ten years ahead. Because you are all involved very much on a daily basis with these kinds of questions, project for us, if you could—let's not try to jump 10 years ahead. That is impossible.

Let's just say 4 or 5 years ahead. What do you see us looking like, in terms of capability?

General LEAF. Sir, I would offer, Mr. Chairman, that given that 5 years from now, we will have, by and large, the same systems that were used in Operation Iraqi Freedom, some new systems, what we will see is an improvement in machine-to-machine communication to increase the timeliness of data, decrease the error rate.

We will see better and more prolific user equipment. We will see concepts for integration that are formalized. They were developed by the component commanders and their major subordinate commanders, like General Wallace in Iraqi Freedom, and worked well.

But we will formalize those concepts. And I suspect that there will be a move towards multi-faceted situation awareness.

Because what we have spoken today about is kind of one dimensional. We could not even get it in 1990 or 1991, whether it was imagery, an ATO, whatever the information was.

Now we can get it. We have better access to it. It is more available, even with the digital divide.

But what we want to do is consolidate, amalgamate, fuse different sources of information, whether it is to build a picture from historical data or to recognize the nature of a changing situation.

So I would hope that that is where we are headed within 5 years, sir.

General WALLACE. Sir, if I might, I would agree with General Leaf, if you look forward 5 years, I do not see any dramatic changes in the equipment that is fielded to the force. I think what we will see are dramatic changes in our awareness, as based on recent experience, awareness on the part of all the services of the great goodness of network solutions and the great goodness of joint application of power across all the services.

I think that our emphasis over the near term needs to be on training of formations and leaders and development of young leaders who can take advantage of what we have seen in the recent past and advance those advantages in the future, so that we are creating both units and leaders that are very adaptable to any situation on the battlefield, using the technologies that are available in the very near term.

General STALDER. Sir, I would add to some of that discussion by saying that in 5 years, I would hope that we could get to a much lower level of digital architecture in the fighting units and reduce that digital divide that both General Wallace and I have spoken to, at least to some degree.

There is a lot of potential in the Unmanned Aerial Vehicle (UAV) world that, over 5 years' time, I would hope we would start to understand and see more use of. The integration of these combat sup-

port applications certainly could be done within 5 years in a way that would make the warfighters—air and ground—function much better together, both in planning and execution.

I think you will see continued improvements in joint tactics, techniques and procedures. The relationships and experiences that have come from this war will propel all the services to do more of that and improve on the already good things that they have done.

And hopefully, those systems that are coming in—joint tactical radio and so on—will arrive, if not sooner, earlier so that we can pick up on some of these problems, rather than waiting more than 5 years to solve it.

Mr. SAXTON. General Rogers.

General ROGERS. Sir, I believe that regardless, the globe will move ahead and we will be more and more connected. The information age will not go backwards. We will be more and more connected.

And we will have to acknowledge that our adversaries will be able to use that same environment and they will. So we must learn how to operate within that environment better than them, that will take all of these tactics, techniques, procedures, training and capabilities that have been discussed here.

And I think one of the challenges will be keeping in mind that, in order to execute, it is always going to be about the people with mud on their boots and jet fuel dripping on their back and those kinds of things and being able to provide the command and control to enable those people the best. I think we will make headway in certain areas, such places as standing Joint Forces Headquarters capability to be more ready to command and control of joint operations.

And I think that we will fill a huge gap at the operational level that is comparable to what General Wallace talks about, Battle Command On the Move, deployable joint force command and control capabilities. We have not had any existing standard, joint task force headquarters facility, that is deployable to this date.

So we have had to build a different one every time. And those kind of capabilities will be necessary to operate in an environment where there will be more information than ever flowing around the battlefield.

And to give you an example, in World War I, the point-to-point communication capability was about 30 words a minute. In World War II, it was about 60.

In Vietnam, it was a little over 100. It was about 192 K in Desert Storm. I think it was on the order of 800 megabytes in this operation. And by 2010, it is projected to be 1.5 trillion words per minute flowing around the theater.

That is the equivalent of the Library of Congress every minute. And buried in there somewhere is the information that a battalion commander or a squad leader or a component commander or a joint force commander needs.

So you can see, we have a lot of work to do to figure out how to manage that and operate within it. It will take some investment to get us there.

I think we are up to it. Our problem generally is that every time we look out ahead a couple of decades and imagine what might be,

we just advance the clock a few years and it moves forward a little quicker.

Mr. SAXTON. Thank you.

General MORAN. Sir, I think you will see great improvements in bandwidth management to make that bandwidth more effective. And really what that translates to is exactly what General Rogers just talked about, is the more efficient movement of information and getting it down to the soldier, the sailor, the airman and the Marine that needs it to make a decision as he or she is engaging the enemy.

And I think where the challenge is going to be is in the battle command systems and how we fine tune those systems so they can present to the soldier, sailor, airman, Marine a relevant common operational picture that he or she can make a decision on.

Mr. SAXTON. You each sound as if you are saying a couple of things. One is that these systems are going to continue to evolve and that the systems that are out there today will continue to evolve closer together.

Is that right? Is that a fair conclusion?

General MORAN. I think so, sir.

Mr. SAXTON. Can we expect that maybe we could get some kind of an overall architecture plan of how this can be expected to happen in the foreseeable future? You know, Mr. Larsen mentioned that we reached out, under the leadership of the chairman of the full committee and myself, a few months ago and reduced by 10 percent, across the board, $2 billion—I guess it was not 10 percent, $2 billion across the board—expenditures.

And we did it for two reasons. One was that we did not understand where all of this was leading. And we have a better picture now.

And the second was we needed to get people to talk to us. And when we decided that $2 billion should be cut, a lot of people came and talked to us. And we are starting to understand this a whole lot better now.

But one of the things that we still have not been able to do is to get a plan laid out, where we can see how at least your vision is that things are going to evolve together. That seems to us to be really important.

And I am wondering if we can expect, based on what you are saying, that all seems to be happening, but we have trouble seeing the overall architectural plan. Can you help us with that somehow?

General Wallace.

General WALLACE. Yes, sir. We can. [Laughter.]

Damn, that is something we all want. I mean, a single, joint architecture that makes life easier for all of us is something that we all aspire to. The road map to getting there, I leave to the technicians on my far right and my far left.

But from a perspective of a warfighter, regardless of service, I think that is something we all want to get to—a single, joint architecture which allows us all to communicate and share information and make decisions in a coherent manner for the——

Mr. SAXTON. I am asking these questions just for information, not to be contrary. Why is it so hard?

General LEAF. Mr. Chairman, I think it is difficult for a purely technical reason; and that is, capturing in what we now know as an architecture both present and future. It is very difficult because architectures, as you fully appreciate, are extraordinarily intricate.

To capture where we are and then capture, first on a service level, where we are going and then integrate that with the overall joint view. I know the Air Force has a warfighting integration directorate, Air Force XI, and a Chief Information Officer (CIO) who worked hand in glove to develop that. And we are speaking to the other services.

I would suggest that, knowing that the Army, Navy, Marine Corps and Air Force are working that, that through the leadership of Joint Forces Command and the Joint Chiefs of Staff (JCS) J–6, we should be able to bring you such a road map, if not a complete finished architecture.

But I will defer to General Rogers. That is more work for him.

Mr. SAXTON. He is going to thank you.

General ROGERS. And it is a lot of work, sir. To amplify a bit on what General Leaf said, this is an immensely complex challenge. It goes back to what I have said a couple of times here.

It just becomes obvious to me, several times a week. We just now got this far in the information age and realizing these types of capabilities. And we make new discoveries every day about what it means to us.

And it is not like we can just throw up an architecture out there. It is based on what real people have to do from the trenches all the way to the top, of reaching back to decision levels here in Washington and at senior levels coalition.

And when you try to look at how you are going to operate the capabilities you want to deliver operationally and then try to build your systems and technical architectures for that, it becomes a mind-exploding experience. And the ability for hundreds or thousands of people across the services and in the joint commands to pool together to work this problem has still not worked out all the details.

I think it is going to be a huge challenge to achieve the single architecture. But I do not for a minute believe it is unachievable.

As I mentioned before, every time we think about something in the out years, and think it is X amount of time away, just the very fact that we conceived of it and put a little brain time on it, we just advanced the clock. So I cannot tell you exactly when we will achieve that nirvana vision, but I have great hopes for it.

It is a challenging dilemma.

General MORAN. Sir, again, speaking from my current hat within the Army, I can lay out for you, in excruciating detail, first of all, what we understand is the DOD architecture, the global information grid with its three components of GIG bandwidth expansion, the Network Centric Enterprise Services (NCES) and the transformational communications architecture.

And I can show you, over time, how the future combat systems, the war fighter information network terrestrial and the other satellite initiatives that the Army is investing in, along with the other services, I can show you how all that stitches together with the Office of the Secretary of Defense (OSD) global information grid.

And I can also show you, through the joint battle management command and control road map, how the Army battle command systems must be stitched together with the Air Force, the Marines and the Navy and also satisfy the unique requirements for our special operating forces. So the architecture that you are looking for, I believe does exist. But I am afraid I am not in a position to speak for Mr. Stenbit and be the one that delivers it to this committee.

But I do feel that there is a vision that certainly we in the Army are operating in, and ensuring that our systems are interoperable certainly with the other services, but also are going to be able to leverage the investments that DOD is making with the Defense Information Systems Agency in both terrestrial and space-based systems.

Mr. SAXTON. Okay. Well, we do not have the advantage of seeing what you do every day. We have the advantage of having occasions like this when we get to talk about it a little bit.

And we are wanting to be supportive obviously because the capabilities that we have been able to collectively demonstrate have been very impressive. But we need to recognize where we have been and take note of where we have been and recognize what that means, going forward. And those of us who would, looking at this situation, still think an overall plan would get us there in a more effective, efficient, financially efficient way.

So to the extent that we can work with you to understand or at least gain a better understanding of this evolution which we think is taking place together, it will help us out a whole lot and help us make resources available to you to make even further progress.

Anything else? Mr. Wilson.

Well, we want to thank you for being here with us today. This has been extremely informative. The members asked great questions and you gave great answers. And we appreciate that.

And we look forward to seeing you again in the future. And keep up the great work.

[Whereupon, at 1:05 p.m., the subcommittee was adjourned.]

APPENDIX

OCTOBER 21, 2003

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

OCTOBER 21, 2003

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

---

Subcommittee Hearing

"C4I Interoperability: New Challenges in 21st Century Warfare"

October 21st, 2003

Good morning ladies and gentlemen. The Subcommittee on Terrorism, Unconventional Threats and Capabilities meets this morning to assess command, control, communications, computer, and intelligence systems (C4I) interoperability issues and lessons learned from Operation Iraqi Freedom (OIF). We are also interested to learn more about how these issues present new challenges in 21st century warfare.

Ensuring that systems work effectively together is a vital issue for the Department of Defense as it transforms itself into a lighter, faster, more lethal force. Information technology (IT) plays a critical role in the Department's transformation. The objective is to decrease the decision making time process—to effectively shorten the sensor-to-shooter time to deliver rounds on targets.

Network centric warfare (NCW) is an essential element of the Department's transformation. The foundation of NCW is to use technology—computers, data links, networks—to connect members of the armed services, ground vehicles, aircraft, and ships into a series of highly integrated local and wide-area networks capable of sharing critical tactical information on a rapid and continuous real-time basis.

NCW's components include: interoperability of various command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems. NCW eliminates stove-pipe systems, parochial interests, redundant and non-interoperable systems, and optimizes capital planning investments for present and future IT systems. The Subcommittee supports the Department's initiative to attain the goals of NCW by implementing network-centric activities and programs.

To provide our warfighters the most accurate real-time information, they must have the latest command, control, communications, computer, and intelligence systems to receive and move that data over secure communication links. The key is to have this information move seamlessly within a chain of command and between the service commanders.

During OIF, the United States had over 170,000 military personnel in theater. With such a large number of people involved in operations that spanned across several countries, it was imperative to have real-time C4I interoperability between the services at every level to coordinate missions, air-strikes, troop movement, and to prevent fratricide.

Interoperability is more than just the individual C4I and weapon systems that move information to leverage firepower. Interoperability also includes procedures and techniques. But most importantly, interoperability is about how people—warfighters—can obtain real-time access to intelligence and information to make informed decisions in battle. Information, access to it, and how fast it can be delivered now determines combat power.

There are several C4I interoperability issues that should be addressed during today's hearing. These include battle command on the move—the integration of C2, intelligence, logistics, force protection, and weapon systems, bandwidth constraints and satellite communications, and coalition interoperability. These fundamental issues need to be addressed as the U.S. military transforms to meet and defeat conventional and asymmetric threats in the 21st Century battlespace.

Today, we are pleased to have Lieutenant General William Wallace, Lieutenant General Daniel Leaf, Major General Keith Stalder, Brigadier General Dennis Moran, and Brigadier General Marc Rodgers testify before the subcommittee on the importance of C4I interoperability following combat operations in OIF.

Lieutenant General Wallace commanded the U.S. Army's 5th Corps—which was responsible for the capture and occupation of Baghdad. His headquarters synchronized the decisive execution of the 3rd Infantry Division, the 101st Airborne Division, the 3rd Armored Calvary Regiment, the 82nd Airborne Division, the 2nd Cavalry Division, the 4th Infantry Division, and the 1st Armored Division, along with the associated combat support and combat service support under the 3rd Corps Support Command. Gen. Wallace then assumed responsibility for all of Iraq upon his transition to the Commander, CJTF-7. Presently, Gen. Wallace is Commanding General for Combined Arms Center, U.S. Army Training and Doctrine Command, Fort Leavenworth, Kansas.

Lieutenant General Leaf served as Director, Air Component Coordination Element with the Coalition Land Forces Component Commander in Kuwait and Iraq. Lieutenant General Leaf was the Joint Forces Air Component Commander's representative to the land component commander. He worked with the Coalition Forces Air Component Commander to develop the air and space strategy and coordinated close-air-support missions with the Army. General Leaf acted as the coordinating authority between the land and air commanders. Presently General Leaf is Vice Commander for U.S. Air Force Space Command.

Major General Stalder served and continues to serve as the Deputy Commanding General of the 1st Marine Expeditionary Force (MEF), the command element for all Marine air, ground, and combat service support operations during OIF. During command operations he was responsible for the MEF's rear headquarters. From this vantage point, General Stalder was able to assess the effectiveness of the Corps C4I systems operating

within the MEF, and those networked to higher headquarters, sister services and coalition partners.

Brigadier General Moran served as U.S. Central Command (CENTCOM's) J-6 and was responsible for all programs that provide command, control, and communications (C3) support to the Commander of CENTCOM and his staff. In addition, he was responsible for the integration of all C3 support required by the ground, air and sea components of CENTCOM. General Moran also provided the planning and execution of the communications architecture for Operation Enduring Freedom (OEF) and OIF. Presently, General Moran is the Director of Information Operations, Networks, and Space for the U.S. Army.

Brigadier General Rogers is the Director, Joint Requirements and Integration Directorate, J-8 for U.S. Joint Forces Command (JFCOM). He is responsible for integrating the national military strategy with the Department of Defense's planning programming and budgeting system. His directorate conducts reviews of future capabilities requirements outlined by the combatant commanders. The directorate focuses on the degree of interoperability among all force components and then validates emerging technology for testing through experimentation and demonstration.

Welcome, Gentlemen.

Meehan Opening Statement C4I
Hearing 10-21-03

Thank you Mr. Chairman.

I am impressed by the success of our offensive military operations in Iraq, and I share your view that this success represents the culmination of extensive investment in advanced command and control systems. I returned recently from a trip to Iraq. Despite serious misgivings about the way we are attempting to stabilize and rebuild Iraq, I can personally attest to the professional dedication of the men and women in uniform. As for equipment and information systems, it is clear that the joint successes of Operation Iraqi Freedom are the direct result of investments made five to 10 years ago. That said, however, I also recognize many of the past and present shortcomings as well as the future challenges.

Information fusion is perhaps the greatest challenge – particularly in the intelligence collection and dissemination architecture.

Yet the delivery of actionable intelligence from the point of collection to the people who need to use it is a necessary and vital component of battlefield success.

There are many other challenges as well, and I hope this hearing serves the purpose of increasing our focus on the appropriate investments, whether they are financial or intellectual. I look forward to the testimony. Thank you.

RECORD VERSION

STATEMENT BY

LIEUTENANT GENERAL WILLIAM S. WALLACE

COMMANDING GENERAL, COMBINED ARMS CENTER,

U.S. ARMY TRAINING AND DOCTRINE COMMAND

BEFORE THE

SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES

ARMED SERVICES COMMITTEE

UNITED STATES HOUSE OF REPRESENTATIVES

ON C4I INTEROPERABILITY: NEW CHALLENGES IN 21ST CENTURY WARFARE

FIRST SESSION, 108TH CONGRESS

OCTOBER 21, 2003

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

Mr. Chairman, Members of the Committee. My name is Lieutenant General William S. Wallace, Commanding General for the Combined Arms Center, U.S. Army Training and Doctrine Command (TRADOC), Fort Leavenworth, Kansas. I appreciate the opportunity to testify on a very broad area of military capability labeled "Command and Control, Communications, Computers, Intelligence" or what we mercifully call C4I interoperability in acronym.

As the commander of the Combined Arms Center, one of my focus areas is Battle Command (BC). I am the TRADOC's proponent for BC. Also, it was my privilege to command U.S. Soldiers in our nation's recent invasion of Iraq and the removal of Saddam Hussein's repressive regime. Relying on that experience and my current role with BC, I will focus my testimony on "what worked" and "what did not work" in regards to the C4I interoperability in context of Operation Iraqi Freedom (OIF).

It's important that you understand that my perspective of OIF is quite different than those heard earlier this month from Admiral Giambastiani and Brigadier General Cone. Their study focus was on the joint/operational level of OIF. As V Corps Commander, my view was considerably more from the tactical level – the pointy end of the spear.

Inherent at this tactical level is the prosecution of maneuver warfare; characterized by mobile, widely dispersed, high operational tempo, and simultaneous execution on a very fluid and non-linear battlefield. More so than at the operational level of warfare, the tactical level requires C4I technologies that are untethered from fixed architectures. The tactical level requires mobile command posts and communication networks that can

support a corps in the attack. Quite frankly, it is at the tactical level that we face our greatest C4I challenges to achieve the capabilities envisioned for the future force.

It's also important that you know the painstaking efforts that V Corps and the Department of the Army (DA) undertook in preparation for OIF in regards to C4I. In August 2002, the Army had a myriad of different automation architectures supporting command and control (C2). They ran the gamut from digital screens to plywood boards covered with maps and acetate.

In recent years Force XXI units, such as 4th ID, received the lion's share of C4I initiatives and were fully digitized. Europe and specifically V Corps, was in the midst of our own C2 redesign to leverage digitization to enhance C2 capabilities. Likewise, the XVIII Airborne Corps had employed its own unique automation solutions to enhance C2. The rest of the Army, especially the Reserve, National Guard, and combat service support (CSS) force structures, had little or no digitized C2 capabilities.

The force configuration necessary for decisive operations in Iraq allocated underneath V Corps was comprised of units representing diverse and sometimes incompatible C4I architectures. In order to fight within a cohesive framework of C4I interoperability, the Army quickly prioritized efforts to patch, modify, and standardize the existing architectures of the deploying units.

Led by U.S. Army TRADOC, an army of smart guys with resources descended upon us adapting the V Corps framework for managing our C2 redesign and C4I integration. We had to get the assembled force on the same sheet of "C4I music" in terms of hardware,

software, and tactics, techniques, and procedures. We focused on developing solutions for Battle Command on the Move (BCOTM), Common Operational Picture (COP), Blue Force Tracking (BFT), joint fires integration, integrated air picture, combat service support; clear voice command net, and collaborative tools.

After seven months of intense C4I integration efforts of fielding, testing, training, evaluating, and fixing, V Corps crossed the line of departure on March 20th commencing the ground war. While not perfect, we had come a long way in terms of C4I. The effort I just described was nothing short of Herculean, a tribute to military men and women, and exceptional support from our civilian and contractor work force.

In spite of its success, this experience was very painful and we must prepare better before crossing the next line of departure. In fact, building upon the lessons learned from OIF, the Army is committed to leveling the C4I playing field across the current force. And because we are a nation at war, the priority of effort is going to those units preparing for the next rotations into Afghanistan and Iraq.

Now, what worked? OIF was characterized by rapid task re-organization across all echelons to enable exploitation of enemy vulnerabilities, and execution of branch, sequel, and follow-on operations. We made aggressive road marches and maneuvers at distances and tempos unheard of in previous campaigns, separating lower echelon combat units beyond Line of Sight (LOS) connectivity to their higher HQs. From my assault command post, we accomplished joint, operational, and tactical collaboration and coordination at the battle's forward edge.

OIF provided a substantial glimpse into the advantage of waging network enhanced warfare, even as it revealed the limitations of our developing C4I capabilities. The situational awareness of commanders at every level during OIF exceeded that of any modern war. Satellite-based Blue and Log Force Tracking with email exchange capabilities enabled synchronization of command and staff tasks at theater, operational, and tactical levels.

Single channel tactical satellite (TACSAT) at the Corps and divisional levels enabled broadcast C2 without regard to terrain or distance. Some would say the ground war was won on TACSAT. Using satellite-based Blue Force Tracking, leaders on the ground were able to successfully control the furious fight, receive changes to missions, achieve situational awareness, and navigate unfamiliar terrain using digitized map sheets that displayed Blue Force locations in near-real time.

I saw more of the fight than I expected to be able to see from my Command and Control Vehicle (C2V). Enabled with satellite based communications my assault command post was mobile, responsive, connected, and allowed me to be where I could best influence the fight anywhere on the battlefield. In the digital environment of my headquarters, the Common Operational Picture provided exceptional situational awareness because of our joint interoperability with higher headquarters.

Having the ability to track the theater air picture and theater ballistic missile launches added to our awareness and provided systems redundancy. Being able to track the adjacent 1st Marine Expeditionary Force (IMEF) on the same screen with the same "iconology" and graphic control measures was essential.

What worked? Outstanding system products like the Command and Control Personal Computer (C2PC), Blue Force Tracking (BFT), Automated Deep Operations Coordination System (ADOCCS), Air Missile Defense Work Station (AMDWS), and the Advanced Field Artillery Tactical Data System (AFATDS) enabled us to achieve an unprecedented level of combined and joint arms synergy. Time Sensitive Targets were deconflicted in a matter of minutes using a Theater-wide Joint Fires Coordination Information System.

For example, through the eyes of the Unmanned Aerial Vehicle (UAV), transmitted by Global Broadcasting System, we could observe an enemy artillery battery firing on our troops, then coordinate over Tactical Voice and single channel TACSAT for its subsequent destruction by Air Force, Marine, or Naval aircraft in close support of the ground campaign.

What didn't work? As I marveled at how leveraging this information technology gave me unparalleled control of my battle formations, I also observed subordinate leaders on the tactical field struggling with the limitations of their static, terrestrial based networks. Despite the introduction of Battle Command On the Move (BCOTM) capabilities that I enjoyed in my assault command post (CP), the vast majority of tactical leaders and CPs enjoyed few *on the move* capabilities. Most were tethered to a CP and largely dependant upon line of sight communications.

Case in point. At the corps level the G2 could see individual fighting positions defending a critical bridge because we had a UAV leading the lead formations. But we could not get the data down to the unit who was taking the objective because all the CP's

were moving. It was a deliberate attack at the corps level, but a movement to contact at the battalion level.

Not having satellite capability, most tactical CPs received connectivity services from Mobile Subscriber Equipment (MSE). What capability MSE provides is done so at the Warfighter's expense, as he must trade considerable strategic lift, force protection, key terrain, tactical flexibility, time of installation, and C4I capability in return for what is largely intra-Corps voice and data service for stationary command posts that take hours to install. The Army's MSE tactical network does not effectively support high tempo, 21st Century maneuver warfare. It must be replaced as quickly as possible.

The Army must exploit the BCOTM principles proven in OIF. We must invest in the redesign of CP structures to enable commander centric operations on the move, while taking advantage of the power of the network. Mobile, satellite networked CPs would have a smaller footprint. Their satellite-enhanced connectivity could feasibly allow for some traditional CP functions to be performed from a distant sanctuary or possibly from Home Station Operation Centers. The CP's smaller footprint could improve its deployability while saving the combatant commander significant amounts of strategic lift. Those enhanced CPs would have improved survivability by offering a smaller physical presence on the battlefield.

No matter how perfect a future network and CP we build, it won't do us much good until we fix the overarching problem of bandwidth management. Limited bandwidth was a major issue during OIF. While fixed command and control installations reliably use high-bandwidth communications, the communications architecture for mobile or semi-mobile

CPs at the tactical level is too fragile and not robust enough to support our needs. It effected collaboration, information sharing and in some cases, the Commander's ability to command. In an environment where competition for limited bandwidth is fierce, we must seek efficiencies through a more sophisticated management solution. The time to fix bandwidth problems is now, before we deploy to the next fight.

Once the Army overcomes satellite bandwidth constraints, we can aggressively address the "Digital Divide" that exists between the operational and the tactical levels of war. We can extend the power of the network down to the tactical level. Despite our efforts to realize network enhanced warfare since Desert Storm, the trigger puller on the ground still can't tap into the network and realize its benefits. In OIF, this was most pronounced in dissemination of intelligence information. Despite all the incredible products at the disposal of my assault CP, we could not get relevant photos, imagery, or joint data down to the soldier level in near-real time. The opportunity to exploit intelligence to our advantage, to the advantage of the fire team in contact was lost.

Empowerment of the Soldier on the ground is also crucial to realizing Army concepts of future warfare in complex terrain. To fight in urban areas for example, our junior leaders require a high degree of specificity about the terrain and the enemy. Today, we can't effectively push information down to help the squad leader fight. Terrestrial based communications limit our warfighting ability under conditions imposed by complex terrain. Yet full motion video (FMV) taken from a UAV pushed down to the battalion or company level would give the Soldier on the ground the ability to see the enemy from multiple viewpoints in relation to the individual enemy fighting positions. With near-real

time, satellite network connectivity, our junior leaders fighting in complex terrain can leverage the power of the network and enjoy increased situational awareness.

In summary, Operation Iraqi Freedom proved the effectiveness and potential of networked enhanced warfare. We know it works. Applying lessons learned, we can rapidly improve our C4I capabilities by discarding technology and concepts that did not work and pursuing those that did. The Battle Command on the Move concept works, but we need to build the Command Posts to support it. Satellite based communication works; but we need more bandwidth to push the synergy of network enhanced operations down to the tactical level. Once we overcome the "Digital Divide," when we can connect the synergy of network enhanced operations to the soldier in the dirt, we can be confident that we have done our very best to ensure his success on the modern battlefield.

But please understand and always remember that regardless of the improvements we gain and the networks we build, warfare in the 21st Century will remain lethal, up close, and personal. The American Soldier, supported by family and nation, will be our most treasured and lethal weapon. His bravery, heroism, sacrifice and compassion will continue to be our inspiration.

UNCLASSIFIED
FOR OFFICIAL USE ONLY
UNTIL RELEASED BY THE
HOUSE ARMED SERVICES COMMITTEE
TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE

STATEMENT OF

LIEUTENANT GENERAL DANIEL P. LEAF

VICE COMMANDER

AIR FORCE SPACE COMMAND

BEFORE THE UNITED STATES HOUSE ARMED SERVICES COMMITTEE

TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE

21 OCTOBER 2003

UNCLASSIFIED
FOR OFFICIAL USE ONLY
UNTIL RELEASED BY THE
HOUSE ARMED SERVICES COMMITTEE
TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE

Mr. Chairman and members of the Committee:

On behalf of the outstanding men and women of the United States Air Force, thank you for this opportunity to appear before you today. It is a privilege to testify on Command, Control, Communications, Computer and Intelligence (C4I) Interoperability: New Challenges in 21st Century Warfare. I had the honor to help defend this great nation during Operation Iraqi Freedom (OIF) as Director, Air Component Coordination Element with the Coalition Forces Land Component Commander in Kuwait and Iraq. I want to thank all of you for your continuing support to the armed forces.

The Armed Services have made remarkable advances in interoperability. Since Operation Desert Storm, we have solved several major problems–timely sharing of tasking orders, common situational awareness tools and improved communications. We embrace a common operating environment that enables communication among component commanders and coalition forces through classified computer networks and video teleconferences. These advances are mandated to us through the joint community and codified in Chairman of the Joint Chiefs of Staff Instructions (CJCSI). Our requirements are driven by key performance parameters to ensure interoperability.

Beyond technical interoperability is what I label "conceptual interoperability." The secret to success in OIF was the working relationship between the Coalition Forces Air Component Commander, General Michael Moseley, Coalition Forces Land Component Commander, Lieutenant General David McKiernan, Coalition Forces Maritime Component Commander, Vice Admiral Timothy Keating, and the Commander of Special Operations, Brigadier General Gary Harrell. This team of commanders demonstrated the understanding and appreciation for the missions and assigned tasks of each service in coalition warfare. They understood conceptual interoperability is more than the capabilities of individual weapons systems and the associated tactics, techniques and procedures.

Conceptual interoperability is when we foster teamwork. As a warrior, trust is crucial. We have learned the hard lesson that we must cooperate to overcome the competing priorities in warfare with overlapping and integrating capabilities. The commanders in OIF balanced their individual perspectives to achieve the objectives established by the President. For example, General Moseley knew that destroying enemy air defenses was paramount to the 3rd Infantry Division's march to Baghdad. He directed the systematic destruction of Iraqi surface-to-air missile systems through the "kill chain" process. Coalition forces would find, fix, track, target, engage and assess through persistent air and space superiority. This enabled the land component freedom to operate their forces and achieve tactical advantage over opposing ground forces.

Finally, I must acknowledge that C4I Interoperability is a product of smart, young troops in the field. Their innovative use of technology in a disciplined manner is vital to our success. Our ability to use software to chat and collaborate with each other improves our lethality. As an example, FalconView software is a simple map program that runs on a standard personal computer. It not only allows aircrews to mission plan at the tactical level but also allows us to share flight routes, threats and imagery with the other components improving situational awareness.

We recognize we must continue to move forward through service partnerships. We are committed to partnerships at the most senior service levels to cultivate good behavior patterns amongst all ranks. We are also committed to developing new technologies. Blue Force Tracking is a possible joint tool to help with combat identification of friends or foes. As we move forward in the 21st Century, our interoperability is necessary to meet the challenges of tomorrow. We appreciate your continued support.

Again, I am honored to appear before you and look forward to your questions.

NOT FOR PUBLICATION
UNTIL RELEASED BY
THE HOUSE ARMED
SERVICES COMMITTEE

STATEMENT OF

MAJOR GENERAL STALDER

UNITED STATES MARINE CORPS

DEPUTY COMMANDING GENERAL FOR I MEF

BEFORE THE HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL

THREATS AND CAPABILITIES

ON

OCTOBER 21, 2003

CONCERNING

I MEF C4I DURING OPERATION IRAQI FREEDOM

NOT FOR PUBLICATION
UNTIL RELEASED BY
THE HOUSE ARMED
SERVICES COMMITTEE

Major General
Keith Stalder
Commanding General, I Marine Expeditionary Brigade

Major General Keith Stalder currently serves as the Commanding General, I Marine Expeditionary Brigade and Deputy Commanding General I Marine Expeditionary Force, Camp Pendleton, California.

He has served in Marine Fighter Attack Squadrons 333, 235, and 115 as well as Strike Fighter Squadron 125 and Marine Aviation Weapons and Tactics Squadron One.

He is a 1985 graduate of Marine Corps Command and Staff College, commanded Marine Fighter Attack Squadron 531 and graduated from the NATO Defense College in Rome, Italy in 1993. Major General Stalder served at Headquarters, European Command, Stuttgart, Germany as the Operations Division Chief for the military-to-military contact program for Central and Eastern Europe and the former Soviet Union from 1993 to 1995. After leaving Europe, he commanded Marine Aviation Weapons and Tactics Squadron One. He next served as the Assistant Wing Commander, 3d Marine Aircraft Wing and following that as the Deputy Director for Plans and Policy, United States Central Command, during Operation Enduring Freedom.

(Revised Jun 7, 2003)

Mr. Chairman and members of the House Armed Services Committee, thank you for this opportunity to appear before the committee to discuss the First Marine Expeditionary Force's experiences and observations from Operation Iraqi Freedom (OIF).

I. INTRODUCTION

As discussed in previous Marine Corps testimony to the House Armed Services Committee, the I Marine Expeditionary Force (I MEF) is structured according to Marine Corps doctrine as a Marine Air/Ground Task Force (MAGTF). The MAGTF consists of four integrated elements; a command element, a ground combat element, an aviation combat element, and a combat service support element. I MEF is composed of the MEF command element, the First Marine Division, the Third Marine Air Wing, and the First Force Service Support Group. This combined-arms team trains as a MAGTF, deploys as a MAGTF, and is employed across the spectrum of conflict as a MAGTF. The MAGTF is an inherently flexible, scalable force that can be sized to meet any contingency. The MAGTF that participated in OIF consisted of the MEF's four organic subordinate commands, listed above, and expanded to include the 1st (UK) Armored Division, Task Force Tarawa (formed around 2nd Marine Expeditionary Brigade, from Camp Lejeune, NC), the 15th and 24th Marine Expeditionary Units, the 11th Marine Expeditionary Unit Command Element, the 1st MEF Engineer Group, and several attached units from the United States Army. In its totality at the height of OIF, I MEF consisted of over 86,000 Marines, sailors, and soldiers. During OIF, I MEF was directly subordinate to the Combined Forces Land Component Command (CFLCC – 3d US Army). Despite the size and complexity of this force, I MEF's success during OIF once again reinforced the flexible, scalable nature of the MAGTF concept.

II. MAGTF COMMAND AND CONTROL

C4I is first and foremost about people and enhancing their ability to accomplish the mission in a complex, rapidly changing, and dangerous environment. The Marine Corps' view of Command and Control (C2) is based on the common understanding that all Marines have of the nature of war and our warfighting philosophy. It takes into account both the timeless features of war, as we understand them, and the TTP's, processes, and hardware available to prosecute the battle. Our doctrine provides for fast, flexible, and decisive action in a complex environment characterized by friction, uncertainty, fluidity, and rapid change. Since we recognize that equipment is but a means to an end and not an end in itself, our doctrine is independent of any particular technology. In fact, the cornerstone of MAGTF C2 is not equipment at all, but rather the individual Marine. No amount of technology can reduce the human dimension of war.

Central to this doctrine are the concepts of the single battle, mission-type orders, and integrated planning. The single battle concept provides a focal point for MAGTF planning and execution; it emphasizes that all elements of the MAGTF engaged in either the deep, close, or rear fight execute according to the MAGTF Commander's desired endstate. Mission command and control relies on the use of mission-type orders, by which commanders assign missions and explain the underlying intent (Commander's Intent), but leave subordinates as free as possible to choose the manner of accomplishment. Mission C2 leverages centralized, integrated planning and decentralized execution at the maneuver unit level. Integrated planning includes subordinate command planners in the MAGTF planning team to ensure a common understanding of the mission requirements and thorough coordination. It leverages limited planning time to allow disparate elements of the MAGTF to plan concurrently. These central concepts empower

subordinate commanders to exercise maximum initiative, capitalize on situational opportunity, and maintain the tempo of MAGTF operations.

III. C2 SYSTEM HIGHLIGHTS

Effective MAGTF C2 systems are characterized by their flexibility, ability to support expeditionary operations, robustness and redundancy, interoperability, and the ability to provide reach-back to organic, theater, and national agencies. Development of an effective system will result in shared situational awareness of the mission, the enemy situation, friendly actions and locations and the environment. This merging of shared information is often referred to as a Common Operational Picture (COP). It allows greater initiative, speed, and freedom of action.

Command and Control systems effectively employed during OIF were able to convey Commander's Intent, disseminate orders, reports, overlays, and intelligence, and support constant communications among and between the MEF Commander, his subordinate commanders, and higher and adjacent units. Detailed planning between elements of the MEF staff and the subordinate commands enabled stable and redundant communications throughout the conduct of OIF, despite unprecedented network complexity and operational distances. Specifically, the MEF C2 architecture easily incorporated Task Force Tarawa, and the 15th and 24th MEU's into a cohesive whole. Combining the well-planned and scalable architecture with proven tactics, techniques, and procedures, I MEF C2 supported the successful accomplishment of the Marine Corps' mission during OIF.

In order to support these C2 systems, the MEF and its major subordinate commands incorporated several recently fielded communication technologies. Among these were the Secure Mobile Anti-Jam Reliable Tactical-Terminal (SMART-T), the Tactical Data Network

(TDN) gateway, the Digital Technical Control (DTC) facility, and the Deployable KU Earth Terminal (DKET). Overall, these new technologies were a great success story and contributed significantly to the MEF and Major Subordinate Command (MSC) Commander's ability to command and control forces in combat.

The SMART-T, a HMMWV-mounted mobile satellite terminal, designed and fielded to provide a satellite communication path to the regimental level, exceeded all expectations. With this expeditious satellite terminal, regimental commanders were able to stop, set up, and establish secure tactical phone connectivity with the Division Commander, often within 10 to 15 minutes.

The employment of the TDN/DTC combination and its inherent multiplexing capability enabled the MEF to establish the most complex and extensive communication architecture the Marine Corps has ever employed in combat. From the start of combat operations on 20 March 2003 to the cessation of major combat operations on 1 May 2003, this system completed 2.5 million tactical telephone calls, over 240 video and audio teleconferences, over 700 video TS/SCI video teleconferences over the Joint Military Intelligence Communications System, and innumerable secure and unsecure e-mail transmissions. Leveraging these new communications technologies, the MEF Commander was able to conduct twice-daily teleconferences with his subordinate Commanders, and the MEF Staff was able to conduct numerous daily video teleconferences with CFLCC (our higher headquarters), and with the MEF Home Base Staff at Camp Pendleton.

The TDN/DTC combination also facilitated the Secure Internet Protocol Router Network (SIPRNET), which supported the MEF's primary Command and Control Applications, including the Global Command and Control System (GCCS), the Intelligence-Operations Systems (IOS), and Command and Control PC software (C2PC). One great leap in capability the MEF gained

since the days of Desert Storm was the addition of Blue Force Position-Location Information (PLI). Unit PLI, when aggregated across the force, showed the location of selected units in real time, permitting commanders at all levels the ability to watch the battle unfold. GCCS, IOS, and C2PC received and processed data from Blue Force Tracking (BFT) devices such as the Marine Corps' Mounted Digital Automated Communications Terminal (MDACT) and a system called MTS-2011 both of which produced unit blue force PLI. This data, when added to the enemy position-location information delivered by the intelligence community, was the basis for the COP for the MEF.

Additional intelligence dissemination was accomplished through the use of the Trojan Spirit II (TS), which was fielded down to the regimental level. TS enabled the regiments to carry with them a rapidly deployable Secure, Compartmented Intelligence communications system with which they could pull theater and national data and analysis products that would have otherwise been unavailable.

Complimentary to the Trojan Spirit was the Global Broadcast System (GBS). This system relieved the burden on our transmission and data networks by providing additional bandwidth, thereby enabling the MEF to receive various intelligence products such as real time video and imagery products.

Other warfighting information was disseminated between the MEF, higher headquarters, and other commands via web-based technologies. This information, including operational orders and overlays, daily intelligence data, and reports, provided the common information framework for the MEF. This critical technology lowered internal friction by reducing required reports and allowing warfighters to focus on leading Marines instead of answering requests for information from higher headquarters.

I also want to highlight one of our big successes, which was the creation of a deployable MEF Combat Operations Center. This center provided operational flexibility to the MEF commander and fulfilled our C2 requirement for a mobile, expeditionary, survivable, and effective command post. We are working with our Systems Command who helped us construct this command post to incorporate lessons learned into our program of record, the Unit Operation Center (UOC).

Marine Command and Control must be expeditionary in order to succeed. Traditionally coming from the sea, the Marine Corps has never conducted sustained combat operations so far inland. Our Command and Control facilities and equipment required tactical and operational mobility greater than that previously envisioned or expected and performed remarkably well under the extremely harsh environmental conditions of Kuwait and Iraq. Particularly noteworthy were the sustained performance of our satellite and terrestrial transmission systems. Interoperability of our C2 systems was critical due to the joint nature of this operation and the introduction of UK forces. One application that greatly aided interoperability across the joint force was the use of C2PC software. This software, which displays and manages the COP, creates and disseminates operational overlays and other graphics, and provides a common baseline for warfighters, was deployed at every echelon of command from CENTCOM down to the individual Battalion to include UK forces.

The robustness of our network allowed us to establish reach-back. Reach-back is the ability to use the communication network to draw critical information from sources far from the forward edge of the battlespace. Reach-back, to both airfields and command posts in Kuwait and national assets in CONUS, was a requirement for the MEF command element. It was planned for and incorporated into the overall MEF C2 architecture. This robust communications

architecture engineering, and availability of SATCOM (i.e. commercial and military) greatly increased our reach-back capability. This gave us the edge by enabling support from our home base at Camp Pendleton, CA and national agencies in CONUS. Future operations will require a greater need for satellite communications and expanded use of both military and commercial satellite systems. Our recent fielding of the Lightweight Multi-band Satellite Terminal (LMST) provides us with the capability to leverage both commercial and military satellite systems with a single terminal.

IV. C2 SYSTEMS IN EXECUTION

I MEF validated its C2 philosophy and systems architecture prior to combat operations through the conduct of three Command Post Exercises (CPXs). Exercises Lucky Warrior 1 and 2, and Internal Look thoroughly tested our C2 architecture and systems in simulated combat conditions in the CENTCOM AOR. More importantly, they helped I MEF develop the close working relationship required for combat with our higher, adjacent, and attached units.

Although we planned, established and refined the most complex and advanced C4I system the Marine Corps has ever used, it remains clear that our best "C2 System" was our Marines. Upon reaching our staging areas, I MEF sent liaison cells (including operations, fire support, and intelligence Marines) with communications and C2 equipment to our attached UK forces, our adjacent Army units, and our Higher Headquarters. These trusted liaison officers fulfilled the critical role of communicating the MEF Commander's intent at all echelons. In particular, the liaisons to the attached First UK Division brought robust C2 systems and communications support that provided the primary method to communicate situational awareness data, such as the Common Operational Picture (COP), cleared intelligence products, and all the

other benefits that a complete connection to the SIPRNET brings. These liaisons also provided real-time friendly force Position-Location Information (PLI) to the UK Forces. This data, overlaid on the UK's own paper-map based processes, provided the common Situational Awareness required across the force. Finally, these liaisons provided a crucial targeting intelligence function both to and from the UK. It is clear that no C2 system can take the place of a Marine who won't take no for an answer.

During major combat operations, the MEF Command Post maintained operational tempo by displacing three times, moving a total distance of 700 kilometers, while never losing positive Command and Control of assigned forces. In fact, our C2 systems were so robust that we easily passed command and control functions from Jalibah, Iraq to Commando Camp, Kuwait during the worst Iraqi sandstorm in 20 years. As further evidence of our flexible C2, the First Marine Division Command Post moved nineteen times during combat operations. Meanwhile the Third Marine Air Wing established twenty-two Forward Arming and Refueling Points and supported six airfields in both Iraq and Kuwait simultaneously. The Force Service Support Group conducted six Command Post Displacements. Finally, Task Force Tarawa and both 15th and 24th MEUs were well integrated into the force and conducted similarly effective operations throughout their battlespace.

Logistics convoys traveled over unprecedented distances in this theater, stretching our C4I architecture to its physical limits. As an example, reaction forces were in some circumstances limited by the range of line-of-sight communications. Logistics operations were supported by a combination of Iridium satellite phones, Blue Force Tracker Systems, and an extensive terrestrial communications infrastructure built as the MEF moved toward Baghdad.

V. OBSERVATIONS

The Marine Corps installed, operated and maintained the largest and most complex C4 architecture in the history of the Marine Corps, which required 80% of the Marine Corps' communication assets and augmentation of commercial satellite resources. These assets supported both Marine Corps and British coalition forces. The scheme of maneuver, distances covered and speed of advance imposed significant demands on all echelons of the MAGTF and required a reliable and flexible command and control architecture.

The overall consensus from commanders at every level was that communications worked very well. Most noteworthy was the sustained performance and reliability of many of the newly fielded communication systems despite an extremely challenging environment. Critical data services were provided using the newly fielded Tactical Data Network (TDN) and both voice and data circuits were routed using the Digital Tech Control (DTC) facility. With the increased demand on beyond line of sight communications systems such as Iridium Satellite phones and the TRC-170 radio systems, the newly fielded SMART-T provided critical bandwidth within the MAGTF. The SMART-T in particular was essential in providing voice and data services between the Division Headquarters and subordinate units. Most of these systems remained on line for the entire duration of the operation from the initial deployment of forces through combat operations and retrograde.

The systems providing the COP were critical in unifying situational awareness information across the MEF. However, these systems began to reach their limit. Specifically, as the number of tracks increased to beyond several thousand, our systems began to get saturated. The Global Command and Control System (GCCS) must be upgraded to accommodate the increased number of tracks.

Combat Identification (CID) remains problematic, but it continues to be our top concern. The MEF continues to have an enduring requirement for an active Combat Identification (CID) system that enables our Marines to identify friendly forces from foes or non-combatants at the point of decision. CID components are distinguished from those systems that provide Battlefield Situational Awareness in that CID must be applied to each Marine and vehicle and work from the shooter to the potential target. CID must have both an air-to-ground and ground-to-ground component. We must continue to press for an end-to-end joint solution.

Another system employed was the MTS-2011, Blue Force Tracking device, which allowed adjacent Marine, Army and UK units to see the current position of adjacent units. While the MTS system was a success because of its satellite-based communications pathway, it uses commercial satellite and encryption capabilities that are pending National Security Agency (NSA) certification. As a result, it could not be seamlessly integrated into our COP. Therefore, MTS-equipped units could only see other MTS unclassified feeds, eliminating their ability to see classified track data.

The M-DACT, our program of record for blue force situational awareness/blue force tracking, provided a secret high capability and visibility of the entire COP. However it was dependent on the Enhanced Position-Location Reporting System (EPLRS), which is a line of sight data radio. Due to the size and scope of the MEF operational area and the rapid advance of our maneuver units we exceeded the line of sight capabilities of the EPLRS network. Because of the vital role EPLRS plays in our tactical data network, we are developing a beyond line of sight EPLRS bridge called the Ship-To-Objective-Maneuver (STOM) Bridge. This bridge will extend the reach of this vital tactical data network. In addition to this effort the Joint Requirements Oversight Council has directed the Army to lead a joint effort to identify the most effective and

efficient means to achieve Joint Blue Force Situational Awareness (JBFSA). The Marine Corps is actively involved with this effort and heads the programmatic development efforts to support this initiative.

As operational planning commenced it became evident that the network being developed would require the latest in computing technologies. We had new systems (e.g. TDN) being fielded with commercial components that required upgrading to satisfy our expanded requirement from the original specifications. Too often, the length of time to field a new piece of hardware is excessive. We must continue to refine our acquisition process to increase its flexibility to accommodate new technology enhancements and changing requirements.

Like all US Forces undergoing transformation, the MEF is getting more digital with every passing day. This transformation requires us to also transform how we train our Marines to keep pace with these advancing technologies. Training our Marines must continue to be the priority as we move forward into this dynamic net-centric environment. Our Training and Education Command recently established a C4 Center of Excellence to provide a training continuum for our Marines to keep pace with the advancing technologies.

Digital communications on the move is another area that captured our attention. Specifically, mobile units require Situational Awareness and threat intelligence data. Equally stressing is the digital divide, the line between those larger units that have large bandwidth satellite connectivity and those disadvantaged smaller units that have only line of sight communications. The Future fielding of SATCOM systems like the Mobile User Objective System (MUOS), Transformational Communications, and Joint Tactical Radio System (JTRS) will help reduce the Digital divide between those forces at the MEF and Major Subordinate

Commands, while providing much better data to those maneuver elements that need it most at the fighting edge.

Significant progress has been made and continues in the joint requirements arena to develop joint concepts of operations and architectures – that's the good news. However, a number of difficult legacy interoperability challenges still remain to be overcome. Here are a few examples we faced, but successfully conquered through some hard work and compromise. The Theater Battle Management Core System (TBMCS) allowed the MEF and 3rd Marine Air Wing to process the Air Tasking Order (ATO) in real time. Having visibility on individual missions permitted a greater control of the effects of airpower, delivering better results more quickly. While this system provided a dramatic improvement from Desert Storm in the ability to disseminate, view and manipulate the ATO, TBMCS was not completely integrated with other fire support systems. Specifically, ATO information was inconsistent between air and ground systems. Additionally, TBMCS was difficult to set up and use. Also, the Army's All-Source Analysis System (ASAS) did not share intelligence information with the Joint-standard USMC's IOSv2. As a result, the USMC had to field an ASAS terminal into our intelligence section in order to effectively share and exchange information. Further, the CFACC used a third system, the Intelligence Targeting System that was not fully compatible with either the Army or Marine Systems. Similarly, AFATDS, a system designed for fire support at the Division level and below, was pressed into service as the primary fire support system at the CFLCC level. At Corps and above level, AFATDS functionality is limited by system design. Instead the MEF used ADOCS to get the functionality the MEF required.

Operating with our coalition partners offered unique challenges as well. Although the current coalition information sharing system of choice (i.e. CENTRIXS) allowed us to exchange

information, technical and procedural obstacles impaired our operational effectiveness. We must continue to pursue multi-level secure solutions that allow us to seamlessly operate with our coalition partners in the future without requiring multiple networks. The alternative is to provide them access to our classified networks.

VI. SUMMARY

The application of C4I contributed to the success of I MEF during OIF. More than any other contributing factor, this success was due to the efforts of individual Marines and the proven tactics, techniques and procedures developed over time. Once again, our best C2 system was our Marines. The combination of our systems and people allowed for better Command and Control, shared Situational Awareness, a faster operational tempo, effective destruction of known enemy elements, and rapid victory. As we continue to find ways to improve systems interoperability and reduce acquisition times, we will further enhance our effectiveness in joint and combined operations.

STATEMENT BY

BG (PROMOTABLE) DENNIS C. MORAN
DIRECTOR, INFORMATION OPERATIONS, NETWORKS, AND SPACE, CHIEF INFORMATION OFFICER/G-6
UNITED STATES ARMY

BEFORE THE

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

ON C4I INTEROPERABILITY: NEW CHALLENGES IN 21st CENTURY WARFARE

OCTOBER 21, 2003

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

STATEMENT BY
BG (PROMOTABLE) DENNIS C. MORAN

ON C4I INTEROPERABILITY: NEW CHALLENGES IN 21st CENTURY WARFARE

Introduction

Mr. Chairman and members of the subcommittee, thank you for the opportunity to provide testimony describing Operation Enduring Freedom (OEF) and Operation Iraqi Freedom (OIF) C4I Lessons Learned based on my experiences as the CENTCOM J-6 from June 2000 thru June 2003.

Background

Prior to 9/11, the US Central Command (USCENTCOM) Area of Operation (AOR) was an "economy of forces" theater. The mission set revolved around enforcement of UN sanctions issued after Operation Desert Storm. Force levels in the theater hovered around 25,000 sailors, soldiers and airmen. The communications architecture to support the missions was austere, consisting of tactical satellite communications and a small amount of commercial satellite support. Much of this communications equipment had remained in place after the end of Operation Desert Storm due to the lack of a suitable commercial infrastructure in the theater. The headquarters in Bahrain, Kuwait, and Saudi

Arabia were relatively small and required minimal communications services to execute their mission.

The modest funding levels only permitted limited improvements to this communications infrastructure. However, the communications infrastructure was sufficient to accomplish the mission and provide the Commander of USCENTCOM the minimum essential command and control capability required.

C4I Architecture—Operation Enduring Freedom (OEF)

Execution of combat operations in support of OEF came quickly after 9/11/2001. The operations plan that was hastily developed for OEF moved additional combat forces into the theater to locations the command had never envisioned occupying. Operational imperatives also dictated a different force mix in much greater numbers than anticipated. This force mix and C4 requirements in austere locations mandated an immediate expansion of the communications architecture in an ad hoc manner to meet these emerging requirements. Using the existing command post structure as a baseline, USCENTCOM grew a communications network to meet the minimal essential command and control requirements of Operation Enduring Freedom. As combat operations moved into their steady state in early 2002, a critical investment for a stable, long-term communications infrastructure in Afghanistan was made to support the stability operations and to sustain the remaining combat operations.

USCENTCOM, in coordination with the US Army and US Air Force, invested in a modest amount of commercial Ku- band satellite bandwidth to augment the military satellite bandwidth available in the theater. This investment allowed USCENTCOM to increase communications connectivity between key command posts that now extended into Afghanistan and Uzbekistan. The investment also gave the USCENTCOM Commander a significant increase in command and control capability.

Now, almost two years after the end of major combat operations in Afghanistan, there is a robust and resilient communications network in place to support current operations in that part of the theater.

Preparation for Operation Iraqi Freedom (OIF)

As the plan for OIF came together, it was apparent that the ground, air, naval and special operation forces would require a significant amount of satellite communication capacity using all bands across the spectrum to satisfy their mission requirements. USCENTCOM, in coordination with the Defense Information Systems Agency (DISA), the Joint Staff, and the services, took the necessary actions to move all available military satellite systems into a position that allowed USCENTCOM forces to utilize them. In addition, the services made investments in commercial Ku-band satellites to satisfy the requirements at the stationary command posts. This allowed military satellite bandwidth to be used at the mobile and more tactical command posts.

DISA invested in several long-term fiber optic cable leased lines between numerous Middle Eastern countries and Europe to reduce the dependence on satellite communications. This investment strategy reduced the cost for expensive satellite bandwidth, and improved the performance of several critical command and control software applications.

As the Army conducted an analysis of its planned scheme of maneuver, it was determined that the existing tactical communications systems would not be able to keep up with the expected speed of advance and dispersion of the combat forces. Thus, the Army developed a commercial satellite solution that could be installed on critical command and control vehicles that would give the tactical commanders the connectivity and bandwidth required while dispersed, beyond line of sight, and on the move.

Key OIF Lessons Learned from the J-6 CENTCOM Perspective

1) Beyond Line-of-sight (BLOS) Communications.

The current family of US Army communications systems was designed to support the Cold War scenario. These systems were created to operate in a European theater and based on a maneuver scheme to defeat the Soviet Military. As such, the Mobile Subscriber Equipment (MSE) system, which is currently fielded to Army forces, relies on a grid network of line-of-sight connected node centers to link command posts at all levels. In order

to ensure a command and control capability, commanders are tied to this relatively large, inflexible, and immobile infrastructure, which limits their agility, speed, and distance between command posts.

As a lesson learned in OEF, operations in Southwest Asia are highly reliant upon beyond line-of-sight communications. The distances between command posts at all levels (strategic, operational, and tactical) greatly exceed the line-of-sight capabilities of the current communications equipment fielded to the US Army and the US Marine Corps.

To ensure consistent connectivity during OIF, senior commanders utilized single channel (25 KHz UHF) tactical satellite (TACSAT) assets while on the move and fell back on military X-band and commercial Ku-band TACSAT on the halt. This hybrid solution, though heavily dependent on commercial assets, proved invaluable in providing the robust, available on demand, communications data and voice links required by the Corps Commander down to his Division and Brigade TOCs.

2) Battle Command on the move.

US forces fully expected that movement of combat formations from the Kuwaiti border to the city of Baghdad would be swift. This speed of maneuver produced distances that exceeded the capability of today's

tactical radio systems normally assigned to these formations and hindered effective communications between tactical headquarters.

The Army, in response to this requirement, fielded Blue Force Tracking (BFT), a Force XXI Battle Command Brigade and Below (FBCB2) system that would allow V Corps to execute "battle command on the move" utilizing commercial L-band satellites. L-band connectivity was chosen because it could quickly be leveraged to provide a data connectivity path to 3rd Infantry Division given the compressed time constraints and exigent requirements of Operation Iraqi Freedom.

Blue Force Tracking permits low bandwidth connectivity over greater distances than had been doctrinally perceived to be within the realm of the possible. This connectivity allows the BFT equipped units to be visible on the Common Operational Picture (COP), which makes their location visible, in near real- time, at all levels. This provides the combat forces with a high degree of situational awareness, letting the units fight digitally enabled. This also produced the positive aspect of friendly force identification on the battlefield, which drastically reduced the possibility of fratricide in this non-linear fight. The Blue Force Tracking capability was critical to the success of 3rd Infantry Division and V Corps as they moved to Baghdad.

3) Importance of Coalition Information Sharing.

Operation Iraqi Freedom was executed with both the British and Australian combat forces playing an integral part of the scheme of maneuver. Both of these nations contributed land, air, and special operating forces to the campaign. These forces were, in many cases, integrated into the US formations. This type of integration mandated a level of information sharing and interoperability to achieve success.

Coalition forces required an unprecedented amount of operational and intelligence information to ensure they maintained an adequate level of situational awareness during combat operations. USCENTCOM, in coordination with the Office of the Assistant-Secretary of Defense-Network and Information Integration (ASD-NII), developed a coalition information sharing system called Coalition Enterprise Regional Information Exchange System (CENTRIXS). This system provided a variety of command and control computer applications, and allowed British and Australian tactical forces to receive the operational and intelligence information they required to execute operations. This computer based data network was fielded down to the brigade level in British formations and made available to Australian liaison officers working in the operation centers of US forces.

Conclusion

The US Army continues to take an analytical look at the lessons learned from Operation Iraqi Freedom to determine what adjustments must be made. The Army is thoroughly reviewing the force development areas of Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities (DOTMLPF) to improve our capability. The Army is continually trying to improve the force development cycle. The goal is to enable immediate changes that improve near-term combat capabilities, as well as better position itself for future success through stable longer-term research and development programs.

The Army is in the midst of a two-pronged operation that will be ongoing for the foreseeable future. Fighting the Global War on Terrorism with the current C4I systems while simultaneously over-watching the development of the Future Force, which in itself is part of the largest transformation in both Army and DoD history, and can only be successful if adequately resourced. What is clear is the need to invest in both emerging technology and emerging operational concepts that will make our forces more combat effective. The future war fighter will face a very cunning and adaptive enemy that practices asymmetric war fighting techniques more so than conventional. They will face-off on a non-contiguous battlefield separated by enclaves spread out over vast distances. The war fighter is looking to the signal community to provide a global interoperable, integrated network, which allows distributed planning and decentralized execution down to the individual soldier. The analysis that is underway within the services will

ensure that we are in a position to make improvements on the Joint C4I architecture and the systems that support that vision.

STATEMENT OF

BRIGADIER GENERAL MARC ROGERS, USAF

DIRECTOR, JOINT REQUIREMENTS AND INTEGRATION DIRECTORATE, J8

UNITED STATES JOINT FORCES COMMAND

BEFORE THE 108TH CONGRESS

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS, AND TERRORISM

21 OCTOBER 2003

FOR OFFICIAL USE ONLY
UNTIL RELEASED BY THE
COMMITTEE ON ARMED SERVICES
UNITED STATES HOUSE OF REPRESENTATIVES

Mr. Chairman, distinguished Members of the Committee, I am honored to testify on U.S. Joint Forces Command's role in Joint Battle Management Command and Control.

Let me open by assuring the Committee that U.S. Joint Forces Command is focused on strengthening Department of Defense capability to execute battle management command and control for our forces engaged in joint operations world-wide.

To achieve this goal, U.S. Joint Forces Command continues to maximize the Nation's future and present military capabilities by advancing joint concept development and experimentation, identifying joint requirements, ensuring interoperability, conducting joint training, and providing ready forces and capabilities - all in support of the Combatant Commands. Command and Control is fundamental to all of these efforts.

Joint Forces Command is a dynamic command that learns from and works with our partners throughout the Department to lead continuous evolutionary and revolutionary improvements in command and control. These collective efforts advance U.S. warfighting capabilities and enable continued success, including rapid, decisive military action.

In this regard, USJFCOM has received new authorities to ensure interoperability and integration of joint, coalition, and interagency capabilities in support of on-going military operations. In January 2003, internal Pentagon documents directed expanded responsibilities for Joint Forces Command in establishing Joint Battle Management Command and Control (JBMC2) requirements, identifying system-of-systems capability requirements and ensuring the integration and interoperability of JBMC2 capabilities. In this expanded role, JFCOM will lead JBMC2 mission and capability area

requirements to include: concepts, integrated architectures, systems interoperability and integration efforts, training and experimentation. These important aspects of JBMC2 will allow us to develop the overarching framework for joint command and control capabilities which will guide our future systems acquisitions, provide a basis for interoperability and integration of our legacy system capabilities, and allow a reference for prioritizing near term solutions to capability shortfalls.

Additionally, USJFCOM has assumed oversight responsibility for the Deployable Joint Command and Control program and the Single Integrated Air Picture, with expanded responsibilities for the Family of Interoperable Operational Pictures. This will allow Joint Forces Command to integrate programs and initiatives within the Joint Battle Management Command and Control arena and ensure joint requirements are funded and addressed on a priority basis.

In parallel with these new JBMC2 authorities, our Joint Interoperability and Integration Office (JI&I) efforts will continue to deliver solutions to interoperability challenges by working closely with Combatant Commanders, Services and Defense Agencies to identify and resolve joint warfighting deficiencies. JI&I's current efforts support military operations by fielding:

- Interoperable capabilities between US Army and US Marine Corps ground commander Command and Control elements
- Collaborative planning and coordination capabilities for the Combatant Commanders
- Improvements to Joint Task Force information assurance and information management

- Adaptive mission planning and rehearsal capabilities for the Combatant Commanders

Additional JI&I efforts that directly support the commanders of Northern, Central, Pacific and Special Operations Commands in the near future include fielding capabilities for:

- Joint Task Force (JTF) situational awareness, a Common Operational Picture (COP), and enhanced integration of the Joint Deployment
- Integrated joint targeting, and intelligence analysis
- Integrated Joint Intelligence, Surveillance, and Reconnaissance (ISR)
- Integration of Distributed Common Ground System multi-intelligence sources

New authorities under JBMC2 provide for an expansion of JI&I's mandate to increase operational through tactical level joint integration of the following capabilities:

- Common Operational and Tactical Pictures
- Combat Identification
- Situational Awareness
- Adaptive mission planning and rehearsal
- Interoperability among service intelligence systems
- Interoperable joint fires, maneuver, and intelligence
- Integrated Joint Battle Management Command & Control

This new emphasis will bolster U.S. Joint Forces Command's ability to deliver near-term enhancements to our joint force command and control capabilities.

The need for this comprehensive approach to JBMC2 is validated by some of the command and control lessons we have learned during operation IRAQI FREEDOM. Our preliminary insights concluded that one overarching theme summarized the results of the joint transformation since Desert Storm, which we characterize as Overmatching Power vice traditional Overwhelming Force.

As an example, in Desert Storm, our military thinking was to field **Overwhelming Force** to ensure victory. Certainly, this entails fielding well-trained and well-equipped forces, which is as important today as it was back then. However, the emphasis was on numbers as befits a traditional, attrition-based campaign. Our observations in Operation IRAQI FREEDOM tell us there is another approach to modern warfare. We like to describe this new approach as the employment of **Overmatching Power**.

The emphasis is on harnessing all the capabilities that our Services and Special Operations Forces bring to the battlespace in a coherently joint way. Advances in technologies, coupled with innovative warfighting concepts joined together by a new joint culture, are enabling a level of coherent military operations that we have not been able to achieve before. The emphasis now is on the effectiveness of joint capabilities employed at times and places of our choosing to achieve strategic effects. General Franks later remarked on this level of jointness, saying "Operation IRAQI FREEDOM was the most joint and combined operation in American history." The insights and perspectives gained from Operation IRAQI FREEDOM emphasize and rely on a cohesive and agile joint battle management command and control capability that supports new paradigms in planning, execution, and assessment of effects.

Essential to the power of adaptive planning and execution is our ability to conduct large scale, vertical and horizontal collaboration. This collaboration is on a scale that dwarfs any extant commercial application.

In today's collaborative environment, every level of command throughout the entire force and including coalition partners is electronically linked to the Combatant Commander's decision-making process. Subordinate commanders and staffs understand the context behind key changes across the battlespace and are fully aware of changes in the commander's intent to guide their actions during specific missions. In short, the entire joint force is acutely sensitive to any nuances that occur in the battlespace and are highly adaptive to changes, seizing opportunities as they arise or preventing mishaps before they occur.

At the top of the areas that achieved new levels of capability are joint planning, adaptation and joint force synergy. These capabilities are directly centered around our ability to collaborate. We have done well in this area, but we need to do better. Our investment in new initiatives such as the Deployable Joint Command and Control System (DJC2) and the Standing Joint Force Headquarters (SJFHQ) prototype will enable our future joint warfighting capability. Both of these initiatives are essential JBMC2 elements directly coupled under MID 912 authorities. I emphasize that they are not simply additional information technology programs. They are new capabilities at the core of our transformational Joint Command and Control initiatives.

While General Franks and his staff achieved these successes in Joint command and control, the overall information architecture they created for Operation Iraqi Freedom was patched together during the conflict in Afghanistan and the period preceding the outbreak of conflict. The many service and functional systems had to be linked together. The lack of seamless architectures affected their ability to collaborate in real time and use information from various databases. Our JBMC2 initiatives are designed

to eliminate the requirement for each Combatant Commander to create such ad hoc systems on the eve of conflict.

Intelligence architectures need to address the needed fusion of information and analysis necessary at various level of command. The overall system must enable sensors to plug and play from the strategic level to the soldier on the battlefield. Automated data fusion is needed to help manage this onslaught of information. Assessment of effects in a timely manner needs to be incorporated.

Our operational systems need to integrate fires throughout the battlespace. They need to be flexible and adaptive for on-call targets and direction from all levels of command. They should leverage both Blue Force Tracker and Combat ID in combination to reduce friendly fire incidents. They should incorporate dynamic airspace control. They must be fully integrated with other information architectures like the intelligence architecture. U.S. Joint Forces Command has conducted various studies related to horizontal integration of intelligence information, and recently the Defense Acquisition Board (DAB) has approved a strategy to integrate the various Service Distributed Common Ground Systems (DCGS) into a single interoperable capability.

Finally, as we build our information architecture, we need the capability to integrate interagency partners from other parts of the Federal government. Multi-level secure environments are needed to integrate coalition partners into our collaborative environment while fully protecting our US-only information and systems. U.S. Joint Forces Command is currently working directly with the staff of the Chairman of the Joint Chiefs of Staff and the Assistant Secretary of Defense, Networks and Information Integration to develop a roadmap for resolving Multi-National Information Sharing.

Clearly, improved coordination of initiatives and programs though authoritative oversight of related concepts, interoperability and integration efforts will enhance our ability to identify and implement solutions to lessons learned shortfalls. Our new JBMC2 authorities have already been instrumental in supporting implementation of the Standing Joint Force Headquarters prototype (SJFHQ). The SJFHQ is comprised of a small but powerfully enabled team of planners specifically trained to speed the operational employment of a larger joint task force headquarters with real-time, actionable and shared knowledge crucial to the conduct of rapid and decisive operations. This shared understanding is enabled by what we call the Collaborative Information Environment, or "CIE," that, in our judgment, may very well change the conduct of future warfare. This prototype is being implemented today in Pacific Command, European Command, Southern Command and Northern Command, with the target date of FY05 for the SJFHQ to be fully operational in all Regional Combatant commands. JBMC2 authorities have enabled us to directly couple the SJFHQ Warfighter requirements to the infrastructure provided by the Deployable Joint Command and Control (DJC2) capability.

Finally, fully networked forces supported by well defined joint battle management command and control requirements enable the creation and sharing of that knowledge needed to collaboratively plan, decide, and act quickly. It will allow the joint force to accomplish many tasks simultaneously from distributed locations in the battlespace. Networked forces (based upon systemic, organizational, and personal links) are necessary to compress and change today's sequential, echeloned way of planning and conducting operations. Networked forces use shared situational awareness among all elements of the joint force, to include interagency and multinational partners. This increases the speed and precision in planning, decision to act

and application of power. They allow streamlined, dynamic joint processes for the integration of information operations, fires, and maneuver elements as well as for sustainment and joint intelligence, surveillance, and reconnaissance management. Fully networked forces are necessary to employ a coherently joint force to achieve the Overmatching Power paradigm we glimpsed in Operation Iraqi Freedom.

Conclusion

U.S. Joint Forces Command, in coordination with our Service, Defense Agency and Combatant Command partners, will continue to execute our new JBMC2 authorities and build on our Joint Interoperability and Integration responsibilities by developing the command and control processes, architectures, systems, standards, and operational concepts to be employed by the Joint Force Commander. Our collective efforts, strengthened by the above partners, will continue to aim for an integrated, interoperable, and networked joint force that will:

- Ensure common shared situational awareness

- Provide fused, precise and actionable intelligence

- Support coherent distributed and dispersed operations, including forced entry into anti-access or area-denial environments

- Ensure decision superiority enabling more agile, more lethal, and survivable joint operations

While I have outlined our new authorities and focus for improving joint battle management command and control, I note the importance of continued

Congressional support in our efforts to break paradigms and accelerate improvements in command and control. U.S. Joint Forces Command looks forward to working with the committee to provide the men and women of our Armed Forces the joint command and control capabilities they need today and the transformational capabilities they will require in the future. Thank you.

QUESTIONS AND ANSWERS SUBMITTED FOR THE RECORD

OCTOBER 21, 2003

QUESTIONS SUBMITTED BY MR. THORNBERRY

Mr. THORNBERRY. Several of you mentioned in your testimony, the reliance on military and commercial satellite communications and the fact that you did not necessarily have enough bandwidth to get all the information you need. Admiral Cebrowski, Office of Force Transformation, is actually conducting an experiment for a small satellite, cheap and quick launch capability to provide more access to the battlefield commander. It could be one of those big bets that may pay off to help improve our C4ISR challenges. Are you familiar with this experiment that is supposed to support PACOM and are you working with the Office of Force Transformation to support this effort?

General LEAF. Yes, I am familiar with this initiative, and as the executive agent for space, the Air Force is working with the Office of Force Transformation on this effort. We are committed to developing operationally responsive space capabilities. This means delivering responsive spacelift and payloads. Within Air Force Space Command, the Space and Missile Systems Center at Los Angeles Air Force Base is leading the way to help ensure mission success on this venture through a streamlined safety review process. Additionally, this experiment will capitalize on current efforts at our Space Battlelab to allow theater forces to task the payload from the field. We look to base our operational requirements for future space capabilities on the results of experiments like this one. We value our partnerships with other offices and agencies in developing innovative ways to keep our space asymmetric advantage.

General MORAN. The experiment mentioned above is known as the Office of Force Transformation TacSat 1 project. The Army Space Battle Lab in Colorado Springs, working through the Air Force Space Battle Lab, has partnered with the Office of Force Transformation on this experiment. It is a significant project in that a major shortfall of today's full spectrum operations is the lack of a launch on demand capability. Experimenting with a satellite project of this nature is not a new experience for the Army. In 1999 the Space and Terrestrial Communications Directorate (S&TCD) of the Army Communications-Electronics Command (CECOM) managed a "smaller cheaper" satellite program that resulted in the launch of the Multiple Path Beyond Line-of-sight Communications (MUBLCOM) satellite into a Low Earth Orbit (LEO). It was a Technology Reinvestment Project (TRP) sponsored and partially funded by the Defense Advanced Research Projects Agency (DARPA) at an estimated project cost of $15M. The prototype system was designed to address many Department of Defense needs for secure, mobile, netted, interference-resistant, terrain-independent, all-weather communications, supporting combat network radios, as well as special missions such as long-range surveillance and fire support. I will direct CECOM provide lessons learned to Admiral Cebrowski's team.

General ROGERS. U.S. Joint Forces Command has not been involved with this experiment. However, USJFCOM J9 Space Experimentation Cell has been involved with a Defense Advanced Research Projects Agency sponsored program called Tactical Satellite 21. This program will give the warfighter the ability to launch a single satellite which will divide into three separate but identical satellites to provide an increased loiter time over the designated target area. USJFCOM J9 Science and Technology cell is monitoring the progress of this DARPA program.

Mr. THORNBERRY. Everyone has recognized our dependence on communications and intelligence and the tactical improvements to our operations that have resulted from improved connectivity and situational awareness. I say everyone and that includes our adversaries, who may in future conflict try to interfere with our communications. Who is responsible for protecting our communications and can you explain what you are doing to protect our C4ISR capabilities and what plans you have for the future?

General LEAF. First and foremost, every airman, soldier, sailor or Marine has a responsibility and role to play in protecting our C4ISR capabilities. It begins with good communications, computer and operations security procedures by everyone. Information operations will ensure the ability for C4ISR to occur. In addition to conventional means, we conduct information warfare to defend against adversary attacks. The Armed Forces, through United States Strategic Command and the Na-

tional Security Agency, deter and protect against advancing technologies that our adversaries may use. We use unique encryption devices to secure our communication transmissions. These devices authenticate data sources and guarantee data integrity. The Air Force, along with the others, are planning for future threats by continuing to research and develop more advanced defensive measures. Our vision is to have dominant C4ISR through 2020 and beyond.

General MORAN. The U.S. Army Network Enterprise Technology Command /9th Army Signal Command (NETCOM/9th ASC) is a worldwide command, control, communications and computers (C4) mission organization that has been assigned the mission to operate, manage, and defend the Army's portion of the Global Information Grid (GIG). The Army views Computer Network Defense (CND) as an activity within the greater context of the Computer Network Operations (CNO) Spectrum. In addition to CND, the other mutually supporting CNO activities include: Network Operations (NETOPS), Computer Network Exploitation (CNE), and Computer Network Attack (CNA). It is important to understand that all elements of the CNO spectrum (NETOPS, CND, CNE, CNA) are interrelated. CND efforts achieve maximum effectiveness only when executed in coordination with the other CNO elements. NETCOM/9th ASC teams with several other Army organizations to accomplish the CND mission, principally the 1st Information Operations Command (1st IOC) of the Army's Intelligence and Security Command (INSCOM), and the Computer Crime Investigative Unit of the Army's Criminal Investigation Command.

The Army's lead operational CND activity is the Army Network Operations and Security Center (ANOSC) of NETCOM/9th ASC. The ANOSC is physically colocated with the Army's Computer Emergency Response Team (ACERT), a subordinate element of the 1st IOC, at Ft. Belvoir, VA. Together, the ANOSC and ACERT direct, coordinate, and synchronize subordinate NETOPS/CND forces located worldwide supporting every regional Combatant Commander including Europe, South West Asia, Pacific, Korea, South and Central America, and the Continental United States (CONUS). In each of these theaters, the ANOSC/ACERT coordinate and direct Theater Network Operations and Security Centers (TNOSCs) that are co-located with Regional Computer Emergency Response Teams (RCERTs). These theater NETOPS/CND teams are responsible for the operation, management and defense of the theater information grid. Currently, they provide technical direction and control to subordinate NETOPS/CND forces within their theater, principally the Directors of Information Management (DOIM) at each Post, Camp, and Station and to the tactically deployed signal forces. In the near future, each theater TNOSC/RCERT team will have the capability to plan and synchronize the full spectrum of CNO in support of their Combatant Commander. At the tip of the spear are the Systems Administrators and Network Administrator (SA/NA) assigned to the Army's Major Commands (MACOMs) who are responsible for managing systems and ensuring they maintain current security baselines and patches.

The Army is a stakeholder in the Department of Defense's (DOD) efforts to mandate information assurance (IA) core enterprise services across the GIG and is fully engaged with DOD in facilitating DOD's transition to a net-centric IA strategy. Army is executing DOD's mandate to employment IA/CND technical solutions to the greatest extent possible through its Defense-in-Depth strategy of layering security tools and technologies throughout its cyber infrastructure. For example, Army is redesigning its attack sensing and warning and situational awareness sensor grid in cyber space, first implemented in 1998, to employ state-of-the art, high-speed intrusion detection, prevention and blocking capabilities to protect the Army's new cyber infrastructure. The Army will improve efficiencies by reducing the number of Army gateways from almost 300 down to 32 high capacity gateways, called Global Information Grid-Bandwidth Expansion (GIG-BE) sites. The first three of these gateways will be fielded in FY04.

The Army is also acquiring state-of-the-art, attack/event correlation and analysis tools capable of sorting through the "tons" of data generated by the Army's reengineered sensor gird in cyber space to provide attack sensing and warning. Automated analysis correlates seemingly diverse, disparate events that are in reality the product of a coordinated network attack. Current capabilities employ some visualization and automated correlation tools, but they are not sufficiently robust. Only through automated analysis of sensor grid data can the Army effectively find not only parasitic hackers and cyber terrorists, but also low visibility, highly lethal nation state attacks that currently threaten Army networks and systems.

The Army's innovative and highly successful use of reverse proxy technology to protect its publicly accessible web sites from hackers was recognized by the National Security Agency's (NSA) Red Team as the most effective means of protecting web sites employed in DOD during its test of DOD security. The NSA Red Team did not breech the Army's proxy defenses during its test.

At the core of layered defense are the system administrators/network managers who protect the servers and workstations by applying fixes/patches to computer vulnerabilities. In DOD the process to find, fix, report, and verify that system vulnerabilities have been fixed is known as the Information Assurance Vulnerability Management (IAVM) process. Up to now, finding and fixing vulnerabilities has been largely a manual process. As more and more vulnerabilities are identified, Army system administrators, with current capabilities, will not be able fix them in a timely manner. Army experience indicates a 2000% decrease in time required to find and fix vulnerabilities using automated tools. Automated scanning and remediation tools are essential and Army is participating with DOD in a U.S. Strategic Command (USSTRATCOM) led effort to select and deploy enterprise-wide automated scanning and remediation tools to be used by system administrators to find and fix computer vulnerabilities. The importance of automating the IAVM process received added emphasis from a General Accounting Office (GAO) review, directed by Congressmen Davis (VA) and Putnam (CA), of DOD/Service patch management capabilities. GAO is expected to report their findings to Congress in the Spring of 04.

The Army is improving its current security posture by implementing DOD Public Key Infrastructure (PKI) and Smart Card technology on a global scale. The benefits of PKI include authentication, data integrity, confidentiality, and nonrepudiation. While current PKI/Smart Card capabilities are being fielded for the sustaining base, Army is currently reviewing processes for infusing PKI technology into tactical applications.

In addition to cryptographic authentication, the Army is a key player in the future use of biometric information to augment or possibly replace cryptographic authentication. Biometrics technologies utilize measurable physical or behavioral characteristics in order to authenticate the identity of an individual. Examples of biometric technologies include fingerprint scanners, voice recognition devices, finger/hand geometry scanners, iris scanners, and facial recognition cameras, among others. Biometric technologies have the potential to greatly enhance IA, physical security, force protection capabilities and to improve business processes. In FY 2000, Congress directed the DOD to establish a DOD Biometrics Program with the Army as the program's Executive Agent. As the Executive Agent, the Army's vision for the DOD Biometrics program is to make biometrics an empowering technology that ensures that the right person, with the right privileges, can authenticate for timely access to secure systems and facilities and support war fighter dominance. The Army established a DOD Biometrics Management Office (BMO) to execute the DOD Biometrics Program. The BMO's mission is to establish various DOD enterprise solutions and frameworks required to permit biometrics to be adapted throughout DOD. To this end, the BMO performs such functions as biometrics policy development, biometrics technology standards and architectures development, technology demonstrations, biometrics education and training development, planning, programming, and budgeting for biometrics requirements, and executing DOD Biometrics Program funds.

The Army's current inventory of cryptographic systems are technologically outdated, becoming logistically non-supportable and do not support the transition to DOD's net-centric strategy. The Army is modernizing its cryptographic systems with state-of-the-art technology embedded in radios, communications systems, and telemetry devices to provide robust encryption, achieve interoperability with joint and coalition forces, and transform to DOD's net-centric functionality. The Army is also implementing DOD's Electronic Key Management System (EKMS) that will migrate to the Key Management Infrastructure (KMI) program. The EKMS/KMI program provides modern management for the ordering, generation, distribution, storage, tracking, and accountability of cryptographic keying material. The KMI program ensures that cryptographic keying material gets to the warfighter in a timely and effective manner and is a technology enabler for scalable, reconfigurable, and reprogrammable cryptographic products.

General ROGERS. The protection of communications capabilities is critical to the successful execution of our missions. This is a shared responsibility of all members and organizations within the Department of Defense. At USJFCOM our area of responsibility is the future, and we have four initiatives underway to improve the ability of DOD to protect information and the Global Information Grid.

First, in support of a DOD Computer Network Defense Solutions Steering Group pilot effort, we recently deployed a tool within the headquarters and several of our subordinate units intended to track and audit compliance with Information Assurance Vulnerability Alerts. This tool will enable commanders at all levels to verify that their information systems have been updated with the latest software patches, thereby preventing a hacker from exploiting a known vulnerability to gain access to a network or deny services provided by that network. The results of this initial

deployment will be used to support ongoing DOD efforts to improve the security of the Global Information Grid.

Second, we are also working on establishing requirements for modernizing our cryptographic equipment. Specifically, the Chairman of the Joint Chiefs of Staff recently approved the Capstone Cryptographic Modernization Requirements Document defining requirements and standards for families of cryptographic equipment, thereby preventing the acquisition of stovepipe solutions by the Services, Combatant Commands and Agencies.

Third, we are working to establish requirements and identify secure solutions to implement Multi-National Information Sharing. Our Lessons Learned Team's analysis of Operation Iraqi Freedom highlighted the requirement to establish secure and reliable architectures permitting our forces to share information with our coalition partners.

Fourth, the Joint C4ISR Battle Center (JBC) established an Information Assurance Computer Network Defense (IA/CND) center of excellence, to maintain pace with rapidly changing developments in IA/CND and to educate and share expertise. JBC has also developed IA/CND prototypes.

Mr. THORNBERRY. Does DOD have an overall IT Enterprise Architecture today? If so, is it viable and does it encompass commonality among services, staffs, and defense agencies?

General LEAF. Yes, the Global Information Grid and associated enterprise services form the framework for an overall architecture. This framework will enable horizontal and vertical integration of forces to achieve our national strategy and objectives. It provides the necessary vision and guidance to develop systems and tie interoperable architectures together for net-centric operations and warfare. The Air Force embraces these architectural concepts in developing its enterprise and lower level architectures. This framework and associated models are being used as a starting point for Air Force development efforts. It guides our budgeting and acquisition decisions to make sure future Air Force capabilities are compatible in joint, interagency, and coalition environments.

General MORAN. Yes, The Department of Defense has an Enterprise Information Technology (IT) Architecture called the Global Information Grid (GIG) Architecture. An initial baseline (GIG Arch Version 1.0) represents the current "As-Is" Enterprise IT Architecture. While the GIG Architecture (Version 2.0) depicts the objective "To-Be" Enterprise IT Architecture. The Net-Centric Operations & Warfare (NCOW) Reference Model describes the net-centric strategy to move from the "As-Is" GIG Architecture to the objective GIG Version 2.0. The GIG Architecture is based upon the Joint Task Force (JTF) "business model" as described in joint doctrine. Therefore, they have a particular "look and feel" that is Combatant Command (COCOM) and warfighting domain specific. The NCOW Reference Model is being developed to ensure the means to simplify compliance with the GIG Architecture and to achieve interoperability and commonality among all DOD Components.

Additionally, the DOD Comptroller is developing the "business side" of the GIG as the DOD Business Enterprise Architecture (BEA).

General ROGERS. DOD strategy to obtain IT Enterprise Architecture is described in the Global Information Grid Enterprise Service (GES) and Net Centric Enterprise Service (NCES) architecture documents and products. The DOD Chief Information Officer is lead for this emerging effort.

Mr. THORNBERRY. You mentioned a prototype project called the Collaborative Information Environment that helps with real time, actionable, and shared knowledge. You also mentioned the need for multilevel security and information sharing with partners and allies. It seems to me that some of this philosophy has applications for homeland defense and homeland security. Can you tell me if it would be possible to talk to the folks in DHS to see if you can share some of your ideas and lessons learned to help them with similar problems?

General ROGERS. We have recognized and documented the issue relating to information sharing within the interagency context. The USJFCOM sponsored Content Based Information Security (CBIS) Advanced Concept Technology Demonstration (ACTD) Operational Manager visited U.S. Northern Command (USNORTHCOM), at their request, to present the ACTD objectives and status. The USNORTHCOM representatives realized that a CBIS-like capability is needed to share information among the interagency organizations it collaborates with during Homeland Defense exercises and real world, current operations.

USJFCOM has been working Collaborative Information Environment (CIE) development and implementation across the Combatant Commanders for over 10 months. We have also been working with Homeland Defense (HLD) and other Services, Agencies and research facilities through an ongoing "Government Convention on

Emerging Technologies" whose membership includes key officials in the Department of Homeland Security.

QUESTIONS SUBMITTED BY MR. LARSEN

Mr. LARSEN. During combat, the battle commander relies on computer programs to indicate where his troops are located and where the enemy is. How can the commander ensure that the information being displayed is accurate and not being disrupted by a hacker who is displaying inaccurate information?

General LEAF. Any combat identification needs proper authentication to prevent spoofing by an adversary. Through automatic and manual interrogations, we depend upon challenge and reply techniques to guarantee integrity of information in tactical and operational engagement decisions. We use vetted rules of engagements and a balance of technology and human decisions to make certain accurate information is presented. We must have a sound understanding and awareness of the battlespace to achieve maximum efficiency of effort. Commanders trust technology and their troops to properly employ in the heat of battle.

General MORAN. Networks and systems that carry intelligence data on the position and disposition (orders of battle) of enemy (red) forces are highly secure and employ varying degrees of encryption security, dependent on the level of security required, e.g., confidential, secret, top secret, sensitive compartmented information, etc. The Secure Internet Protocol Router Network (SIPRNet) and the Joint Worldwide Intelligence Communications System (JWICS) are two examples of secure networks currently in use. Battle commanders can track their own forces (blue force tracking) using both Government-Off-The-Shelf (GOTS) and Commercial-Off-The-Shelf (COTS) security devices. These devices are currently in use (integrated) on many networks and platforms that provide the capability to ensure the integrity and the authenticity of information being exchanged. These solutions employ varying degrees of encryption security, dependent on the level of security required (e.g., unclassified sensitive, confidential, secret, top secret), that have corresponding progressive levels of security robustness. Inline Network Encryption (INE) (end-to-end source encryption) devices, crossdomain solutions (high assurance data guards) and secure appliqués (modules) integrated on COTS and GOTS provide the commander with the assurance of information integrity and accuracy as data is only unencrypted (intelligible) in the operations center and the vehicle's display unit.

General ROGERS. Accuracy of data presented to a battlefield commander is of the utmost importance. Data integrity exists when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed. To ensure our information systems achieve data integrity, we continuously assess the risks and threats that would cause the data to change. Through our concept of Defense in Depth, we utilize our people, technology, and operational procedures to ensure that data integrity is maintained as a key element of Information Assurance.

One factor in ensuring data integrity is to protect the pathways used to transport the information, the Global Information Grid (GIG). The GIG is protected through the use of firewalls and intrusion detection systems intended to identify and thwart potential hackers and by authentication systems to assure data integrity. At the tactical level, information exchanges are protected by National Security Agency certified cryptographic devices at the information and transport levels.

Thus the use of protective devices such as firewalls and intrusion detection systems, authentication, and encryption ensures that the data received by the battlefield commander is accurate and has not been tampered with by a hacker.

Numerous complementary actions are taken to ensure the information provided to the commander is accurate, timely, and trusted. Beginning with basic network connectivity, Secure Internet Protocol Router Network (SIPRNET) infrastructure is established, tested, and accredited by both the Defense Information Systems Agency (DISA) and Service network providers. This includes fielding of appropriate firewalls and approved guards for the trusted exchange of information between networks of different classification levels. Procedures are established to grant users accounts on this classified network, as well as our unclassified network.

Applications running on the SIPRNET are designed to ensure trusted operation. Security design requirements become increasingly stringent based on the sensitivity of the data processed and the criticality to the ongoing operation.

Prior to fielding, applications are subjected to security testing to validate their compliance with security requirements, and a Designated Approving Authority must accredit the application in order for it to be placed in operational use. Safeguards built into classified systems include authentication, authorization (access control),

and auditing capabilities. In addition, system-to-system interfaces are tested for secure operation.

Finally, system administration personnel use automated tools to constantly monitor both the networks and applications for unauthorized, suspicious, and malicious activity. Through the use of automated tools and manual procedures, system administrators ensure that only authorized personnel have access to the network and only those authorized users with a valid need are permitted access to applications. System-to-system interfaces are configured securely, as they were designed/tested. Blue Force and Red Force data is typically confirmed and correlated via multiple trusted and authoritative data sources.

These multiple and complementary actions ensure the data presented to the Commander is trusted and timely.

Mr. LARSEN. I am also concerned about the so-called digital divide between our armed forces and those of our allies. As we continue to rely on international coalitions to fight the Global War on Terrorism, maintaining some ability to communicate and fight alongside our allies is important. While I strongly support efforts to improve our nation's military prowess, technology, and weaponry, working with allies must be a priority for us as we move forward. Please respond to this statement.

General LEAF. I fully agree that coalition interoperability is critical to the way we fight. We depend on our allies to help fight the war on terrorism and engage in military operations around the world. The Air Force is actively working both policy and systems to better incorporate our allies in planning and executing coalition operations.

General MORAN. The application of military force in the 21st Century will be demanding. Unilateral capability is important to nations but most planning is made on the assumption of alliance and coalition operations in scenarios that are difficult to predict and which often arise on short notice. To achieve this, an assured capability for interoperability of information is essential. Additionally, forces must interact with non-governmental organizations, including international aid organizations. The Project Managers of the Army Command and Control Information Systems (C2IS) of Canada, France, Italy, the UK and the US established the Multilateral Interoperability Program (MIP) in April 1998.

The MIP aims to deliver an assured capability for interoperability of information to support land focused coalition/joint operations at all levels from corps to the lowest appropriate level in order to support combined and joint operations and pursue the advancement of digitization in the international arena to include NATO. In an MIP environment, a community of MIP systems, nations, command levels and organizations can share: 1) Situational Awareness; 2) Plans and Orders; 3) NBC Alerts and critical messages.

The MIP specification consists of common interface and exchange mechanisms to exchange information between co-operating but diverse C2 systems. The common interface is the Land C2 Information Exchange Data Model, LC2IEDM. It models the information that allied land component commanders need to exchange both vertically and horizontally.

General ROGERS. The "digital divide" is a concern not only with our closest allies but also with our coalition partners that bring considerable knowledge and assets to the Global War on Terrorism (GWOT). Two projects within USJFCOM are beginning to address some of these concerns.

The first is the Multinational Information Sharing (MNIS) Transformation Change Package (TCP). Organization policy and capability considerations are defined in the TCP. It recommends actions to prepare warfighters for better information sharing. The second is the Content Based Information Security (CBIS) Advanced Concept Technology Demonstration (ACTD), which will potentially answer the material capability requirements of the TCP. The project encrypts information at its source and only allows access to that information based on proper authorization.

USJFCOM and the National Security Agency are building and integrating several CBIS technologies to meet international standards. This will allow the lead nation of a coalition to provide its own sovereign encryption mechanisms for use by the coalition. The ability to put all the GWOT partners on a single network is an attempt to bridge any "digital divide."

○