CYBER SECURITY CHALLENGES AT THE DEPARTMENT OF ENERGY

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

JUNE 9, 2006

Serial No. 109-107

Printed for the use of the Committee on Energy and Commerce

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

U.S. GOVERNMENT PRINTING OFFICE

29-892PDF WASHINGTON : 2006

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 ENERGY AND COMMERCE

JOE BARTON, Texas, *Chairman*

RALPH M. HALL, Texas
MICHAEL BILIRAKIS, Florida
Vice Chairman
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
NATHAN DEAL, Georgia
ED WHITFIELD, Kentucky
CHARLIE NORWOOD, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING, Mississippi
Vice Chairman
VITO FOSSELLA, New York
ROY BLUNT, Missouri
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
C.L. "BUTCH" OTTER, Idaho
SUE MYRICK, North Carolina
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee

JOHN D. DINGELL, Michigan
Ranking Member
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MIKE DOYLE, Pennsylvania
TOM ALLEN, Maine
JIM DAVIS, Florida
JAN SCHAKOWSKY, Illinois
HILDA L. SOLIS, California
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas

BUD ALBRIGHT, *Staff Director*
DAVID CAVICKE, *General Counsel*
REID P. F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

ED WHITFIELD, Kentucky, *Chairman*

CLIFF STEARNS, Florida
CHARLES W. "CHIP" PICKERING, Mississippi
CHARLES F. BASS, New Hampshire
GREG WALDEN, Oregon
MIKE FERGUSON, New Jersey
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
JOE BARTON, Texas
(EX OFFICIO)

BART STUPAK, Michigan
Ranking Member
DIANA DEGETTE, Colorado
JAN SCHAKOWSKY, Illinois
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
HENRY A. WAXMAN, California
JOHN D. DINGELL, Michigan
(EX OFFICIO)

CONTENTS

CYBER SECURITY CHALLENGES AT THE DEPARTMENT OF ENERGY

FRIDAY, JUNE 9, 2006

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:42 a.m., in Room 2123 of the Rayburn House Office Building, Hon. Ed Whitfield [Chairman] presiding.

Present: Representatives Whitfield, Bass, Walden, Burgess, Blackburn, Barton (Ex Officio), Stupak, DeGette, and Inslee.

Staff Present: Mark Paoletta, Chief Counsel for Oversight and Investigations; Dwight Cates, Professional Staff Member; Tom Feddo, Counsel; Matt Johnson, Legislative Clerk; and Chris Knauer, Minority Investigator.

MR. WHITFIELD. This meeting will come to order.

Once again, I apologize to you all for the delay, but there were a few items that came up at the last minute that we needed to discuss.

Today, we are going to have a hearing on the review of cyber security challenges at the Department of Energy; and today's hearing will focus on ongoing challenges to secure DOE's unclassified network as well as the Department's efforts to address specific cyber security weaknesses that have been identified by the Department of Energy Inspector General and the Office of Security and Safety Performance Assurance.

This is not a new issue for the subcommittee. In April of 2001, this subcommittee held a hearing to review the security of government computer systems. At that hearing, Mr. Glenn Podonsky, who is the Director of DOE's Office of Security and Safety Performance Assurance, provided a demonstration of cyber penetration techniques used to gain access to the DOE unclassified network.

In the 5 years since that hearing, there has been a worldwide surge in the number of identified cyber security vulnerabilities as well as a surge in malicious cyber activity designed to exploit those vulnerabilities. In fact, looking back at our April, 2001, hearing, I think we could consider that period as the good old days, compared to the challenges that we face today. All indications point to a continually evolving cyber threat

environment where malicious activity will continue to increase in complexity.

A recent report from Simtek Corporation points out that computers based in the United States account for 31 percent of all cyber attacks. Ranked second is the rapidly increasing cyber threat originating from China. According to a March, 2006, report from Simtek, attacks originating in China last year increased by 153 percent. According to Simtek, these attacks from China are a likely sign that more attackers have become active within the country.

In response to the growing cyber threat, it is critical that DOE develop and maintain a robust cyber security posture to defend against unauthorized penetrations into its unclassified network. A comprehensive cyber security effort at DOE is particularly challenging due to the large number of systems maintained by the Department and their geographical dispersion.

In a recent portion, Mr. Podonsky noted that DOE's approach to cyber security does not provide the degree of structure, direction and management involvement necessary to support effective decision making and program implementation.

To emphasize this point, last year, Mr. Podonsky conducted an unannounced internal red team penetration test that successfully gained control of a DOE site network. From there, the red team exploited existing network interconnections to gain control of several other DOE site networks. This internal performance test identified previously unsuspected vulnerabilities.

In response to these alarming findings, the DOE Office of the Chief Information Officer has worked in conjunction with NNSA and DOE program officers to develop a revitalization plan to revitalize the DOE's cyber security posture.

The committee staff has reviewed the Chief Information Officer's revitalization plan, and it does appear to be comprehensive. When implemented, the revitalization plan should resolve many of the Department's cyber security weaknesses, or at least that's our hope. Unfortunately, based on a recent update from the Department, progress on many of the corrective actions in the revitalization plan have already fallen behind schedule.

Although the unclassified network does not contain classified information, it does contain sensitive and confidential information. In some cases, important research at the national laboratories are initiated and developed on unclassified networks until they reach a stage of development that requires them to be classified. These and other sensitive unclassified information require the best protection.

I would also note that approximately 75 percent of the DOE computer systems are actually operated by contractors. Thus, in order to successfully address the Department's cyber security challenges, the Department will need to have each of its contractors on board.

We look forward to hearing today from Mr. Tom Pyke, the Department's CIO, as well as Under Secretary Linton Brooks and Under Secretary David Garman on the steps they are taking to improve cyber security.

We plan to conduct as much of this hearing as possible in an open public format. However, we know that at some point we are going to move the hearing into Executive Session where we can discuss sensitive information.

One of the pieces of information that came to our knowledge just last night that raises serious concerns for all of the members of the subcommittee relates to the fact that the personnel files, including Social Security numbers, of 1,500 Federal and contract employees at DOE, were exfiltrated by an unknown hacker. The point that really upsets us in the committee about this is that this information was known somewhere within the Department of Energy 8 months ago and yet, from the information that we have, that information was not shared with the Secretary of Energy himself, and was not shared with the CIO.

Of course, Mr. Brooks will be with us on the second panel, as well as others, and we will be asking some questions about this. But we are going to have to go into Executive Session to get into any detail on that issue because of the classified information.

But I do want to just reiterate the fact that this alleged breach occurred 8 months ago within the Department of Energy and personnel files of 1,500 DOE employees has been obtained by some unknown hacker and is of great concern to all of us.

With that, I recognize the gentleman from Michigan, Mr. Stupak.

[The prepared statement of Hon. Ed Whitfield follows:]

PREPARED STATEMENT OF THE HON. ED WHITFIELD, CHAIRMAN, SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

This hearing will come to order. Today we will review the status of cyber security at the Department of Energy and the National Nuclear Security Administration. Today's hearing will focus on ongoing challenges to secure DOE's unclassified network, as well as the Department's efforts to address specific cyber security weaknesses that have been identified by the DOE Inspector General and the Office of Security and Safety Performance Assurance.

This is not a new issue for the Subcommittee. In April of 2001 this Subcommittee held a hearing to review the security of government computer systems. At that hearing, Mr. Glenn Podonsky - who is the Director of DOE's Office of Security and Safety Performance Assurance - provided a demonstration of cyber-penetration techniques used to gain access to the DOE unclassified network. In the five years since that hearing there

has been a worldwide surge in the number of identified cyber security vulnerabilities as well as a surge in malicious cyber activity designed to exploit those vulnerabilities. In fact, looking back at our April 2001 hearing, I think we could consider that period as "the good old days" compared to the challenges we face today.

All indications point to a continually evolving cyber threat environment where malicious activity will continue to increase in complexity. A recent report from Symantec Corporation points out that computers based in the United States account for 31% of all cyber attacks. Ranked second behind the US is the rapidly increasing cyber threat originating from China. According to a March 2006 report from Symantec, attacks originating in China last year increased by 153%. According to Symantec, these attacks from China are "likely a sign that more attackers have become active within the country."

In response to the growing cyber threat, it is critical that DOE develop and maintain a robust cyber security posture to defend against unauthorized penetrations into its unclassified network. A comprehensive cyber security effort at DOE is particularly challenging due to the large number of systems maintained by the Department, and their geographical dispersion. In a recent report, Mr. Podonsky noted that DOE's approach to cyber security "does not provide the degree of structure, direction, and management involvement necessary to support effective decision-making and program implementation."

To emphasize this point, last year Mr. Podonsky conducted an unannounced internal "red team" penetration test that successfully gained control of a DOE site network. From there, the red team exploited existing network interconnections to gain control of several other DOE site networks. This internal performance test identified previously unsuspected vulnerabilities.

In response to these alarming findings, the DOE Office of the Chief Information Officer has worked in conjunction with NNSA and DOE programs offices to develop a "revitalization plan" to revitalize the DOE cyber security posture. The Committee staff has reviewed the CIO's revitalization plan, and it appears comprehensive. When implemented, the revitalization plan should resolve many of the Department's cyber security weaknesses. Unfortunately, based on a recent update from the Department progress on many of the corrective actions in the revitalization plan have already fallen behind schedule.

Although the unclassified network does not contain classified information, it does contain sensitive and confidential information. In some cases important research at the national laboratories are initiated and developed on unclassified networks until they reach a stage of development that requires them to be classified. These and other sensitive unclassified information require the best protection. I would also note that approximately 75% of DOE's computer systems are actually operated by contractors. Thus, in order to successfully address the Department's cyber security challenges, the Department will need to have each of its contractors on board.

I look forward to hearing from Mr. Tom Pyke, the Department's Chief Information Officer, as well as Under Secretary Linton Brooks and Under Secretary David Garman on the steps they are taking to improve cyber security.

I plan to conduct as much of this hearing as is possible in an open, public format. However, I expect that at some point we will move the hearing into executive session where we can discuss sensitive information. I look forward to hearing from the witnesses and I yield back the balance of my time.

MR. STUPAK. Thank you, Mr. Chairman; and thank you for holding this hearing.

Today's hearing is on a subject that most people don't think about and, quite frankly, take for granted. Nonetheless, the issue of cyber security can have profound consequences to the Nation's national security if not handled competently and aggressively.

The issue of cyber security is a matter that this subcommittee has examined for years. How Federal agencies and departments protect sensitive systems and the information they contain from malicious hackers or foreign agents is something that we should all be concerned about.

The Department of Energy has literally hundreds of thousands of computers and a myriad of networks that can all serve as potential vectors for external threats. These computers and networks, both classified and unclassified, hold very sensitive information on a range of issues. These systems must be protected with vigor. Failure to do so can result in huge losses of critical data, including data related to national security.

Mr. Chairman, what we will hear today, however, is a mixed report card. On one hand, we will hear that improvements in securing this information have been made and continue to be made. However, we will also hear that significant progress is still needed on behalf of the DOE Chief Information Office to better secure the Department's key systems.

The Department of Energy Inspector General and DOE's Director of Office of Security and Safety Performance Assurance have both found considerable weaknesses in key DOE systems. Both of these entities in various audits and red teaming examinations have determined as recently as last year that DOE systems, particularly those networks which contain unclassified information, are entirely too vulnerable. We will hear from both offices that, while DOE strives to close these weaknesses against outside threats, more must be done and it must be done soon.

Mr. Chairman, I do note that this hearing will be conducted partially in open session and partially in closed session. I support this approach because it is only during the closed session that we will be able to discuss the details of where DOE has failed to secure key systems in the past and where the Department remains vulnerable today. I believe that a vigorous discussion in the closed session will underscore what many of us know, which is that significantly more attention must be paid to this important area.

Mr. Chairman, I do look forward to the testimony from the excellent witnesses we have before us today. I look forward to continuing to work with you to explore additional ways to secure DOE key information systems.

As many have noted in their testimony, the threats of DOE information systems have never been greater, and those threats continue

to grow in sophistication and intensity every day. I concur with those statements based on what I have seen through this investigation, and I underscore the need to hold the Department accountable in this regard.

Mr. Chairman, I look forward to hearing from our witnesses. You mentioned about the exfiltrated information, and I look forward to going into closed session to discuss it. I really would like to know why it takes 8 to 9 months for this committee, which has jurisdiction and has taken a great interest for a number of years on this issue, that we once again are about 8 to 9 months behind without any proper notification.

MR. WHITFIELD. Thank you, Mr. Stupak.

At this time, I recognize the gentleman from Texas, Dr. Burgess, for his opening statement.

MR. BURGESS. Thank you, Mr. Chairman. I will be brief, because I am anxious to get to the testimony of the witnesses, and much of the information we have had prior to this hearing we only got this morning.

But we live in a dangerous world, and there are clever enemies both within and without our country. Our national security has become the most important issue facing the Nation, and indeed it is our most important job here in the United States Congress. We must do everything within our power to ensure that we do not become victims of terrorism again.

Our committee has a very important responsibility to the American public, and I am glad that we are conducting the oversight of the nuclear facilities. As terrorists become more and more sophisticated, we must continue to implement and maintain comprehensive measures to secure our safety.

Mr. Chairman, I welcome the fact that you are holding so much of this hearing in open session. You are to be commended for that. I do understand the necessity for holding a portion of this hearing in closed session.

I am concerned about the reported lack of safety and security surrounding some of our nuclear facilities. As we have recently learned, there have been instances where cyber attacks could have been avoided if simple security controls such as security patches and passwords had been implemented.

While many cyber problems cannot be cured by a patch or password, it's astonishing the agency responsible for so many of our national security measures could have overlooked the simplest of solutions. It is no wonder that Inspector General Gregory Friedman has given the Department of Energy an unsatisfactory assessment during its recent evaluation under the Federal Information Security Management Act.

I am encouraged by the assessment, I am encouraged by the Department of Energy's revitalization plan, and Mr. Stupak pointed out

that is part of a mixed report card, but I am encouraged by the revitalization plan, and I look forward to discussing this issue in more detail.

Again, Mr. Chairman, I thank you for calling this crucial hearing; and we will discuss all of these issues in more detail later this morning. Thank you.

MR. WHITFIELD. Thank you, Dr. Burgess.

At this time, I will recognize the full committee Chairman, Mr. Barton of Texas, for his opening statement.

CHAIRMAN BARTON. Thank you, Mr. Chairman. I am going to submit my formal statement for the record.

I think it is a very important hearing. I have just learned of something within the last 15 minutes that makes it even more important. I am attempting to touch base with the Secretary of Energy and consult with Mr. Dingell, but we have got some major problems, and if the Administration won't do something about it, this committee, I hope, will.

So thank you for holding this hearing.

MR. WHITFIELD. Thank you, Chairman Barton.

[The prepared statement of Hon. Joe Barton follows:]

PREPARED STATEMENT OF THE HON. JOE BARTON, CHAIRMAN, COMMITTEE ON ENERGY AND COMMERCE

Thank you for holding this hearing, Mr. Chairman. I think this may be one of the most important hearings we will have on DOE security matters.

Over the past several years the Subcommittee has held multiple hearings on the status of physical security at DOE sites. We reviewed whether the Department has enough guards and guns to protect our nuclear facilities, but the threat from threat posed by malicious intruders on the internet is a growing security problem, and its a problem that DOE needs to more attention on.

If left unattended, cyber security weaknesses at DOE could allow malicious individuals, hackers, or even groups backed by nation-states to penetrate DOE and gain access to sensitive information. We know the hackers are out there and we know their attacks have caused damage to DOE networks. We also know that thousands of attempts to beat DOE cyber security occur literally every day.

Recent penetration testing conducted by DOE's Office of Security and Safety Performance Assurance showed that DOE has plenty of work to do to convince me that its computer networks are secure. I understand that the Department has responded to these recent findings with a comprehensive plan to improve cyber security across the weapons complex.

The Department's new comprehensive plan probably identifies several good solutions to address cyber security problems. However, I am concerned with DOE's ability to follow through with its implementation plans.

Due to extensive network interconnections that exist between DOE sites, a comprehensive cyber security program will require coordinated teamwork among very different DOE sites and programs that have not worked well together in the past. A strong central policy on cyber security will also require NNSA to operate less like an autonomous agency, and work more closely with DOE policy and oversight programs.

It is important that the Office of Security and Safety Performance Assurance and the DOE Inspector General continue to oversee DOE's implementation of corrective actions. Ongoing site inspections and unannounced network penetration testing by these offices will provide a good indication of whether DOE has successfully implemented better cyber security protections. I thank the Chairman and I yield back.

MR. WHITFIELD. At this time, recognize the gentlelady from Tennessee, Mrs. Blackburn, for her opening statements.

MRS. BLACKBURN. Thank you, Mr. Chairman. I, too, will be submitting my statement for the record.

I want to thank the witnesses that are joining us today, and I want to thank you for working with us. It is an imperative that our constituents, the American people, know that they can trust this Government; and when there are items that cause that distrust, when there are actions that occur from the bureaucracy that encourage distrust, it is of tremendous concern to us.

So I thank you for your willingness to be here and to work with us; and, with that, I yield back.

MR. WHITFIELD. At this time, I recognize Mr. Walden of Oregon, who is Vice Chairman of the committee, for his opening statement.

MR. WALDEN. Thank you very much, Mr. Chairman.

I am deeply concerned about the vulnerability we continue to see in our data files not only in this agency but across this Government, and I think this committee is doing its due diligence along with those on this first panel to figure out how to fix those problems.

I am also deeply disturbed about the loss of employee records. Some 1,800 employees, I understand, have had their records compromised or taken in a breach of security; and it troubles me even more that it maybe has been 8 months and they still don't know.

That lack of notification is problematic. It seems to be symptomatic across the Government and raises very serious issues in this Member's mind about notification systems to the highest levels of the Government, and by that I mean up at least to the Secretary's office as well as in consultation with the Congress.

I also am concerned about--not necessarily in this agency, perhaps, although we may learn more in closed session, but in other agencies about people who have access to data both in and out of the Government and especially those inside the Government, what kind of background checks we do.

We have had a policy in the Government of encouraging people, for example, to telecommute, and yet in a discussion I had with a Cabinet Secretary earlier this week, he pointed out we don't do background checks on those people. So in the name of energy conservation and employment morale, we open up our systems to people who work from

home. They are able to access systems that may give them access to very important data; and who knows what cross pressures they are under and what they could do with that data, those employee records or Social Security numbers, with identification theft being so rampant and so expansive and so troubling for people in America today.

I think we have got to look across the Government, not just at this agency, especially at this agency because of its security issues, but also across the rest of the Government and definitely for a better cyber security policy than we are seeing today.

So, Mr. Chairman, I appreciate your leadership on this issue; and I look forward to delving into why these records were accessed, why people weren't notified, why the Secretary himself was not notified for, apparently, many months.

So I yield back, and I appreciate your work and that of our staff on this issue.

MR. WHITFIELD. Thank you, Mr. Walden.

At this time, recognize the gentleman from New Hampshire, Mr. Bass.

MR. BASS. Mr. Chairman, I thank you for holding this hearing. I have no opening statement. Look forward to hearing from our witnesses.

MR. WHITFIELD. Thank you.

That concludes the opening statements.

I want to welcome the first panel, the Honorable Gregory Friedman, who's the Inspector General at the Department of Energy, and Mr. Glenn Podonsky, who is the Director of the Office of Security and Safety Performance Assessment at the Department of Energy.

As you all know, this is an Oversight and Investigations hearing, and it is our policy to take testimony under oath. Do either of you have any difficulty testifying under oath? Do you have legal counsel that you would like to introduce?

Okay. Then if you would both stand up and raise your right hand.

[Witnesses sworn.]

MR. WHITFIELD. Thank you very much. You are now under oath.

TESTIMONY OF THE HONORABLE GREGORY FRIEDMAN, INSPECTOR GENERAL, U.S. DEPARTMENT OF ENERGY; AND GLENN S. PODONSKY, DIRECTOR, OFFICE OF SECURITY AND SAFETY PERFORMANCE ASSESSMENT, U.S. DEPARTMENT OF ENERGY

MR. WHITFIELD. Mr. Friedman, I recognize you for your opening statement of 5 minutes.

MR. FRIEDMAN. Mr. Chairman and members of the subcommittee, I

am pleased to be here at your request to testify on cyber security issues at the Department of Energy.

The Department, which spends over $2 billion each year on information technology, has a current inventory of approximately 800 information systems. These systems process highly classified national security information as well as sensitive operational and financial data. The need to protect these systems is of paramount concern to the Department and to the Office of Inspector General.

My office has a proactive program to assess the effectiveness of the Department's cyber security strategy. We perform the annual cyber security evaluation required under the Federal Information Security Management Act, commonly referred to as FISMA, and other reviews that focus on potential vulnerabilities in the information technology arena. In addition, our technology crimes unit regularly, and I am pleased to report successfully, investigates malicious attacks on Department information technology resources.

In today's testimony I would like to highlight continuing challenges identified through our work in these areas.

During our 2005 FISMA evaluation, we noted systemic problems that exposed the Department's critical systems to an increased risk of compromise. Specifically, the Department had not yet established a complete inventory of networks, applications, or external interfaces. Many sites had not completed or properly performed certification and accreditation of all their major systems. The Department had not resolved problems with critical security controls such as access authority, segregation of duties, and configuration management. Contingency plans, necessary to ensure that information systems could continue or resume operations in the event of an emergency or malicious intrusion event, had not been completed in certain critical areas. Finally, Department elements did not always report cyber security incidents to law enforcement officials as required.

Similarly, our audit of the Department's 2005 consolidated financial statements identified network vulnerabilities, weaknesses in access controls, and other unclassified systems security shortcomings. In the aggregate, these problems increase the risk of malicious destruction or alteration of data. Further, in many cases, contractors were not required to comply with the full complement of Federal cyber security directives.

In our law enforcement role, my office aggressively pursues those who have attempted to compromise or inflict damage on the Department's computer systems. We have successfully investigated a number of intrusions, working closely with Department of Justice prosecutors and the FBI and in cooperation with external law

enforcement agencies such as New Scotland Yard and the Royal Canadian Mounted Police.

Because of frequent intrusion attempts, it is critical that strong security controls be implemented. Our investigations, however, have revealed problems with the deployment of basic controls such as those related to password administration. In three separate investigations, we determined that Department of Energy systems were compromised after hackers took advantage of password vulnerabilities. In all three cases, individuals pled guilty to criminal charges in connection with their activities. Sentencing included incarceration, probation, and home detention.

We are currently conducting reviews to focus on three key elements of cyber security: the Department's System Certification and Accreditation Process; Cyber and Computer Forensic Analysis Capabilities; and its Security Configuration and Vulnerability Management Program.

As part of our ongoing FISMA evaluation, we also intend to determine if the Department has taken action to prevent compromises similar to those that recently occurred at the Department of Veterans Affairs.

The Department has informed us that, as a result of the concerns raised by our office, it has initiated actions to strengthen its cyber security program. In particular, under the direction of Secretary Bodman and Deputy Secretary Sell, the Department has implemented a number of countermeasures to reduce network vulnerabilities and embarked on a revitalization initiative that will focus high-level management attention on cyber issues. These efforts, if fully and timely implemented, should improve the Department's cyber security posture.

However, let me be very clear, much remains to be done. The Office of Inspector General is committed to fulfilling its responsibility by continuing to conduct a wide range of reviews to identify opportunities for improvement in cyber security and to investigate intrusion attempts on the Department's systems and networks.

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

MR. WHITFIELD. Thank you, Mr. Friedman.

[The prepared statement of Hon. Gregory H. Friedman follows:]

PREPARED STATEMENT OF HON. GREGORY FRIEDMAN, INSPECTOR GENERAL, U.S. DEPARTMENT OF ENERGY

Mr. Chairman and members of the Subcommittee, I am pleased to be here at your request to testify on cyber security issues at the Department of Energy.

The Department of Energy, which spends over $2 billion each year on information technology (IT), has a current inventory of approximately 800 information systems, including up to 115,000 personal computers; many powerful supercomputers; numerous servers; and, a broad array of related peripheral equipment. These systems process operational, financial, and highly classified national security data. The need to protect this data and the related systems is of paramount concern to the Department and to the Office of Inspector General (OIG).

As is widely recognized both in the private and public sectors, the threat of intrusion or damage to information networks and systems continues to grow as cyber-related attacks become more sophisticated. The media regularly carries stories about malicious intrusions and compromises of sensitive data. Within the Department of Energy complex, on a regular basis, hackers attempt to intrude or cause damage to the Department's networks and systems. Cyber security threats of this sort reinforce the need for an aggressive Departmental program of controls and safeguards to protect against any compromise of vital data.

The Office of Inspector General has a proactive program to assess the effectiveness of the Department's cyber security strategy. For the last four years, the OIG has categorized information technology and systems security as one of the Department of Energy's most significant management challenges. This was based on internal control weaknesses identified as part of the Inspector General's regular evaluation of the Department's cyber security program. These reviews include the annual evaluation required under the Federal Information Security Management Act (FISMA) and other cyber security-related reviews focusing on high-risk activities. In addition, the OIG's technology crimes unit, with its highly trained special agents, regularly and successfully investigates malicious attacks on Department systems.

In today's testimony I would like to highlight continuing challenges identified through our work in cyber security. I will outline results from completed activities and criminal investigations, and discuss ongoing review efforts.

2005 FISMA Evaluation

The purpose of the Federal Information Security Management Act of 2002 was to elevate attention to the issue of information technology security within the Federal sector. Under FISMA, each agency is required to develop, document, and implement an agency-wide program to provide security for the information and systems that support core operations. It also requires that agency Inspectors General conduct an annual independent evaluation of their Department's unclassified cyber security program and practices. At the Department, the evaluation is performed in conjunction with our annual Audit of the Department's Financial Statements and leverages testing of information technology controls performed on individual site and Department-wide financial systems.

Last year, as part of this evaluation, we conducted reviews at 27 sites, which, depending upon the location, included examinations of the Department's compliance with information system-related laws and regulations; tests of general and application controls; and, vulnerability and penetration testing. We also incorporated information gathered by and conclusions reached by KPMG, our financial statement contractor; reports issued by the Government Accountability Office; inspection results obtained from the Department's Office of Independent Oversight; and, other internal studies.

Our 2005 review noted systemic cyber security problems that exposed the Department's critical systems to an increased risk of compromise. Specifically:

- The Department had not yet established a complete inventory of information systems; nor, had it identified all of the existing interfaces between internal and external systems and networks. These tasks are critical to planning and implementing protective efforts.

- Many sites had not completed or properly performed certification and accreditation of all their major and general support systems. This process verifies that the Department's systems are secure for operation and enables program officials to address high-risk issues through cost-effective mitigation strategies.
- The Department had not resolved noted problems with critical security controls such as access authority, segregation of duties, and configuration management. These safeguards and controls are designed to protect computer resources from unauthorized modification or loss and to prevent fraudulent activities.
- Contingency plans, necessary to ensure that systems could continue or resume operations in the event of an emergency, disaster, or malicious intrusion event, had not been completed for certain critical systems.
- Department elements did not always report cyber security incidents to law enforcement officials, as required. Failure to report these occurrences jeopardizes the timely investigation and resolution of these matters.

Similarly, our *Audit of the Department of Energy's 2005 Consolidated Financial Statements* (DOE/OAS-FS-06-01, November 2005) noted network vulnerabilities; weaknesses in access controls; and, other security shortcomings in the Department's unclassified computer information systems. These shortcomings increased the risk that malicious destruction, alteration of data, or other unauthorized processing could occur. As a result, "Unclassified Network and Information Systems Security" was designated as a reportable condition. An Information Technology Management Letter, which detailed 25 site-specific vulnerability findings, was issued as part of the 2005 Financial Statement Audit Report.

Criminal Investigations and Internal Control Weaknesses

As part of its law enforcement mission, the OIG aggressively pursues those who have attempted to compromise or inflict damage on the Department's computer systems. In this role, we have successfully investigated a number of intrusions with both national and international connections. We work closely with Department of Justice prosecutors and the Federal Bureau of Investigation in pursuing these matters and have worked on specific cases with external law enforcement agencies such as New Scotland Yard and the Royal Canadian Mounted Police.

Because the Department has to deal with frequent intrusion attempts that could compromise systems, it is critical that strong security controls are implemented and appropriately executed. Our investigations have revealed problems with the deployment of controls in certain areas; for example, we have observed, in past investigations, a number of internal control weaknesses related to poor password administration. In one investigation, we determined that employees of a United States-based computer security company compromised unclassified Department of Energy and other government systems. Company officials were able to gain access to scientific data from a Headquarters system through the use of hacker tools that exploited a password vulnerability. Three individuals pled guilty in connection with those activities.

During another criminal investigation, we determined that two individuals within the United States gained access to an unclassified website belonging to Sandia National Laboratory, part of the Department of Energy's national laboratory network. They were able to gain access by exploiting a default password. These individuals pled guilty and have been sentenced in connection with their activities. In yet another investigation, an individual compromised a network at the Fermi National Laboratory, again by taking advantage of problems with weak password administration. The hacker, who pled guilty to his activities, used the system as his personal storage site to host illegal software –

creating the ability for others to download the intruder's data from the Department's systems.

Ongoing Reviews

As noted previously, the Department invests over $2 billion each year for information technology throughout its complex. It is essential, especially given the size of the resource commitment, that all IT and cyber security initiatives be economic and efficient. To address this concern, we perform focused reviews on information technology-related areas. Over the course of such work, we have identified millions of dollars in potential savings in findings related to enterprise architecture, enterprise licensing, and IT support services.

The OIG is currently conducting comprehensive reviews directed at three key elements of cyber security: the Department's Systems Certification and Accreditation Process; its Cyber and Computer Forensics Analysis Capabilities; and, its Security Configuration and Vulnerability Management Program.

Systems Certification and Accreditation Process

Systems certification and accreditation is an essential step in verifying that the Department's systems are secure for operation. As noted previously, we identified multiple problems with the certification and accreditation process at certain sites; and, as a consequence, we initiated a review to determine whether the Department's systems have been appropriately certified and accredited for operation.

Cyber and Computer Forensics Analysis Capabilities

An ongoing effort is examining whether the Department had formally developed and implemented a unified, effective, and efficient means of analyzing and acting on information related to malicious attacks or intrusions. As part of this audit, we are following up on problems with cyber incident reporting previously identified by the OIG in 2003.

Security Configuration and Vulnerability Management

Building on findings in prior years and on the work already completed by our financial statement auditor, an audit team is examining operating systems and applications. This effort will determine, among other things, whether minimum security configuration standards have been established and implemented at Headquarters and Department field sites.

Status of the 2006 Office of Inspector General FISMA Evaluation

The Office of Inspector General is currently conducting the 2006 evaluation of the Department's Cyber Security Program. This Department-wide effort includes site-level evaluations – consisting of vulnerability and penetration testing and general and application controls testing – at eight sites: the NNSA Service Center in Albuquerque; Los Alamos National Laboratory; Sandia National Laboratories; the Chicago Operations Office; Argonne National Laboratory; the Kansas City Plant; the Y-12 Plant; and the National Energy Technology Laboratory. We are performing follow-up reviews at 12 additional sites. We are also specifically evaluating corrective actions and new initiatives begun this year by the Office of the Chief Information Officer.

As you are no doubt aware the Department of Veterans Affairs (VA) recently experienced the loss of sensitive personal data for millions of Veterans and, apparently, a large number of active duty personnel. This has understandably raised concerns about identity theft and related problems. My colleague, the Inspector General for the VA, has initiated several probes into this matter. As part of our ongoing FISMA evaluation, we intend to determine if the Department has taken action to prevent compromises similar to those which recently occurred at the VA.

Conclusion

The Department has informed us that, as a result of the concerns raised by our office, it has initiated actions to strengthen its cyber security program. In particular, under the direction of Secretary Bodman and Deputy Secretary Sell, the Department has implemented a number of countermeasures to reduce network vulnerabilities and embarked on a revitalization initiative that will focus high-level management attention on cyber issues. These efforts are promising and, if fully implemented, should help improve the Department's cyber security posture. While the Department is moving aggressively in this area, much remains to be done. As the House of Representatives Committee on Government Reform has recognized for the past three years through its ratings of Federal agencies' cyber security programs, significant weaknesses continue to exist at the Department of Energy.

The threat to the Department's systems is constantly evolving as hackers develop new and increasingly sophisticated tools and techniques. The potential for harm is not limited to malicious internet-based attacks, but also includes other efforts by internal users to gain access to resources or information to which they are not entitled. Constant vigilance is required to establish and maintain a defensive posture that is sufficient to prevent or quickly detect problems. The Office of Inspector General is committed to fulfilling its responsibilities by continuing to conduct a wide range of reviews to identify opportunities for improvement and investigate intrusion attempts on the Department's systems and networks.

Mr. Chairman, this concludes my statement and I would be pleased to answer any questions.

MR. WHITFIELD. At this time, Mr. Podonsky, you are recognized for your opening statement of 5 minutes.

MR. PODONSKY. Thank you, Mr. Chairman and members of the committee, for inviting me to testify regarding the status of the Department of Energy's cyber security programs.

Like all Federal agencies, the Department faces a constant challenge to identify, evaluate, and apply cyber security measures that will establish an appropriate protection posture for information and information systems in this ever-changing cyber threat environment.

Both the Secretary and Deputy Secretary have demonstrated exceptionally strong leadership in making cyber security one of the Department's highest priorities. The Department's new CIO is leading a revitalization effort designed to implement needed improvements across the Department's programs and sites.

Before discussing the status of the Department's cyber security, I would like to take a moment and give you a brief overview of my office responsibilities with respect to cyber security.

Within the Office of Independent Oversight, the Office of Cyber Security Evaluation executes one of the most aggressive and sophisticated cyber security corporate oversight programs in the entire Federal government that allows the Department to proactively identify and address weaknesses. The cornerstone of our cyber security oversight is a rigorous penetration testing program that includes announced external and internal penetration testing of DOE networks, unannounced

remote penetration testing or red teaming, which emulates the sophisticated external hacker exploding weak links to the network, and continuous scanning of all DOE Internet protocol addresses to identify vulnerabilities to Internet-based threats.

In addition to this testing, we conduct assessments of key management processes such as risk management, certification and accreditation, and configuration management. While our technical testing provides a good snapshot of the effectiveness of the networks of cyber security posture, the programmatic evaluation of management processes provides an assessment of the strength and direction of the cyber security program.

Results of our independent oversight activities have identified weaknesses that lead us to conclude that the Department's unclassified information assets have been operating at an elevated level of risk for compromise and disruption, given today's threat environment.

The effectiveness of the unclassified cyber security program has varied across the Department and is often dependent on the knowledge and initiative of key network personnel utilizing expert-based approaches. This in some cases has led to a lack of rigorous processes necessary for a solid program foundation.

Our oversight activities, however, have also found that some DOE organizations have developed mature cyber security programs for their own classified computers that include well-constructed security controls. We have seen progress in addressing identified cyber security concerns.

The sharing of lessons learned from our red team testing as well as the high level of focus on cyber security by DOE senior officials has raised the awareness within the DOE cyber community in increased expectations and threats.

In contrast to the unclassified program, our independent oversight activities indicate that the classified cyber program is providing an adequate level of protection.

In response to the independent oversight findings, especially the recent penetration testing that I referred to as the red team testing, the Deputy Secretary directed my office to also lead an effort to develop a comprehensive plan of action to remedy existing management and operational technical weaknesses at the Department's unclassified cyber security program. Our office, together with the Office of the CIO, led a team of departmental cyber security professionals to develop a plan of action and remedy these long-standing weaknesses. These recommendations, issued by the team in what we call the Cyber Security Project Team Summary Report and Plan of Action, represent the consensus of senior representatives from the Office of the CIO, NNSA,

SSA, and others and put us on a path of improving cyber security throughout the Department.

The revitalization efforts the Department has taken on shows many initial steps to upgrade cyber security and improve the posture. Our new CIO has proactively developed a cyber security revitalization plan that includes in its appendix the recommendations from the CSPT. The revitalization plan is an important next step in the difficult process to define a cyber security management and operational framework that can institutionalize yet be responsive to the dynamic world of cyber threats.

The line managers responsible for implementing the technical controls necessary to reduce the risk are taking immediate actions where feasible, but must carefully evaluate a balance for the need for any additional controls with their site-specific mission requirements, threat environment, and resource limitations.

In conclusion, the Office of the CIO and the program offices we believe have laid the necessary groundwork to build a responsive program that will begin to assure that our information and information systems are adequately protected. We have already seen improvements in this area and continue to be cautiously optimistic that historic systemic problems with departmental cyber security processes will be addressed.

Individual sites in both Under Secretaries for ESC and NNSA are working to reevaluate the need for improved security measures based on their mission requirements and accepted risk management principles.

Our office will continue to implement an aggressive schedule of internal and external penetration and performance testing and use the results of those tests to aid the Office of the CIO program offices and site managers in maintaining a protection posture that proactively manages and anticipates new and emerging threats and the use of new technologies by our adversaries.

Mr. Chairman, this concludes my testimony.

MR. WHITFIELD. Thank you very much, Mr. Podonsky.

[The prepared statement of Glenn S. Podonsky follows:]

PREPARED STATEMENT OF GLENN S. PODONSKY, DIRECTOR, OFFICE OF SECURITY AND SAFETY PERFORMANCE ASSESSMENT, U.S. DEPARTMENT OF ENERGY

Summary of Testimony of Glenn S. Podonsky
Director, Office of Security and Safety Performance Assurance
U.S. Department of Energy
Before the
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
U.S. House of Representatives
June 9, 2006

Background

- The Office of Independent Oversight, within the Office of Security and Safety Performance Assurance (SSA), is responsible for conducting independent evaluations of the effectiveness of cyber security policies, programs, and performance throughout the Department of Energy.
- The SSA oversight program evaluates the full range of DOE information systems, including unclassified, classified, and intelligence systems.
- Independent Oversight inspections evaluate both the management and technical aspects of cyber security, with a heavy emphasis on penetration testing. Penetration testing is conducted both internally and from outside DOE networks as part of announced and unannounced inspections.

Current Status of Department of Energy Cyber Security Programs

- Results of our independent oversight activities leading up to and including last fall's red team assessments have identified fundamental weaknesses in both the management processes and operational controls employed to protect the Department's unclassified information systems.
- While some DOE organizations have effective security controls, our overall assessment is that the Department's unclassified information assets have been operating at an elevated level of risk for compromise and disruption given today's threat environment.
- In contrast to the unclassified program, our inspections indicate that the information security program for national security systems is providing an adequate level of protection. A malicious insider represents the greatest threat to DOE's classified information.
- Since last fall, SSA has been working in partnership with the Chief Information Officer and Under Secretaries in an aggressive effort to improve cyber security within DOE. The cyber security revitalization plan is the logical next step in the process of institutionalizing a robust management and operational framework across DOE using the recommendations in the *Cyber Security Project Team Summary Report and Plan of Action*.
- The focus on cyber security by senior Departmental leaders and sharing of lessons learned from red team assessments has clearly raised awareness throughout DOE of the importance of cyber security, possible threat vectors, and increased expectations for performance.
- Numerous security controls have been added or upgraded at DOE Headquarters, the NNSA Service Center, and the National Training Center to strengthen the protection of their respective networks.
- Sites are continuing to evaluate the *Summary Report and Plan of Action* recommendations relative to their information processing mission requirements, threat environment, and competing priorities.

Conclusion

- The Department has made substantive progress in improving cyber security in the past six months. Progress is evident at both the program management and technical implementation levels.
- SSA is guardedly optimistic that the revitalization effort will be effective in fully addressing long-standing weaknesses in the Department's cyber security management processes, but success will require consistent and sustained effort at all management levels.
- SSA will continue to evaluate and report on progress in improving technical security controls through an aggressive cyber security penetration testing program.

Testimony of Glenn S. Podonsky
Director, Office of Security and Safety Performance Assurance
U.S. Department of Energy
Before the
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
U.S. House of Representatives
June 9, 2006

Mr. Chairman and members of the Subcommittee, thank you for inviting me to testify regarding the status of the Department of Energy's cyber security programs and ongoing efforts to revitalize those programs throughout the Department. Both the Secretary and Deputy Secretary recognize the importance of cyber security and have demonstrated exceptionally strong leadership in making cyber security one of the Department's highest priorities. The Department's new Chief Information Officer is leading this revitalization effort which we are guardedly optimistic will result in implementation of needed improvements across the Department's programs and sites.

The Department of Energy (DOE) relies upon an extensive array of information technology and computer resources to accomplish its national security, energy, science, and environmental management missions that range from the desktop computers used by Federal and contractor staff to some of the world's most sophisticated and complex supercomputers. It is of paramount importance that we protect the confidentiality, integrity, and availability of these resources utilizing sound risk management approaches given their critical role in enabling the Department to accomplish its vital missions. The threats to our information systems have never been greater and continue to grow in sophistication and intensity every day. Like all Federal agencies, the Department of Energy faces a constant challenge to identify, evaluate, and apply cyber security measures that will mitigate these threats and establish an appropriate protection posture for our information and information systems in this ever-changing cyber threat environment. Before I discuss the status of the Department's cyber security programs, I would like to provide an

overview of the Office of Security and Safety Performance Assurance's responsibilities, with a particular focus on our activities related to cyber security.

Overview of SSA Activities

As a direct report to the Office of the Secretary, the Office of Security and Safety Performance Assurance (SSA) is responsible for several major functions within the Department. These functions can be divided into two very distinct categories - the independent oversight of security and safety program implementation and responsibility for a wide spectrum of security-related functions including policy, training, security technology deployment, field assistance, classification and declassification, and nuclear material control and accountability. In the area of cyber security, our role is to serve as the independent oversight for the entire Department of Energy. Our Office of Independent Oversight conducts performance-based evaluations of safeguards and security, cyber security, emergency management, and environment, safety and health program implementation throughout the Department. Within this office, the Office of Cyber Security Evaluations executes one of the most aggressive and sophisticated cyber security corporate oversight programs in the Federal government that allows the Department to proactively self-identify and address weaknesses. The cornerstone of our cyber security oversight is a rigorous penetration testing program that is implemented in a variety of ways to achieve multiple objectives. These include:

- announced external and internal penetration testing of Departmental networks conducted in conjunction with announced cyber security inspections that evaluates a broad set of threats and is designed to assess protection boundaries, physical and logical security configurations and controls, access authorizations, and activity monitoring practices;
- unannounced remote penetration testing or "red teaming", which emulates a stealthy, methodical, and sophisticated external attacker attacking weak links in the network and is designed primarily to test intrusion detection and incident response capabilities; and
- Continuous scanning of all Department of Energy internet protocol addresses to identify vulnerabilities to internet-based threats on an ongoing basis.

In conjunction with our penetration testing activities, the Office of Cyber Security Evaluations conducts assessments of key management processes that are essential to an effective cyber

security program such as risk management, certification and accreditation, configuration management, and patch management. While our technical testing provides a good snapshot of the effectiveness of the network's cyber security protection posture, the programmatic evaluation allows an assessment of the direction and sustainability of the cyber security program along with identification of underlying root causes for implementation weaknesses identified through technical testing. The Office of Cyber Security Evaluations applies this same basic approach to assessments of unclassified, classified, and intelligence systems operated by the Department. Other cyber security performance testing conducted by our office includes evaluating the protection posture of telephone modems and identifying vulnerable wireless access points that could potentially provide an unprotected alternate pathway into one of our networks. Pursuant to the Federal Information Security Management Act (FISMA), the Office of Security and Safety Performance Assurance has been designated by the Secretary of Energy to conduct the annual assessment of the Department's information security program for national security systems. The Office of the Inspector General is responsible for conducting the annual evaluation of the Department's information security program for unclassified systems; however, Independent Oversight provides significant input in the form of our inspection results. We have an excellent working relationship with the Office of the Inspector General and coordinate extensively to eliminate any duplication of effort.

Current Status of Department of Energy Cyber Security Programs

Results of our independent oversight activities leading up to and including our recent red team assessments this past fall have identified fundamental weaknesses in both the management processes and operational controls employed to protect the confidentiality, integrity, and availability of the Department's unclassified information and information systems. While the perimeters of our sensitive unclassified networks are relatively well controlled and monitored, internal Departmental networks were found in many cases to have unpatched and/or unrecognized vulnerabilities, lack of segmentation or barriers, common local administrator passwords, poorly controlled inter-connections with other networks, and insufficient intrusion detection mechanisms. As demonstrated in the recent red team assessments, a malicious insider or sophisticated adversary that has managed to penetrate the network could take advantage of

these types of weaknesses to gain broad access and control over information technology resources. As a result, our overall assessment is that the Department's unclassified information assets have been operating at an elevated level of risk for compromise and disruption given today's threat environment.

At the most basic level, the Department's unclassified information systems suffer from a lack of defense in depth. It is no longer acceptable or prudent to rely on a single layer of protection at the perimeter of a network to ensure that the information contained therein or functions performed are protected from unauthorized access, disruption, or manipulation. Further, the technical implementation weaknesses we have observed are symptoms of inadequate management processes that are essential to an effective cyber security program such as configuration management, patch management, asset management, risk management, and vulnerability scanning. We have routinely identified weak certification and accreditation processes as an underlying root cause of many of the problems identified above.

The effectiveness of the Department's unclassified cyber security programs has been highly dependent on the knowledge and initiative of key network personnel utilizing "expert-based" approaches. This, in some cases, led to a lack of rigorous and repeatable processes that are necessary to form a solid program foundation. In addition, line managers have not been sufficiently involved to ensure the adequacy of controls and managing risk. As a result, the effectiveness of unclassified cyber security programs has been highly variable across DOE organizations. Of concern, Departmental cyber security management processes have been insufficient in the past to drive needed improvements throughout the Department.

Oversight activities have found that some DOE organizations have developed mature cyber security programs for their unclassified computers that include well constructed defense in depth security controls. It is clear that the sharing of lessons learned from the Red Team as well as the high level of focus on cyber security by senior Departmental leaders has clearly raised the awareness within the DOE cyber security community of increased expectations and threats. We have seen some initial progress in addressing identified cyber security concerns. For example, at DOE Headquarters, common local administrator passwords for system administrators have been

eliminated and access control converted to two factor authentication. Virtual local area networks have been deployed on the Headquarters network to provide a greater degree of network segmentation. Host-based intrusion detection has also been added to the Headquarters network as part of adding additional defense in depth. Additionally, the Department's Chief Information Officer is leading the recovery effort to respond to the security weaknesses at DOE Headquarters and the National Nuclear Security Administration (NNSA) Service Center. Additional plans have been developed to more fully evaluate and mitigate cyber security risks at DOE Headquarters through a broad modernization effort. While Independent Oversight has not yet assessed and validated the effectiveness of these new measures on the DOE Headquarters network through penetration testing, we believe that these represent positive steps.

In contrast to the unclassified program, our independent oversight activities indicate that the information security program for national security systems is providing an adequate level of protection. Established security controls have been found to be generally consistent with DOE's longstanding requirements for these systems. During Independent Oversight inspections over the past year, improvements were noted in a number of areas related to both technical security performance and site management practices. However, the Department faces continuing challenges in resolving longstanding weaknesses in policies governing the management of national security systems, continuing programmatic deficiencies, and adherence to some FISMA requirements. As a result, malicious insiders continue to present the largest threat to DOE's classified information.

Cyber Security Assistance Activities

In response to independent oversight findings, the results of other external evaluations, and especially recent penetration testing performance, the Deputy Secretary directed us to step out of our normal oversight role in order to lead an effort to develop a comprehensive plan of action to remedy existing management, operational, and technical weaknesses in the DOE unclassified cyber security program. To execute the Deputy Secretary's directive, the Office of Security and Safety Performance Assurance, together with the Office of the Chief Information Officer, led a team of Departmental cyber security professionals which developed a plan of action to remedy

long-standing weaknesses in the unclassified cyber security program. The recommendations issued by the team in the *Cyber Security Project Team Summary Report and Plan of Action* represent the consensus of senior representatives from the Office of the Chief Information Officer; National Nuclear Security Administration; Under Secretary for Energy, Science, and Environment (ESE); SSA; and others on a path forward for improving cyber security throughout the Department. Normally, it would have been preferable for the Department to focus first on establishing a robust management structure and governance process that would subsequently drive improvement in operations and security at the system administrator and computer user levels. However, the team felt it was important for sites to begin improving their protection posture immediately through prudent measures and give the management processes a chance to catch up before ultimately driving improvements through risk based decision-making. As a result, a set of programmatic and technical recommendations for improving cyber security throughout the Department were provided. It should be recognized that these recommendations are not mandatory but were offered as suggestions for each DOE program and site to assess for applicability and to make determinations based on cost, benefit, and feasibility of implementation.

As part of another initiative to help improve the Department's cyber security protection posture, the Office of Cyber Security Evaluations is partnering with the Office of Science in conducting site assistance visits at all Office of Science field sites to help them identify vulnerabilities and implement improved security controls and processes. Since last summer, ten site assistance visits have been completed; five more are scheduled to be completed this year. Other site assistance visits have been conducted or are planned with the Office of Environmental Management, the Office of Energy Efficiency and Renewable Energy, and the Power Marketing Administrations. We have also worked closely with the Office of the Chief Information Officer, the National Nuclear Security Administration's Service Center, and the Department's National Training Center to significantly strengthen their cyber security defenses by implementing more robust security controls following red team assessments conducted on their networks. We have shared the results of our red team assessments extensively through a variety of communications forums.

Revitalization Efforts

Recently, the Department has taken many important initial steps to upgrade its cyber security protection posture. For example, our new Chief Information Officer has proactively developed a cyber security revitalization plan that encompasses many of the recommendations from the *Cyber Security Project Team Summary Report and Plan of Action.* The revitalization plan is an appropriate next step in the difficult process to define a cyber security management and operational framework that can be institutionalized yet responsive to the dynamic world of cyber threats and counteracting security measures. The line managers who are responsible for implementing the technical controls necessary to reduce risk are taking immediate actions where feasible, but also must carefully evaluate and balance the need for any additional controls with their site-specific information processing mission requirements, threat environment, and resource limitations.

The Office of Security and Safety Performance Assurance continues to monitor progress in improving the Department's cyber security programs on a daily basis. We actively participate in and routinely provide feedback to the Office of the Chief Information Officer and other line managers through the Department's Cyber Security Executive Steering Committee and Cyber Security Working Group. We continue to conduct critical reviews of proposed changes in Departmental cyber security policies and guidance with an eye toward the likelihood that those policies will result in the desired level of protection when applied to the wide spectrum of information management and processing needs. We are reviewing site-specific progress in evaluating and implementing the recommendations of the cyber security project team and providing feedback to cognizant line managers in this regard as an integral part of our independent oversight inspections. The most important measure of progress, however, will be the degree to which the Department's information and information systems can prevent an intrusion or can rapidly detect and respond to an intrusion such that the damage to a system can be readily recognized, contained, and mitigated. A realistic evaluation of these capabilities can only truly be gained from the types of performance testing that are conducted as part of our independent oversight. To that end, we are continually developing new penetration testing tools

and attack techniques to keep pace with advances in technology and new approaches to exploiting human behavior.

Conclusion

The Department is making progress in improving its cyber security programs. The Office of the Chief Information Officer and program offices have laid the necessary groundwork upon which to build a robust and responsive program that assures that our information and information systems are adequately protected. We have already seen improvements in this area under the new Chief Information Officer's leadership and continue to be cautiously optimistic that historic, systemic problems with Departmental cyber security management processes will be addressed. Individual sites and both Under Secretarys for ESE and NNSA are working to reevaluate the need for improved security measures based on their mission requirements and accepted risk management principles. Our office will continue to implement an aggressive schedule of internal and external penetration and performance testing and use the results of those tests to aid the Office of the Chief Information Officer, program offices, and site managers in maintaining a protection posture that proactively manages and anticipates new and emerging threats and the use of new technologies by our adversaries. Thank you. This concludes my testimony.

8

MR. WHITFIELD. I notice that in your testimony you said there was an elevated level of risk for compromise on this unclassified material. That's basically your statement regarding the DOE system at this time?

MR. PODONSKY. Yes, sir. That was based upon our red team effort. Since that red team effort, there have been corrective actions that are under way, but, nevertheless, we still have serious concerns.

MR. WHITFIELD. Now I'm assuming that there are many hackers around the world that would have the expertise and sophistication of your red team, is that correct?

MR. PODONSKY. Yes, sir. Our red team, many of whom sit behind me in this hearing room, are really quite technically competent in what they do. However, we are aware that there are others that are equally as competent and perhaps even more so.

MR. WHITFIELD. So not casting any aspersions on their expertise, there are a lot of other people out there that would be as competent as they are.

MR. PODONSKY. Yes, sir, I would say that's an accurate statement.

MR. WHITFIELD. On April 15th, 2001, we had a hearing of this subcommittee, and your staff demonstrated at that time cyber penetration techniques that penetrated a single DOE computer and from that computer you gained complete and utter control over the entire system.

Now I understand that during a recent November 2005 red team network penetration test, you again successfully gained control over a DOE site network; and from there your team used network interconnections to gain control over the computer systems at several other DOE sites. Is that true?

MR. PODONSKY. That is true. You are describing our red team effort.

MR. WHITFIELD. Now based on the degree of access privileges your red team obtained during this cyber security penetration test last fall, would you describe that they had utter control over the system?

MR. PODONSKY. What the red team was able to demonstrate after a very long and protracted test is that we had access to sensitive data, which could be including financial or personal data. We could have had access to have the ability to impersonate or monitor departmental executives. We had the ability to impact the availability of integrity of computer-serving business functions. We had the ability to launch aggressive denial service attacks.

We basically--in the parlance of cyber security, we had domain control.

MR. WHITFIELD. You had domain control.

How would you gauge DOE's overall efforts with respect to cyber security over the 5 years since the subcommittee's April 2001 hearing?

MR. PODONSKY. Mr. Chairman, it is easy for us to say the following, and that is the Department is moving far too slow to our liking. But we are not the ones who have to fix the problems, so we are out there identifying the problems.

But given today's emerging threats that are continuous, we feel that, since the 2001 hearing, that while there are a lot of steps that the

Department is taking and is currently taking, including in response to our most recent red team, we do think that there is a sense of urgency that must be represented. As the Deputy Secretary and the Secretary, and I know the two Unders feel, that we need to keep on moving, and I believe the CIO feels that way as well.

MR. WHITFIELD. In your November 2005 report, you noted that previously secretarial-led initiatives launched in 2004 and 2005 to improve DOE cyber security posture had been largely unsuccessful in effecting needed improvements. Is that still your view on that?

MR. PODONSKY. It is a varied success story. There are different sites that are being more aggressive, and I said--and I would like to iterate the point--we're guardedly optimistic that the new CIO will be much more aggressive in working together with the line offices and the under secretaries to fix the problems that have been identified.

MR. WHITFIELD. So, as you said, your responsibility is to exploit these weaknesses and make them known to the CIO and the Secretary and others at the Department of Energy.

MR. PODONSKY. That's part of our responsibilities, yes, sir.

MR. WHITFIELD. It's their responsibility to make the network more secure so that your red team and others cannot infiltrate.

MR. PODONSKY. That's correct, sir.

MR. WHITFIELD. Now when you do a report, you certainly give that report to the Secretary, the CIO, and others, I'm assuming. Do you all generally sit down and go over in some detail about exactly how you were successful?

MR. PODONSKY. Yes, sir. We have a very good partnership with the CIO office in working together in finding ways to solve some of the problems we are finding, but we what we call validate our report findings so we make sure that what we find is technically accurate, and when we report that forward to the various managers we want to make sure that--we are not there to fix the problems but we at least work with them to identify ways that they might pursue.

MR. WHITFIELD. Mr. Friedman, in your testimony, you stated that the Department did not always report cyber security incidents to law enforcement officials as required; and your staff has informed us that DOE has failed to report as many as 50 percent of all reportable cyber attacks to the appropriate authorities. Can you explain why DOE has failed to report these incidents and why it is important that these incidents be reported?

MR. FRIEDMAN. Mr. Chairman, let me take the second part of your question first.

The reporting of these incidents, number one, gives law enforcement the opportunity to track down those who are responsible for the

malicious attack, bring them to justice, and set an example for others, which hopefully leads to prevention of individuals in the future attempting to do the same thing.

Number two, it allows for trends analysis.

Number three, it allows us to determine whether similar sorts of intrusions or attempts at destruction are occurring at other locations so that we can assist the Department and make recommendations for corrective actions, patches, fixes to prevent that from happening. So we think it's extremely important that these issues be reported and be reported promptly.

In terms of why it's not happening, tragically, Mr. Chairman, I don't have a good answer. I wish I did. We ask, we probe, we try to find out. I think to some degree it is individuals who think that they can fix it internally; therefore, there is no need to bring in an outsider; people who may not fully comprehend the gravity of the situation. But I really don't have a satisfactory answer to your question.

MR. WHITFIELD. That's a rather large percentage, 50 percent.

MR. FRIEDMAN. That's correct.

MR. WHITFIELD. That is one of the disturbing things about an agency as big as DOE. I mean, the Secretary may not even be aware of that. Hopefully, the Chief Information Officer would be aware of that and take some steps to deal with it. That is another issue.

I'm sorry?

MR. FRIEDMAN. I apologize, Mr. Chairman. We have reported that issue on several occasions. It is a repeat finding. So it's not as though this is a one-time finding. This has been a pattern that we have seen. Now it's gotten better in our view, but it's still a problem.

MR. WHITFIELD. That's another thing that's so disturbing to us from this perspective about this breach regarding these personnel files. Although we don't have all the facts about this, the fact that it was known to someone in the Department 8 months ago and the Secretary was unaware of it until maybe a day ago or maybe today, the CIO was not aware of it. It's unbelievable that 1,500 personnel files could be compromised with Social Security numbers, and the impact that that could have on those individuals is quite disturbing. I am sure you would agree with that.

MR. FRIEDMAN. I would.

MR. WHITFIELD. I would ask this to Mr. Friedman and Mr. Podonsky. In the written testimony of Under Secretary Garman, he states that, "While we are not yet where we need to be, I believe we are far better off than we were a year ago." I would just ask you, do you agree with that statement or do you have enough information to disagree with it?

MR. FRIEDMAN. Well, let me say I think there certainly have been improvements. The number of findings we have had in the 2005 FISMA report are less than we had 4 years ago. So there certainly have been improvements.

Your colleagues on the House Government Reform Committee have given the Department an F in cyber security in this arena as a result of their evaluation. So I think that there is a great deal more to be done as I testified.

MR. WHITFIELD. I mean, there is no excuse for a Department having an F in cyber security.

Mr. Podonsky.

MR. PODONSKY. Mr. Chairman, I would answer your question in terms of the red team. If we were to launch the red team today, could we have the same access that we had during the last year? And I would say that we could gain access but we would not be able to have domain control.

So there have been some very distinguished changes that have come about, and that is important. As long as you have any system connected to the Internet, we are going to have vulnerabilities. Not just our agency but the entire Federal government, legislative arm included, needs to be very mindful of the capabilities that are out there and the availability, that people can come into our networks without our knowledge and pretty much, if we don't have the controls in place, have access to our records.

The Department from my point of view is that it has gotten better, but, as Mr. Friedman has stated and I have stated, there's a long way to go.

MR. WHITFIELD. Thank you.

At this time, I recognize the gentleman from Michigan.

MR. STUPAK. Thank you, Mr. Chairman.

Mr. Podonsky, you said you had domain control when you did your red team exercise in November of 2005. Would that domain control allow you to go anywhere you wanted to go?

MR. PODONSKY. At the time that we were in the network, the answer to that is yes, within the unclassified network. That meant that we were able to get passwords, that meant that we were able to go from one account to another account. Perhaps if we stayed longer--and this is a supposition on our part--we make it a policy not to damage anything when we go in.

MR. STUPAK. If it's unclassified, in fact you have passwords and others, what's sensitive about it, then?

MR. PODONSKY. You potentially have financial records, personnel files. Anything that is contained in the unclassified arena.

MR. STUPAK. Did your red team in November 2005 try to go into the classified areas?

MR. PODONSKY. We did, and we were not successful.

MR. STUPAK. You indicated that you thought that DOE was still moving too slowly in cyber security, in response to an answer to the Chairman. What in your estimation or your group's estimation would make DOE move faster in this area. What will it take? Where is it lacking?

MR. PODONSKY. As I stated in the other question, it's easy to be on the side of criticizing. I asked my cyber colleagues what would it take to fix this, and we talk about segmentation, segmentation of systems. We talk about encryption, encryption of all the data. We talk about putting more tools out there for changing passwords on a more frequent basis; tools out there to monitor the perimeter so that we can make sure that we at least know when somebody is coming in. Even though we can't stop them, we can at least know they are in the system.

We believe the CIO is starting to move in that direction. When I talk about impatience for the solution, it is because we have been inspecting the Department for a number of years and we have been seeing a lot of the repeat findings, as Mr. Friedman also talks about in his office. Some of those steps are some of the steps we would like to see done more rapidly.

MR. STUPAK. In response to the Chairman, you said your job is not to fix the problem but to make suggestions or give them ideas on how they can be fixed, like monitor and change pass codes more often. Is that advice ignored?

MR. PODONSKY. I think a better characterization of the office is that we are like the internal GAO. We identify the problems, make recommendations. But clearly the program offices have to prioritize their mission and their functions on how they are going to accept those recommendations. We don't personally or professionally believe that we have been ignored; it's just it hasn't always been the highest of priorities until the most recent 2 years.

MR. STUPAK. Doesn't seem like a priority until something occurs. I can't help think out loud, and I think my colleagues would join me; we learned about the latest breach recently, and that's probably only because we had this hearing. It seems like action occurs only when this Committee on Oversight and Investigations actually has a hearing and is willing to start pushing on some of these issues. That's not a question, so let me ask you a question.

Is there anything in the unclassified network that you were in in November of 2005 that could somehow impact national security? You

say you were bouncing around in the unclassified area, but by having domain control could you impact national security?

MR. PODONSKY. I think that hypothetically that anything is possible once you start delving into the systems. For example, there may in fact be some information that is not yet classified, then later becomes classified, so that you always have that possibility.

MR. STUPAK. One of the things you could do, I thought you said, was denial of service. That could impact national security, could it not?

MR. PODONSKY. Yes, sir.

MR. STUPAK. Especially when we're dealing with cyber security.

Mr. Friedman, and maybe Mr. Podonsky, the cyber security, most employees at DOE--or most, I should say, of DOE's budget is for private contractors. They probably have more private contractors than any other Department in the Government. Cyber security, is that left mostly to private contractors?

MR. FRIEDMAN. To put some context, Mr. Stupak, as best we can determine the numbers, the Department spends about $140 million a year on cyber security, and it is quite clear that the vast majority of the money is spent by contractors; 85 to 90 percent of the Department's budget is spent by contractors. So as a consequence, although it's slightly disproportionate when it comes to cyber security, that rule of thumb applies reasonably well in this context.

MR. STUPAK. Here are the points I'm having problems with. I have been on this committee for 10 years and it seems like, unfortunately, with DOE we're always here talking about things we would rather not be talking about.

What control do you really have, or even this committee, over contract employees? You're a government agency, contract employees working for us. We really can't, unless you fire this individual or hold that individual accountable. How do you bring accountability, then, in your cyber security if 80 to 90 percent of it is contracted out? How do you get the things done that have to be done like you said, no contract with law enforcement, 50 percent still not being reported. Where does the accountability come in, then, in a system that is, in my estimation, sort of fragmented?

MR. FRIEDMAN. As I think the Chairman alluded to in his opening statement, I think it was the Chairman, this is an incredibly complex agency with a lot of stovepipes, and those have to be broken down so that the policy is clear; it is communicated clearly to the Federal officials and communicated clearly to contractors as well.

One of the points I indicated in my testimony and we've reported on is the fact that there is not a complete flow-down of all the Federal

requirements to the contractors in their current contracts. We believe that is a part of the problem.

But to answer your fundamental question, Mr. Stupak, it seems to me that contractor accountability means truly holding their feet to the fire, and that means having meaningful reductions in their award fees if there are problems; and ultimately, if they are not corrected, not continuing their service to the Department of Energy.

I think until tough action is taken and the action is manifest to the contractors as a result of a lack of commitment to cyber security, it seems to me that there will not be significant improvement in that regard.

MR. STUPAK. In the position that you have been in for some time now, and before this committee many times, have you seen that accountability, have you seen holding their feet to the fire, have you seen contracts be terminated? I mean, I sit here and I think of Los Alamos and how many times I have been through that situation. We re-awarded the contract to the same folks that have been unaccountable for so long before this committee.

MR. FRIEDMAN. In part it seems to me it takes commitment on the part of the Secretary and Deputy Secretary. And I don't mean to denigrate any of their predecessors, but it's quite obvious that Secretary Bodman and Deputy Secretary Clay Sell are invested in this issue; and it seems to me the tone at the top with regard to cyber security is extremely important. They set the agenda, and if they pursue the course that they have initiated, it seems to me that we will see a meaningful difference.

MR. STUPAK. Meaningful difference we haven't seen yet. That's what I'm trying to get at.

Mr. Podonsky, since you mentioned the Deputy Secretary, that you were directed by the Deputy Secretary to do more work in this area, you said--I think it's on page 5 of your testimony--who is that Deputy Secretary?

MR. PODONSKY. Deputy Secretary Sell.

MR. STUPAK. I have no further questions at this time.

MR. WHITFIELD. Thank you, Mr. Stupak.

At this time I recognize Dr. Burgess of Texas for 10 minutes.

MR. BURGESS. Thank you, Mr. Chairman.

Seems like we are hearing all too often: Veterans Administration lost data on 27 million veterans, the IRS lost data on 291 employees. These are emerging types of threats that are occurring. And while, Mr. Podonsky, I respect the cleverness and the clever minds that you have working for you on the red team, there also seem to be nimble, clever minds working on the other side as well, so it's a constant battle, struggle, to keep up with what the other side is able to produce.

What role does the imposition of encryption software play in all of these--in a general form in all of these things that we have heard about in recent weeks about theft of sensitive computer data, not just the Department of Energy but throughout the various Federal agencies?

MR. PODONSKY. From our perspective, the encryption of data would make the loss of information virtually less of a concern. It is an issue that Mr. Pyke, our current CIO's predecessor two CIOs back, had introduced.

Again, as I said in previous questions I have answered today, it's easy for us to say I don't know what the cost would be. But from our way of thinking, the cost can't be as high as the loss of data.

MR. BURGESS. That was going to be my next question. You mentioned sequestration and encryption. How expensive are these technologies to put into place? I guess you have already answered that. You don't know.

MR. PODONSKY. I don't know, but I would iterate the point it can't be more expensive than the loss of the data that we are talking about here.

MR. BURGESS. I have a strong notion that you are correct and I hope this committee explores that to some degree. Apart from the expense, or if the expense could be modified or met, would you feel that it would be the position of the Department of Energy to rapidly deploy this type of protection?

MR. PODONSKY. That would be up to the senior managers, the two Unders and CIO, but that would be our recommendation.

MR. BURGESS. Up to the managers and the two Under Secretaries?

MR. PODONSKY. Actually the three Under Secretaries now, as well as the CIO.

MR. BURGESS. Mr. Friedman, do you have any thoughts about encryption software and its implementation and its cost?

MR. FRIEDMAN. We do. We don't have a benchmark but it's not quite as costly as we thought it might have been. As a matter of fact, in response to the problem at the Department of Veterans Affairs, as auditors, inspectors, and investigators, we travel extensively. We have laptops, we're all over in the Department of Energy complex.

We have a policy in which we, number one, substantially control the information that our auditors, inspectors, and investigators can carry with them. Number two, when they leave the DOE complex, the information that they carry with them, regardless of what form, either has to be in a locked box, safe, or equivalent, or must be encrypted.

So we are moving on that internally, and I have shared the policy and procedures that we've implemented with the Department CIO.

MR. BURGESS. Does technology exist so that if a laptop is stolen and they log on to the Internet, that its location can be identified or the hard drive could be destroyed?

MR. FRIEDMAN. I am not expert enough, Mr. Burgess, to give you a good answer on that, but I will tell you we have experienced similar situations, stolen or lost laptops in the Department of Energy over time. So the suggestion--

MR. BURGESS. We have had hearings on that.

MR. FRIEDMAN. So, the suggestion you are making is not without merit. I don't know technically whether it's possible. There are others who might have to answer that question.

MR. BURGESS. Mr. Podonsky.

MR. PODONSKY. My staff was whispering in my ear saying you could probably find it, and the technology is out there.

MR. BURGESS. Let me ask you a question about sequestration because I'm not familiar with that at all; sequestration meaning within the vast domain of unclassified data on the Department of Energy site to keep people from going from one area to another?

MR. PODONSKY. You compartmentalize. You compartmentalize one group from another. I'm not saying this is the way it is, but just for illustrative purposes, if you have science labs that want to talk to one another, well, have them have a network where they can just talk to each other and not bring their network into the overall DOE domain, as you will, because then if they are talking to each other and they get compromised, then they might have an entry into other parts of the Department.

So the more separation you can make among systems, we think you are going to have a greater security and prevention of people just roaming through your network, and that's an overstatement of roaming through, but that's going back to what we felt we were doing during the red team.

MR. BURGESS. It is frustrating to be here on the dawn of the Information Age, where so much power is available to us from information, and have to put up these barriers from our scientists. I know, for example, the sequencing of the human genome would never have been possible without the Internet, with scientists talking rapidly across the Internet, and now that--perhaps that scientific inquiry may be stifled because of having to compartmentalize for security reasons. Just a personal note: It's extremely frustrating.

We had a hearing or markup yesterday on security in medical records and the irony of wanting to expand the HIPAA protections on one hand because of what happened at the VA, and, on the other hand, wanting to keep the data available to researchers at the University of Madison. It's

extremely frustrating, and I hope the bright minds behind you on the red team can figure out ways to keep the bad guys out but yet let our scientists continue to communicate as they need to.

MR. FRIEDMAN. You make a very good point. I mean, in the role that I play, of course, efficiency and effectiveness of Department operations are of paramount concern. Striking a balance between appropriate levels of security and cyber security and yet not impeding the operations of the Department is a very significant conundrum that we face every day, and it is going to take some really bright minds to figure out a way of doing both. I think that is ultimately where we need to be. You make a very good point.

MR. BURGESS. Thank you. On sequestration, encryption, we are already spending $140 million a year, but things like using the security patches provided by software vendors, changing passwords, that is pretty low tech and pretty inexpensive. I understand those simple procedures weren't always followed.

MR. FRIEDMAN. As I indicated in my testimony, I cite three investigations where the individuals involved were incarcerated and pled guilty to the charges, in which password vulnerabilities in each of the cases were the approximate cause or set up an environment in which the malicious attempts could occur.

MR. BURGESS. Mr. Podonsky, you testified in response to a question by the Chairman that your red team now could still gain access but not domain control, whereas a year ago domain control was a possibility, for people to come into the networks without your knowledge.

Can we, sitting on the committee, be completely satisfied that domain control is something that could not be gained by either the red team or the bad guys seeking access into our systems?

MR. PODONSKY. No. I think the only comfort that all of us can have as Americans is that we continue to put up more barriers to make it more difficult. But the more sophisticated the hackers become the more challenging it is for us. So when I answered that question it was based on our capabilities right now plus what we know that the CIO and the cyber security community are doing. It would be much more difficult for us to do that. But since this is a continuously evolving technology I don't think that we can make a definitive statement that it could not happen again.

MR. BURGESS. In the limited time I have left here--this is an observation. We are in the 21st century, but I can remember 10 years ago or more a very popular singer was shot down in Corpus Christi, Texas, and taken to the hospital. People on the hospital staff who did not have a direct responsibility for that patient's care who accessed that patient's data were in fact dismissed from the hospital staff. They were fired.

This is 10 years before HIPAA. So even back in the early '90s we had the systems in place in that hospital--at least I remember reading the news reports--that could identify and locate those individuals. It's just striking to me that we sit here now with all of the advances that have been made in computer technology and we don't even seem as sophisticated as that small hospital in Corpus Cristi, Texas, 10 or 12 years ago. Is that a valid observation?

My time is up, Mr. Chairman. I'll yield back.

MR. WHITFIELD. Thank you, Dr. Burgess.

At this time, I recognize the full committee Chairman for 10 minutes.

CHAIRMAN BARTON. I want to thank Ms. DeGette so I can go out of order. I have got to go give a briefing in about 10 minutes. I appreciate her consideration.

Mr. Podonsky, who do you report to at the Department of Energy?

MR. PODONSKY. My office and I report to the Deputy Secretary.

CHAIRMAN BARTON. And he reports to the Secretary of Energy.

Does your office have any authority or oversight over the National Nuclear Security Administration.

MR. PODONSKY. We do conduct oversight within the NNSA, yes.

CHAIRMAN BARTON. You conduct oversight.

MR. PODONSKY. Oversight of environment, safety, health, safeguard security --

CHAIRMAN BARTON. What does that mean, you "conduct oversight?"

MR. PODONSKY. We conduct inspections of the operational sites within the NNSA.

CHAIRMAN BARTON. And, Mr. Friedman, as Inspector General, you have oversight within your purvey over the entire Department; and that would also include the National Nuclear Security Administration, would it not?

MR. FRIEDMAN. That's correct, Mr. Chairman.

CHAIRMAN BARTON. I am going to ask you some questions, Mr. Podonsky. I'm not an expert on what's classified and what's not, so if I ask you something that requires an answer that's classified, you just say so.

But my understanding is that, as Director of the Office of Security and Safety Performance Assessment, you oversee the implementation of certain exercises that test the security systems of the Department, is that correct?

MR. PODONSKY. Yes, sir. We actually conduct performance testing and physical security as well as in cyber security.

CHAIRMAN BARTON. And I am told that in one of those performance assessment tests, your team was able to penetrate some of the security systems of the Department, is that correct?

MR. PODONSKY. We have had that success in our performance testing on numerous occasions.

With specifics to this hearing, we had long, protracted red teaming tests where we were emulating the same as a hacker would do; and we penetrated throughout the national training center in Albuquerque and the service center there.

CHAIRMAN BARTON. I am also led to believe that when that red team was successful that those results were reported to the appropriate officials in the Department. That included the Secretary and the Deputy Secretary, is that correct?

MR. PODONSKY. Yes, sir.

CHAIRMAN BARTON. Now I am also told that, after that report, there was a discovery that the security system had been breached for real, is that correct?

MR. PODONSKY. Yes, sir. And that we would be better off to go in more detail in a closed session.

CHAIRMAN BARTON. But it's not classified that there was a real breach.

MR. PODONSKY. No, sir.

CHAIRMAN BARTON. Okay. Now who should have been told of that and when should they have been told and who was responsible for the telling?

MR. PODONSKY. Relative to the information sharing, the Secretary, the Deputy Secretary, the Administrators for both ESE and NNSA should have been told immediately.

CHAIRMAN BARTON. Immediately.

MR. PODONSKY. Immediately.

CHAIRMAN BARTON. The Secretary of Energy should have been told immediately.

MR. PODONSKY. Absolutely.

CHAIRMAN BARTON. What would the penalty be or should the penalty be if the Secretary were not told immediately of such a breach of security?

MR. PODONSKY. I can't speak on behalf of the Secretary, but, were I in that position, I would be looking for accountability for the individuals that didn't tell me.

CHAIRMAN BARTON. All right. That's all the questions I have at this point in time. Thank you, Mr. Chairman.

MR. WHITFIELD. At this time, I'll recognize Ms. DeGette of Colorado.

Ms. DeGette. Thank you very much, Mr. Chairman.

Like the full committee Chairman, I am looking forward to probing some of these issues, Mr. Podonsky, more in depth in executive session. So let me just ask a few questions of my own.

Does the DOE have its own firewalls?

MR. PODONSKY. Yes, ma'am, it does.

Ms. DeGette. Are those firewalls sufficient to protect DOE data from hackers and other breaches?

MR. PODONSKY. In many cases the answer is yes. When we did our penetration testing, we used the weakness of the human element. Any time you have people involved, you have different ways that you can penetrate, whether it be through attachments to e-mail or whether it's through the way we did it, with using a disk that we mailed through the U.S. mail. And once you get inside, because somebody was not aware that they were exposing the Department vulnerability by clicking on to something, then you have let somebody through the firewall but you didn't go directly through the perimeter itself.

Ms. DeGette. What kinds of precautions can be put in place, in addition to what we have now, aside from beefing up the firewalls to stop the kind of breaches you're testifying about?

MR. PODONSKY. A major effort which is currently under way by the CIO's office, Tom Pyke, is making everybody aware of the vulnerabilities that exist out there. And that may seem very simplistic, but it really isn't because people sitting at their own desktop sometimes get a false sense of security, not knowing that they are potentially exposed when they open up e-mail. So awareness is a very big part.

Ms. DeGette. That's all well and good, and I am very supportive of it, but, of course, that relies then on human nature to protect against these breaches. Are there any additional technological precautions that we can put in place to protect against people going around in the ways that you have described?

MR. PODONSKY. Yes, ma'am. Earlier, before you came in, I talked about doing encryption of information throughout so that if information was obtained, then it would be protected by the fact that it was encrypted. We talked about segmentation, putting people into different networks so that not everybody is connected to one another. There are tools out there also that routinely change passwords so that people can't just break a password and have access to your files. So there's a lot of technology out there that could be a employed.

Ms. DeGette. Is it being applied?

MR. PODONSKY. In some instances, it is starting to be applied.

Ms. DeGette. Do you think it could be applied more aggressively?

MR. PODONSKY. I answered earlier to your colleagues.

Ms. DeGette. I am sorry. I came in late.

MR. PODONSKY. Because I am repeating myself. I am just--the answer is, for us who do not have to implement the fixes, nothing is going fast enough. So it is easy for us to make those statements. But, yes, ma'am, we believe it could be more aggressive; and we are optimistic that the Secretary and the Deputy Secretary and the Under Secretary and the CIO are looking to be more aggressive in this area.

Ms. DeGette. Mr. Friedman, you noted in your last--I apologize if I am being redundant again, but you noted in your last assessment of DOE's cyber security program you found systemic problems that exposed the Department's critical systems to increased risk of compromise. Which systemic failures troubled you and why?

MR. FRIEDMAN. Firewall issues, incomplete inventory of computers and computer systems and networks, inadequate certification and accreditation processes--all of which are extremely important in creating the safest environment possible. Password authorization problems. Some very basic things.

Ms. DeGette. Why did those failures trouble you?

MR. FRIEDMAN. Well, they led us to conclude that the overall, overarching Department of Energy structure in cyber security is riskier than is satisfactory.

Ms. DeGette. And without going into classified information, would you say some of those problems that you identified led to the breaches that we're going to be talking about in a few minutes in Executive Session?

MR. FRIEDMAN. I would prefer not to answer that question in this environment, if you don't mind.

Ms. DeGette. Mr. Chairman, I yield back the balance of my time.

MR. WHITFIELD. Thank you, Ms. DeGette.

At this time, the gentleman from Washington, Mr. Inslee, is recognized for 10 minutes.

MR. INSLEE. Thank you.

Just looking at some of the history that's gone on here, I just wondered from a budgetary standpoint what has gone on in the last 2 years with DOE in response to these identified difficulties that have been experienced. We've seen penetration by this testing system. We've seen identification by DOE of the need to respond to some of these. From a budgetary standpoint, has there been a commitment of resources to solving these problems or is this just sort of an overlay, that management has said we are going to give an overlay of your current responsibilities and everyone is going to have to increase, or has there been a budgetary response to this problem?

MR. PODONSKY. Mr. Inslee, while I am not involved with the budgetary process for cyber security, I can tell you that we have seen a substantial increase in the CIO's budget and the centralization of the responsibilities for the CIO. So we do believe, from an independent oversight perspective, that the Department is applying resources to fix the problem, as opposed to just reports.

MR. INSLEE. Mr. Friedman, do you have any comment?

MR. FRIEDMAN. At this point, from our vantage point, as carefully as we've tried to look at this, I cannot correlate dollar for dollar increases in the cyber security budget with enhancements taking place. The problem is more environmental, if I may put it that way, than a shortage of resources.

Although I will say that when we talked to contractor personnel in the field, and we had a discussion earlier about the structure of DOE and the importance of the contractors, we do hear a number of complaints that there are things that they say they cannot do because the funds simply are not available. I have not verified that independently.

But, as I indicated earlier, the Department spends between two and two and a half billion dollars a year on information technology in the Department of Energy, Mr. Inslee, and we have a cyber security budget of about $140 million a year, so significant resources are being devoted to this problem.

MR. INSLEE. Is there value to be added by increasing frequency of these external controlled attacks, if I can call it, that our own good guys are attacking our DOE? Is that done with adequate frequency or aggressiveness? Should it be done more often to try to solve this problem?

MR. PODONSKY. Sir, since my office is responsible for conducting the majority of these penetration testings for the Secretary, I would tell you that we believe we are doing it on an appropriate frequency. Could it be more aggressive? We have become more aggressive in the last 2 years. But, at the same time, we also recognize that, as we continue to find the problems, the Department also has to catch up with fixing those problems.

From a standpoint of independent oversight, I would say there could be diminishing returns if we are constantly attacking the Department in ways that they don't have time to fix it. There could be an unintended consequence of never getting to the bottom of getting all of the problems fixed.

MR. INSLEE. Listening to your answers to Chairman Barton's questions about who should be notified when there are breaches, I suspect when we go to our closed hearing we are going to find non-compliance with the expectations that you suggested. What could

Congress do to see to it that if there is non-compliance with those expectations that you enumerated, what could we do to see to it that somebody cracks the whip on this problem? What would you suggest?

MR. PODONSKY. I think you are doing it right now by having a hearing.

MR. INSLEE. I would hope so. I am not sure that we are as omnipotent that you might think on a hearing.

MR. PODONSKY. Depends on if you are sitting up here or up there.

MR. INSLEE. Okay. Thank you very much.

MR. WHITFIELD. Thank you, Mr. Inslee.

One other question I'd like to ask you, Mr. Friedman. Of the total computer systems at DOE, it is my understanding that 75 percent of those computer systems are controlled by contractors. So when we talk about improving cyber security at DOE we certainly have to have contractors on board, and it is my understanding from information we have that during last year's Inspector General's audit of the computer systems you determined that several contractors have refused to comply with the DOE cyber security requirements because they said it's not in the contracts. Is that correct?

MR. FRIEDMAN. That's correct, Mr. Chairman.

Specifically, there are requirements that have been established under the FISMA statute, which I described earlier. Also, there are OMB requirements and extremely important benchmarks that have been established by the National Institute of Standards and Technology that are government-wide. Unfortunately, they have not been incorporated in a lot of the contracts as a flow-down; and, as a consequence, when we have talked to the contractor people who, as you correctly characterize, control many of these systems, 75 percent may be right. I don't quibble with that. I don't know if that's the precise number. They push back and say we don't have to do that, and the reason we don't have to it's not specifically required in our contract.

That gets to sort of a fundamental concern we have with regard to governance in the Department of Energy. There are a number of proposals to change the way we govern our contractors; and I am concerned that if we relax too many of the specifics when we have problems, the contractors come back to us and say, well, you didn't specifically require me to do X, Y, and Z. Therefore, I don't feel the need to comply.

MR. WHITFIELD. Well, in your discussions with the appropriate people at DOE who have jurisdiction over these contracts, are you satisfied with their explanations as to why they are not requiring --

MR. FRIEDMAN. Well, the CRD, which is the contractor requirement document, which is incorporated in the contract, is very general and

basically says use prudent judgment and be responsible. However, the situation is much more complex than that, and requires prudent judgment in the way you institute the cyber security program.

But the specifics presently are missing. We have raised that issue with Department managers on a number of occasions, and I think the response has been less than overwhelming. Hopefully, perhaps as a result of this hearing and your interest and the interest of the subcommittee, there will be more active participation in this program.

MR. WHITFIELD. They certainly have the authority to require that these security requirements be met, correct?

MR. FRIEDMAN. Well, I am not sure at this point whether, unless there was agreement on both sides, it wouldn't be a unilateral change to the contract. It would require a contractor commitment. However, for a new contract, certainly they could be made.

MR. WHITFIELD. If I am offering a contract and you're responding, then I want what I want.

MR. FRIEDMAN. Correct.

MR. WHITFIELD. So, obviously, that's something we are going to continue to look at. Because that is ridiculous that that not be required and in these contracts unless there is some overwhelming reason why it should not be done.

Anyone else? Okay. Okay. Well, that concludes the testimony of the first panel.

Now, Mr. Friedman, we genuinely appreciate you being with us today. It is my understanding you have an obligation that you have to go off to. So we would ask Mr. Podonsky to please stay.

We do intend to go into Executive Session as soon as we finish with the second panel, and there are three witnesses on the second panel. So we don't anticipate it will take us too long. But we do want to hear their testimony. We have some questions for them. So thank you for being with us, and we look forward to seeing you in Executive Session.

MR. FRIEDMAN. Let me say I appreciate your indulgence, and I apologize. My Principal Deputy, Herb Richardson, is here. He speaks for me eloquently, and he will participate in the subsequent session.

MR. WHITFIELD. We look forward to seeing Mr. Richardson there. Thank you.

Okay, first panel is dismissed.

At this time, I'd like to call up the second panel.

On the second panel, we have Mr. Tom Pyke, who is the Chief Information Officer at the Department of Energy. We have the Honorable Linton Brooks, Administrator for the National Nuclear Security Administration; and we have the Honorable David Garman,

Under Secretary for Energy, Science and Environment at the Department of Energy.

I want to welcome all of you. We appreciate your being with us on this important subject matter.

As you know, this is the Oversight and Investigations Subcommittee, and it is our tradition to take testimony under oath. Do any of you object to testifying under oath? Do any of you have any legal counsel that you would like to be with you? If you would raise your right hand.

[Witnesses sworn.]

MR. WHITFIELD. You are now under oath.

TESTIMONY OF TOM PYKE, CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF ENERGY; THE HONORABLE LINTON BROOKS, ADMINISTRATOR, NATIONAL NUCLEAR SECURITY ADMINISTRATION; AND THE HONORABLE DAVID K. GARMAN, UNDER SECRETARY FOR ENERGY, SCIENCE, AND ENVIRONMENT, U.S. DEPARTMENT OF ENERGY

MR. WHITFIELD. Mr. Pyke, I'll recognize you for your 5-minute opening statement.

MR. PYKE. Good afternoon, Mr. Chairman. My name is Tom Pyke. I am the Chief Information Officer of the Department of Energy. I am pleased to be here today to share with the committee a summary of the actions that the Department of Energy has taken to strengthen our cyber security posture.

The Department of Energy takes cyber security very seriously. Our senior management team is working together to ensure that we are taking all appropriate actions to protect our information systems as well as the information processed on these systems. We are taking a risk-based approach, managing the overall risk and the risk that still remains after all appropriate managerial and technical controls have been applied. This risk is sometimes called residual risk.

The Department's cyber security program is guided by the Federal Information Security Management Act, known as FISMA, including its emphasis on certifying and accrediting every information system before it is placed into operation. We are also guided by the actions and products of the Committee on National Security Systems and by the National Industrial Security Program Operating Manual for national security systems.

Based on a risk assessment and a system security plan, each system has controls applied to ensure availability, confidentiality, and integrity of each system and the information on that system. These controls are

tested to ensure they are working properly. After the controls are applied, a statement of the residual risk is presented to an accrediting official. This official makes the determination for the system to become operational based on the residual risk evaluation, taking into account the role of the system in supporting the agency's mission.

I would like to point out to the committee that there is no such thing as no risk and no such thing as perfect cyber security. Well-informed judgments have to be made as to the nature and amount of protection that is to be applied to each system and network, and that is a fundamental part of the certification and accreditation process. We are also guided in managing cyber security by the Office of Management and Budget with its policy and by guidance issued by the National Institute of Standards and Technology.

Our cyber security program responds to risk assessments conducted within the bounds of our assessment of the current threats to our system. The threat to our systems from outside our perimeter as well as from insiders is continually increasing. The hackers and others intent on harming our systems or obtaining information from our systems are becoming smarter in their attacks. The threat is especially challenging given the vulnerabilities in off-the-shelf operating systems and application software that we must use to support our mission. This software is very complex, and vulnerabilities are continually identified over the lifetime of that software.

Although software vendors prepare and distribute software patches after vulnerabilities are identified, there is always a delay in preparing and distributing these software patches, creating a window of opportunity for attacks despite best efforts to maintain secure system configurations and despite best efforts to apply the software patches in a timely way.

I should also point out that software patches need to be tested first before they're applied to our systems to ensure they do not interfere with the systems' ability to meet mission requirements.

Our cyber security posture is bolstered by the testing we do during the certification and accreditation process as well as by systematic continuous vulnerability testing.

We also benefit significantly from the testing that the Department's Office of Inspector General conducts as a part of its financial and FISMA reviews, and we are also fortunate to have within the Department the Office of Security and Safety Performance Assurance, which conducts the red team attacks that you have been hearing about and penetration testing on our systems and networks to identify vulnerabilities as well as performing cyber security assessments and evaluations that are of great help to us.

The Department of Energy has extensive expertise in the area of cyber security, and we are devoting substantial resources to this important area. The challenge in managing cyber security is for us to prioritize our efforts using a risk-based approach as we implement all the parts of a balanced cyber security program. We need to be smart about how to apply our cyber security resources, both in what we do and in the relative priority we give to the various parts of this effort.

When I came on board at Energy at the end of November of 2005, the Department had recognized the cyber security challenge it faced. I have personally given cyber security the highest priority in the management of the Department's information technology. At that time, we had available a recently prepared Cyber Security Project Team report that you heard about earlier. We had that in hand. That summarized some of the kinds of action that needed to be taken to improve our cyber security posture.

At the direction of the Secretary and the Deputy Secretary, I led the development of the Department of Energy Cyber Security Revitalization Plan, which now provides the basis for the Department cyber security program. The plan was developed under the oversight of an executive committee, which I chair, and which has as members the Under Secretaries, including the Administrator of the National Nuclear Security Administration, Ambassador Brooks, and the Under Secretary for Energy, Science, and Environment, Mr. David Garman, as well as the new Under Secretary for Science, Dr. Ray Orback, the Director of the Office of Security and Safety Performance Assurance, the Administrator of the Energy Information Administration, and a representative of the Department's Power Map Marketing Administration.

We have a Cyber Security Working Group that reports to this hearing committee that has coordinated the development of the Revitalization Plan and is actively involved now in coordinating the implementation of the plan.

In developing the Revitalization Plan, we went "back to basics," guided by FISMA and OME policy. We considered the Department's mission and the way the Department is structured, and we considered the cyber security risks currently faced by the Department. We factored into the plan the recommendations from the Cyber Security Project Team report.

Under the Revitalization Plan, my office, the Office of the Chief Information Officer, develops top-level cyber security policy, to be issued by the Deputy Secretary. Our office issues guidance on issues--

MR. WHITFIELD. Mr. Pyke, excuse me for interrupting, but you have gone about 2 minutes over the 5 minutes. If you wouldn't mind

summarizing; we do have your testimony in its entirety, and I would appreciate it.

MR. PYKE. After we had this top-level policy, the Under Secretary established policies and implementation plans for this part of the Department consistent with that policy and guidance; and the plan provides a basis for long-term strength in cyber security in the Department, with the significant beginning to be accomplished in the next 12 months. We've already issued initial guidance in the critical certification and accreditation area.

I should say that it has been very important for us to continue to adjust our priorities and implement the Revitalization Plan based on our assessment of risk. For example, during the last 3 months, we have given special attention to improving our ability to respond to increasingly more sophisticated cyber attacks. The resources required to do so have necessitated changes in our schedule or our initial schedule for completing some other parts of the revitalization effort.

We would like to assure the committee, to which we have provided our current schedule, that we are working very hard and diligently in our area; and we are attempting to accelerate the completion of as many products as possible to the extent that we are able to do so.

MR. WHITFIELD. Thank you very much, Mr. Pyke.

[The prepared statement of Thomas N. Pyke, Jr. follows:]

PREPARED STATEMENT OF THOMAS N. PYKE, JR., CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF ENERGY

Good afternoon, Mr. Chairman. My name is Tom Pyke. I am the Chief Information Officer of the Department of Energy. I am pleased to be here today to share with the Committee a summary of the actions the Department of Energy is taking to strengthen its cyber security posture.

The Department of Energy takes cyber security very seriously. Our senior management team is working together to ensure that we are taking all appropriate actions to protect our information systems and the information processed on these systems. We are taking a risk-based approach, managing the overall risk and the risk that still remains after all appropriate managerial and technical controls have been applied, often called residual risk.

The Department's cyber security program is guided by the Federal Information Security Management Act (FISMA), including its emphasis on certifying and accrediting every information system before it is placed into operation, by the Committee on National Security Systems (CNSS), and by the National Industrial Security Program Operating Manual established by Executive Order 12820 for national security systems. Based on a risk assessment and a system security plan, each system has controls applied to ensure availability, confidentiality, and integrity of each system and the information on that system. These controls are tested to ensure they are working properly. After the controls are applied, a statement of the residual risk is presented to an accrediting official. This official makes the determination for the system to become operational based on this residual risk evaluation and the role of the system in supporting the Agency's mission.

I would like to point out to the Committee that there is no such thing as "no risk" and no such thing as perfect cyber security. Well-informed judgments have to be made as to the nature and amount of protection that is to be applied to each system and network, and that is the nature of the certification and accreditation process. We are also guided in managing cyber security by Office of Management and Budget (OMB) policy and by guidance issued by the National Institute of Standards and Technology (NIST).

Our cyber security program responds to risk assessments conducted within the bounds of our assessment of the current threat to our systems. The threat to our systems from outside our perimeter and from insiders is continually increasing. The hackers and others intent on harming our systems or obtaining information from our systems are becoming smarter in their attacks. The threat is especially challenging given the vulnerabilities in off-the-shelf operating system and applications software that we must use to support our mission.

This software is very complex, and vulnerabilities are continually identified over the lifetime of that software. Although software vendors prepare and distribute software patches after vulnerabilities are identified, there is always a delay in preparing and distributing these software patches, creating a "window" for attacks despite best efforts to maintain secure system configurations and despite best efforts to apply the new software patches in a timely way. I should also point out that software patches need to be tested first before being applied to our systems to ensure that they do not interfere with the systems' ability to meet mission requirements.

Our cyber security posture is bolstered by the testing we do during the certification and accreditation process, and by systematic, continuous vulnerability testing. We also benefit from the testing that the Department's Office of Inspector General conducts as part of its financial and FISMA reviews, and we are also fortunate to have within the Department the Office of Security and Safety Performance Assurance, which conducts Red Team attacks and penetration testing on our systems and networks to identify vulnerabilities, and performs cyber security assessments and evaluations.

The Department of Energy has extensive expertise in the area of cyber security, and we are devoting substantial resources to this important area. The challenge in managing cyber security is for us to prioritize our efforts using a risk-based approach as we implement all the key parts of a balanced cyber security program. We need to be smart about how we apply our cyber security resources, both in what we do and in the relative priority we give to the various parts of this effort.

When I came on board at Energy, at the end of November 2005, the Department had recognized the cyber security challenge it faced, and I have given cyber security the highest priority in the management of the Department's information technology. We had a recently prepared Cyber Security Project Team report in hand at the time that summarized the kinds of actions needed to be taken to improve our cyber security posture.

At the direction of the Secretary and the Deputy Secretary, I led the development of a Department of Energy Cyber Security Revitalization Plan, which now provides the basis for the Department's cyber security program. This plan was developed under the oversight of an Executive Steering Committee, which I chair, and which has as members our Under Secretaries, the Administrator of NNSA and the Under Secretary for Energy Science, and Environment, as well as the Director of the Office of Science, the Director of the Office of Security and Safety Performance Assurance, the Administrator of the Energy Information Administration, and a representative for the Department's Power Marketing Administrations. We have a Cyber Security Working Group that reports to the Steering Committee that has coordinated the development of the Revitalization Plan and is actively involved now in coordinating implementation of the Plan.

In developing this Revitalization Plan, we went "back to basics," guided by FISMA, OMB policy, and NIST guidance. We considered the Department's mission and the way

the Department is structured, and we considered the cyber security risks currently faced by the Department. We factored into the Plan the recommendations from the Cyber Security Project Team report.

Under the Revitalization Plan, the Office of the Chief Information Officer (OCIO) develops top-level cyber security policy, to be issued by the Deputy Secretary. OCIO issues guidance on implementing cyber security management, Department-wide, working with the Cyber Security Working Group in doing so. Our office also leads the charge for awareness by everyone in the Department of the importance of each person's role in cyber security, and provides oversight of the entire Department-wide cyber security program. We also regularly advise senior Department management of evolving threats and the best protection strategies to employ in implementing cyber security protections.

Each of the Under Secretaries establishes policies and implementation plans for their part of the Department, consistent with the overall Departmental policy and guidance. They each tailor their implementation to meet the needs of their respective programs. OCIO works with the entire Department in preparing reports of cyber security status, as required under FISMA, and OCIO also conducts compliance reviews relative to policy and guidance to ensure that adequate protection of our information and information systems is in place. The Office of the Inspector General and the Office of Security and Safety Performance Assurance each conduct appropriate oversight reviews and testing that help ensure that the cyber security program is working as intended. The results of these reviews are expected to continue to be very important inputs to the Department as we continue to improve our cyber security program.

The Revitalization Plan identifies five high priority activities: certification and accreditation; use of an enterprise defense-in-depth strategy, providing layered protection from the perimeter of our networks to our users; asset management, to ensure that all information technology assets are identified and managed well with secure configuration controls and timely software updates; network interconnection and segmentation; and education and awareness. The major components of the revitalization process are identified as: planning, based on a common understanding of risk and threat, to ensure that cyber security is integrated through business practices and Under Secretarial missions; cyber security policy and guidance; architecture and technology that supports Department-wide implementation; common services that support the entire Department, including incident management, education and awareness training, and asset management tools and support; and performance measurement, providing a clear and consistent means to measure the cyber security status of the Department.

The Plan is intended to provide a basis for a long-term, strengthened cyber security program, with a significant beginning to be accomplished in the first twelve months, by February 2007. The highest priority activities, based on risk, are receiving attention and resources first, even as detailed planning and implementation continues throughout the Department. We have already issued revised certification and accreditation guidance, and we have initiated a corporate asset management process. Network segmentation plans have been developed and implementation has begun. We have organized a Department-wide cyber forensics team that is responding daily to cyber attacks, with excellent results. Cyber security awareness for all employees has been jump started with special bulletins containing detailed guidance, focusing on social engineering attacks, against which everyone's participation is essential.

The Secretary has said that "revitalizing our cyber security program is the best way to ensure that we continue to protect our Department's assets and the nation," and he has charged the Department's leadership to commit ourselves to this task. We are all working together to move as quickly as we can to improve the Department of Energy cyber security posture, and I believe our progress is now being felt through an improved ability to thwart attacks and to bring all the necessary resources to bear quickly and effectively as needed. We understand that cyber security is a never-ending process, and

we are committed to maintaining a high level of vigilance to ensure that the Department is able to carry out its mission without disruption caused by cyber threats. I would be pleased to respond to any questions you may have.

MR. WHITFIELD. Mr. Brooks, you are recognized for 5 minutes.

MR. BROOKS. Thank you, Mr. Chairman. As Mr. Pyke's statement made clear, we have to focus on and use a risk-based approach. And the highest risk, of course, would be compromised classified material. I recognize the hearing is focused primarily on threats to unclassified material, but it is important to note that we have to focus on both. I am confident that our classified material is secure, but we need to focus on both unclassified and classified.

I'd like to highlight several specific actions that we are taking to strengthen cyber security. First--and this does apply to classified--is the conversion to diskless work stations. We will be completing that by the end of 2008. About 45 percent of our classified work stations are operating without disks, and that will increase our ability to transmit both classified and other forms of sensitive information around the Department.

Secondly, we are working on continuous asset monitoring systems. That lets us improve real-time security monitoring of both classified and unclassified networks and lets us increase the efficiency and the accuracy of our reporting.

Several of the members of the committee have stressed the very large number of computers that we have spread out over a very large number of organizations. If we do not have a solid handle on what we have, no management system will work. And we have spent, with Mr. Pyke's organization, the last 18 months testing and evaluating a series of offerings. We've selected a customized architecture and last week our Pantex plant became the first DOE site to successfully implement the system.

Third, we are giving increasing attention to deployment of encryption for secure communication over unclassified networks. The fragmented nature of the Department means that we sometimes act inefficiently, so we've worked together with Mr. Pyke's organization to combine our licenses into a single agreement for various commercial encryption software to save about a million dollars.

In addition, we are implementing encryption on laptops in a way similar to that described by the Inspector General.

Fourth, we're working hard on training. Training and awareness are the keys to everything else. Mr. Pyke sets the example by conducting training at pop-up meetings, and at the senior leadership meetings of the Department, and we're attempting to emulate that in a variety of ways. In addition to these, we've developed a comprehensive set of policies to

standardize configuration that gives our individual sites a uniform set of risk management tools. We are trying to use our metrics not just to feed in to the various reports that Mr. Pyke mentioned, but to improve internally. We are developing continuity of operation plans and we are continuing to focus on inventory.

Working with Mr. Pyke, we are making good progress--that is a statement about the progress, not about where we are--toward both better management of risk and more efficient use of resources. I believe every member of the Department's leadership is committed to both improving cyber security and to the security of our information.

The following is not in my prepared statement. I know we will be talking about this more in the classified closed session. But I do want to note that the personnel information which he referred to is not what we would normally call personnel files. It is a list of names, and Social Security numbers. I don't mean to minimize the seriousness, but it might very well have been something else, but that's what it was and we can talk about that in more detail in the closed session.

Thank you, sir.

MR. WHITFIELD. Thank you.

[The prepared statement of Hon. Linton Brooks follows:]

PREPARED STATEMENT OF THE HON. LINTON BROOKS, UNDER SECRETARY OF ENERGY FOR NUCLEAR SECURITY AND ADMINISTRATOR, NATIONAL NUCLEAR SECURITY ADMINISTRATION, U.S. DEPARTMENT OF ENERGY

Good morning, Mr. Chairman, thank you for the opportunity to appear before you today in support of the Department's efforts to strengthen our cyber security.

The National Nuclear Security Administration Act (NNSA) established the NNSA within the Department of Energy (DOE) with the mission to strengthen the United States' security through the military application of nuclear energy and by reducing the global threat from terrorism and weapons of mass destruction. As Administrator, one of my duties is the security of NNSA's information systems and networks.

NNSA is responsible for the majority of the classified networks within the Department and we take this responsibility very seriously. Our classified networks receive our highest priority and we have taken all possible steps to ensure their security. I am confident of the security of our classified systems and networks and to date we have been successful in preventing any breach in security. However, we must maintain constant vigilance over the systems entrusted to us and it is essential that we continue the improvements underway to upgrade the infrastructure and improve integration across the Federal complex. Only by doing so can we ensure the long-term cyber security of the nuclear weapons complex.

NNSA is dependent upon information and upon the systems that create, process, store, and communicate information to carry out our missions. But the management of the security for these systems must rely on a comprehensive understanding of systems, in depth analyses of every new attack, and a timely determination of the best approach to mitigate the efforts of intruders. Doing so requires a substantial commitment of resources-- both financial and intellectual—and a coordinated effort across all elements of the Department.

I look to Mr. Tom Pyke, Chief Information Office (CIO) for the Department, to integrate our Departmental efforts. NNSA supports the Federated approach and is applying that approach across the NNSA complex. We have engaged each of our laboratories, plants, sites and offices in assessing the priorities that must be addressed in the future. These priorities are based on the risks at each site, as each site has different types of information it must protect and transmit.

Cyber security threats are increasing in complexity and number and we are working to strengthen our cyber security posture. We continue to monitor all aspects of cyber security throughout the NNSA complex and to apply risk management to balance cyber security issues with available budget resources. NNSA, with leadership from the CIO, is working closely with the Office of Security and the Office of Counterintelligence to maintain awareness of cyber security threats. We are jointly working to maximize our efforts and resources to ensure a secure environment for the transmission and storage of our information.

Today, I would like to highlight four specific efforts that benefit the department and strengthen cyber security throughout the weapons complex:

Diskless Workstation Upgrades: Plans are in place to convert the department's classified workstations to diskless operations. The plans support the completion of the conversion effort by the end of FY 2008 and as of the end of April 2006 over 45% of the Department's classified workstations were operating without disks. The ultimate success of the effort is tightly linked to the ability of the Integrated Cyber Security Initiative (ICSI) to implement a gateway to permit non-weapons data – both DOE and other agency data – to traverse the Department utilizing the Enterprise Secure Network. Development work on the gateway, including a connection to SIPRNet, is expected to begin in FY 2007.

Continuous Asset Monitoring System (CAMS): CAMS has two overarching objectives: 1) to improve security monitoring of DOE's and NNSA's networks (both classified and unclassified) in near real-time as well as software patch management; and 2) to increase the efficiency and accuracy of congressionally-mandated, asset-based reporting. A joint NNSA-DOE team invested almost 18 months testing and evaluating multiple vendors' offerings with the goal of selecting a common solution for both classified and unclassified operational environments, to minimize cost and standardize the system administration. To meet the Agency's long term reporting obligations, a customized architecture was selected consisting of hardware, software and process solutions which will be implemented across the Department and will include all NNSA sites, labs, plants and offices.

Encrypted Communication: With the support of Congress, we have accelerated deployment of enterprise encryption for secure authentication and communication. We fully support the Department's move to purchase encryption software. Currently, NNSA and DOE have multiple contracts. An agreement is being negotiated where these licenses will be combined into a single agreement and upgraded to a new thin client version. New licenses will be purchased at a reduced rate as needed. This combined arrangement will ultimately save the Department over one million dollars in licensing and maintenance costs.

Cyber Security Training: NNSA has partnered with DOE in a training working group that evaluates products and vendors training programs for all positions in the management and use of computing assets. Training for our cyber security professionals is also key to raising awareness and acceptance of assessing and prioritizing cyber security risks at all sites.

NNSA has also developed a comprehensive set of cyber security policies that standardize the configuration of many of our systems and assists in fully documenting the risks associated with the certification and accreditation of our computing assets. The policies we have directed fully implement national and federal policies in a graded risk

management approach. Site managers now have a uniform risk acceptance based process for assessing requirements and for implementing their cyber security programs.

NNSA is moving forward on multiple fronts to strengthen and ensure a safe information technology working environment. We continue to report our Office of Management and Budget (OMB) cyber security metrics and actively use this information to improve program control and evaluation. We continue to develop our continuity of operations plans as required by Departmental directives. We have established a working group to improve our cyber security by establishing security configurations for each of the computer systems in use across our federal and contractor sites. NNSA is teaching classes in cyber security policy implementation that expand on the DOE information as required for our weapons complex. Finally, we continue to support the Department to improve the inventory of our information systems.

Mr. Chairman, we are working diligently to maintain a secure environment for our information and that of the Department. We are moving ahead, we are making progress, and with the Federated approach, and we will be able to better manage risk and the efficient use of resources.

I look forward to your questions. Thank you.

MR. WHITFIELD. Mr. Garman.

MR. GARMAN. Mr. Chairman, members of the committee, as you have heard from the others, cyber threats are on the rise and I cannot tell you that we can fully guarantee the protection of all of the data that resides on the system or our systems themselves. Moreover, given the evolving and dynamic nature of the threat, I believe it's unlikely that we will ever be fully satisfied with our cyber security posture. However, the fact that we cannot achieve absolute enduring protection against all cyber threats must not deter us from undertaking serious sustained efforts to improve our cyber security posture.

The Secretary and the Deputy Secretary have made cyber security a priority shortly after they came to the Department. They grasped the challenges that confronted us. They recruited a new Chief Information Officer. They established a Cyber Security Executive Steering Committee, on which I serve, along with the others you see here and more. We've established the Cyber Security Working Group comprised of information technology and cyber security specialists to assist us in our responsibilities.

During the ensuing months we have developed and issued a cyber security revitalization plan that we are currently implementing, to put it bluntly and--you mentioned this earlier, Mr. Chairman--it is my view that we are not yet where we need to be. But I believe we are far better off than we were a year ago as a consequence of these actions by the Secretary, the Deputy Secretary and the Chief Information Officer.

In addition to stressing the importance of cyber security to the assistant secretaries and office directors that report to me, I have met with the cyber security information and technology personnel who report to them to discuss and understand the particular challenges that they face.

We've also recently detailed a cyber security expert to my office to assist me in implementing the plan and identifying best practices for replication.

In addition to the efforts embodied in the Security Revitalization Plan, we've engaged in a number of activities that improves the Department's ability to protect our data. For example, in 2005 the Office of Science initiated a cyber security site assistance visit program. Cyber security specialists from the Office of Science, together with inspectors from the Office of Security and Safety Performance Assurance, are conducting, as we speak, cyber security reviews at various sites and national laboratories. These visits are helping sites to identify and remediate potential weaknesses and risks and establish a consistent cyber security baseline.

To date, the Office of Science has conducted 10 such visits and will shortly expand coverage to facilities outside of their purview.

The Office of Environmental Management, meanwhile, has also made significant process in reengineering its own cyber security oversight process. That office has developed several cyber security management applications, such as intrusion detection, monitoring capability, allowing them to identify foreign-based cyber attacks launched against EM facilities from the Internet, and risk assessment management systems which automate cyber security risk assessments in support of their certification and accreditation responsibilities. Those are just some examples of our programs of active cyber security programs, and all are working collaboratively to implement relevant portions of the cyber security revitalization program plan at headquarters and in the field.

Now, this is very important. We know that this is not a quest for an end point where we declare success but, rather, a continuous process where we strive to get ahead and stay ahead of our adversaries. Just as we welcome the efforts of the Inspector General, the Office of Security and Safety Performance Assurance, and others to test and evaluate our success in this regard on an ongoing basis, we also welcome the efforts of this subcommittee as we work to manage cyber security risks in a cost-effective and responsible manner.

This concludes my testimony and I would, of course, be pleased to respond to any questions you have either today or in the future. Thank you, Mr. Chairman.

[The prepared statement of Hon. David Garman follows:]

PREPARED STATEMENT OF HON. DAVID K. GARMAN, UNDER SECRETARY FOR ENERGY, SCIENCE, AND ENVIRONMENT, U.S. DEPARTMENT OF ENERGY

Mr. Chairman and Members of the Committee, I appreciate this opportunity to discuss the Department's efforts to strengthen our cyber security posture.

We recognize the importance of providing adequate protection to our systems and our data, given the criticality of those systems and data to supporting our mission as well as the sensitivity of much of the data in our possession. As such, we continue to assess and evaluate our cyber security posture as it relates to the threat.

Cyber security threats are on the rise. I cannot assert that we can fully protect all our data on our systems today; however, we try. Moreover, given the evolving and dynamic nature of the threat, it is unlikely that we will ever be fully satisfied with our cyber security posture. However, we must not allow the fact that we cannot achieve absolute, enduring protection against all cyber threats to deter us from undertaking serious, sustained efforts to improve our cyber security posture.

The Secretary and Deputy Secretary have made cyber security a priority. Shortly after they came to the Department, they grasped the challenge that confronted us. They recruited a new Chief Information Officer (CIO). They established a Cyber Security Executive Steering Committee on which I serve, along with the Administrator for the National Nuclear Security Administration, the CIO, and others. We have established a Cyber Security Working Group comprised of information technology and cyber security specialists to assist us in our responsibilities. During the ensuing months, we have developed and issued a Cyber Security Revitalization Plan that we are currently implementing.

To put it bluntly, while we are not yet where we need to be, I believe we are far better off than we were a year ago.

In addition to stressing the importance of cyber security to the Assistant Secretaries and Program Directors who report to me, I have met with the cyber security and information technology personnel who report to them to discuss the particular challenges that they face. We have also recently detailed a cyber-security expert to my office to assist me in implementing the plan and identifying best practices for replication.

Therefore, in addition to the efforts embodied in the Cyber Security Revitalization Plan, we have engaged in a number of activities that improve the Department's ability to protect its data.

For example, in 2005, our Office of Science initiated a cyber security Site Assistance Visit (SAV) Program. Cyber security specialists from the Office of Science, together with inspectors from the Office of Security and Safety Performance Assurance, are conducting cyber security reviews at various sites and national laboratories. These visits are helping sites to identify and remediate potential weaknesses, accept risks, and establish a consistent cyber security baseline. In addition, these visits serve to provide training to a cadre of cyber security personnel and help identify best practices. To date, the Office of Science has conducted ten such visits and will shortly expand coverage to facilities outside the purview of the Office of Science.

The Office of Environmental Management (EM) has also made significant progress in re-engineering its cyber security management oversight process. EM has developed several cyber security management applications such as an Intrusion Detection Monitoring capability, allowing them to identify foreign-based cyber attacks launched against EM facilities from the Internet, and a Risk Assessment Management System, which automates cyber security risk assessments in support of their certification and accreditation responsibilities.

Those are just some examples. All of our programs have active cyber security programs in place, and all are working collaboratively to implement relevant portions of the Cyber Security Revitalization Plan at Headquarters and in the Field. We know this is

not a quest for an end point where we declare success, but rather, a continuous process where we strive to get ahead, and stay ahead of our adversaries.

Just as we welcome the efforts of the Inspector General, the Office of Security and Safety Performance Assurance, and others to test and evaluate our success in this regard, we welcome the efforts of this subcommittee as we work to manage cyber security risk in a cost- effective and responsible manner.

This concludes my testimony. I would be pleased to respond to any questions you might have, either today or in the future.

MR. WHITFIELD. Thank you very much and we appreciate your testimony. And, of course, it's not the purpose of this subcommittee to be critical all the time, but we do take our oversight responsibilities seriously and the information that I think all of us could agree to in many ways is that there is a lot still lacking on cyber security at DOE, and some people say that they may have one of the worst systems in the Government, but we may or may not agree with that.

But, Mr. Pyke, I know you have only been there since November of 2005, and you and Mr. Garman referred to the Revitalization Plan of 2006, and I know a great emphasis has been placed on that. But in reviewing the plan, we had noticed that six of the corrective actions that were suggested out of many had already passed their dates, and the one on cyber risk assessment was supposed to have been completed on April 6th; and it's not completed and no new date has been set. The DOE incident management was scheduled to be completed in May of 2006. It's not completed and no new date has been set.

And I know that's easy for us to just pinpoint a few areas where you have not met your plan, but what do you have to say about that, Mr. Pyke? I mean, these evidently were not that complicated because they were going to be completed in a couple of months. And now that it's already gone over, and you are not meeting the goal.

MR. PYKE. Mr. Chairman, as stated in my oral comments, my opening statement, it is essential that we continually adjust our priorities based on our current reassessment of risks. We have adjusted and will continue to adjust or prioritize our schedule for completing the large number of products. We made a lot of progress in the incident management area that will lead to a strong incident management guidance document and, as I said earlier, we have had to deal with increasingly sophisticated attacks and larger number of attacks over the last 3 months. And I can assure you that we have learned from handling those attacks and we have already adjusted our incident management processes within the Department in a positive direction.

Likewise on risk assessment we are learning in the process, the products when they are produced will be strong, and we do intend to continue to adjust our schedule, as is indicated, and we believe we are being responsible in doing that.

MR. WHITFIELD. So you are setting priorities in a different way than what it was originally set at?

MR. PYKE. Yes, sir.

MR. WHITFIELD. Now, Mr. Brooks had mentioned in his opening statement that we all view any breach to be a serious issue, particularly when personnel information is obtained by unauthorized sources outside the Government. We also understand the national security issues involved.

But I want to ask you, Mr. Pyke--you are the Chief Information Officer--when did you first become aware that the information of 1,500 people had been obtained by a third party?

MR. PYKE. Two days ago, sir.

MR. WHITFIELD. Two days ago.

MR. PYKE. Although since I arrived at the Department and was informed of the kinds of attacks that we are under on a continuing basis, and I should say we were attacked several hundred thousand times each day by folks from outside the Department attempting to break through our perimeter. The particular system that was involved here was protected by a firewall, and was protected by intrusion detection software. It had other protective software; and despite that, a very sophisticated attack succeeded, and we are dealing with a very difficult situation which we'll expand on in Executive Session.

MR. WHITFIELD. What is your understanding as to when someone at DOE was first aware of this information being obtained?

MR. PYKE. I do not know--

MR. WHITFIELD. You found out 2 days ago.

MR. PYKE. And that was about the time when a determination was--to my knowledge, when the first determination was placed in black and white on paper that this had happened after an extensive investigation. That's my understanding.

MR. WHITFIELD. Mr. Brooks, when did you find out?

MR. BROOKS. Late September.

MR. WHITFIELD. Now, this was--

MR. BROOKS. Now, with the recognition that, as Mr. Pyke says, this has been an ongoing event, but late September is when I--

MR. WHITFIELD. That's when you first found out that the information on 1,500 individuals had been obtained by an outside party.

MR. BROOKS. Yes, sir.

MR. WHITFIELD. Did you feel like you had an obligation or responsibility to report it to the Secretary or the CIO?

MR. BROOKS. The CIO builds the wall. Once somebody gets over the wall, it is a counterintelligence issue or potential counterintelligence

issue. Pretty much whenever I say the words counterintelligence, whatever I say next is a closed session issue.

There was a problem with fragmented responsibility--and as far as I can tell now, I was not aware, frankly, that the Secretary and the Deputy had not been informed. And as far as I can tell, this is one of the consequences of the split counterintelligence organization, which the Administration has submitted legislation to correct. It's a very important question, but I'd like to go into it more in closed session because I am afraid that the specifics could be in the areas we shouldn't talk about.

MR. WHITFIELD. And, Mr. Garman, when did you become aware the first time?

MR. GARMAN. June 7th.

MR. WHITFIELD. June the 7th.

MR. GARMAN. Two days ago.

MR. WHITFIELD. Okay.

MR. BROOKS. In fairness, I should point out to the best of my knowledge all of the people involved are under my responsibility and not his.

MR. WHITFIELD. And it is my understanding that the Secretary did not know about this until a couple of days ago. Is that your understanding, or do you know?

MR. BROOKS. I think that's right.

MR. WHITFIELD. Okay. Who informed you about this breach, Mr. Brooks, or is that something--

MR. BROOKS. The Director of the NNSA counterintelligence organization.

MR. WHITFIELD. Okay. I have no other questions.

Mr. Stupak.

MR. STUPAK. Yes, thank you.

Mr. Brooks, whose responsibility is it to inform the Secretary?

MR. BROOKS. That sounds like such an obvious, clear question, and I believe that one of the things we are learning from this is the answer isn't as clear as it should have been. Because we treat these things as a counterintelligence issue under our current structure, which we proposed legislation to fix, you can get two answers to that. It appears to me that each of the parts assumed that the other person was involved. That's a preliminary assessment because I, just as the Secretary just learned about this this week, I just learned this week that the Secretary didn't know.

MR. STUPAK. So who are the two people who were supposed to inform the Secretary?

MR. BROOKS. We have under the present system an Office of Counterintelligence for the Department and an Office of Defense Nuclear Counterintelligence for the NNSA. I am not trying to be

unresponsive, but I am really worried that in trying to answer that question I am going to go into areas that I don't want to go, about where the data was and whose data it was and what we think happened. I'd like to save that for the closed session if I may, sir.

MR. STUPAK. Don't you have any responsibility to tell the Secretary?

MR. BROOKS. I certainly wish I had, now that I know that nobody else did. I think that there are a number of us who in hindsight should have done things differently on informing. As far as I can tell in terms of responding to the cyber incident, that was not done well.

MR. STUPAK. Who should have notified this committee?

MR. BROOKS. Um, I am not sure, sir; and part of our problem is I can't answer that question.

MR. STUPAK. Will you get the answer to us?

MR. BROOKS. Yes, sir. I will.

MR. STUPAK. Why does it take the VA when they have a breach, 26.5 million people's information has been obtained, they let us know in about 3 weeks. It's been at least 8 months and DOE doesn't let us know.

MR. BROOKS. I'll find out, sir.

MR. STUPAK. You didn't hold anyone accountable for this.

MR. BROOKS. When I figure out what was done wrong and by who, if anybody, then I'll be able to answer that. I am really reluctant to answer it in the absence of fully understanding what happened.

MR. STUPAK. If you said to the Chairman you are going to build this wall, right, to protect our cyber security, right?

MR. BROOKS. Yes, sir.

MR. STUPAK. Don't you think you should have told Mr. Pyke, who is your Chief Information Officer, about this?

MR. BROOKS. Mr. Pyke was not in the Department at the time this incident happened.

MR. STUPAK. Mr. Pyke has been there for some time. You have known since late September. So when were you going to tell your Chief Information Officer, who is supposed to know how to build that wall. How does he build the wall if you withhold information from him?

MR. BROOKS. I will let Mr. Pyke speak for himself on what he knows. He is very familiar with the specifics of the--more familiar than I with the specifics of the incident.

MR. STUPAK. I thought he testified it was only 2 days ago when Mr. Pyke found out.

MR. BROOKS. What the content of the data was, but you protect the data without regard to its content, and whatever is sitting on a system.

MR. STUPAK. If he doesn't know where the contact is, he doesn't know where the hole in the wall is.

MR. BROOKS. I'll defer to Mr. Pyke.

MR. STUPAK. Before I go there, did you tell your previous CIO officer, then, that you knew since September--Mr. Pyke's been here a couple of months--did you tell the other CIO officer?

MR. BROOKS. I did not. It was my understanding at the time that the organizations had shared that information, but I'll have to answer that for the record, Mr. Stupak.

MR. STUPAK. Okay. Mr. Pyke.

MR. PYKE. Soon after I arrived at the Department of Energy, I was briefed on the current state of cyber security, including a number of very sophisticated attacks that were being made, which will be the subject of discussion in closed session today.

MR. STUPAK. Were you told--

MR. PYKE. I said a few minutes ago the so-called breach was in the context of very sophisticated attacks that went through full protective measures that were state of the art at the time, and that for the most part the Government, and the private sector are state of the art today. We're fortunate in having still additional protective measures in place without which we would not know about this incident. We'll discuss that in closed session. I did not know until June 7th, 2 days ago, that a particular file had been exfiltrated or sent out during one of those attacks.

MR. STUPAK. How do you protect the information in that file if you don't know the file has been breached? How do you know if your security system--how do you know why--if your security patches are working if you don't know which file or which network has been breached? How do you protect that file, then?

MR. PYKE. We protect all files, in part depending on the nature of the system, the risk associated with it, the data and the function of the particular system.

MR. STUPAK. Obviously it didn't work here.

MR. PYKE. We don't necessarily need to know the actual content of the file to provide appropriate protection.

MR. STUPAK. How do you protect what you don't know you lost? How do you protect something after it is lost?

MR. PYKE. Sir, as a part of our cyber security program, we apply a wide-range management and technical means in order to protect the data.

MR. STUPAK. I understand all of that, but how do you protect something if you don't know it's lost?

One part knew you lost it 8 months ago, you knew you lost it 2 days ago. How do you protect it if you don't know it is lost? How do you know your system is working properly if you don't know it's lost?

MR. PYKE. We'll discuss the details in closed session, sir. The determination that anything might have been lost was a long complex process. It deals with the state of the art of cyber security protection.

It's not a simple case.

MR. STUPAK. It's not a simple case of having to know the information that was lost. It's a simple case of you're supposed to have a security system. It was breached. It's not necessarily the information which, you know--it is the fact that you were breached and no one tells you for 8 months; and what the information is and the extent of that security, that's a different issue. The issue is you have the responsibility for cyber security. Something was breached, you don't even know about it.

MR. PYKE. Mr. Stupak, it would have been very helpful for my job to know that that file had been breached and had gone outside. However, one of the things I learned--in fact, one of the reasons I came to the Department of Energy was to try to strengthen cyber security because it was receiving, like many organizations, increasingly sophisticated attacks which in part resulted in the loss of this file.

MR. STUPAK. Maybe we should start with information sharing between each part of DOE.

Yes, sir. Mr. Brooks.

MR. BROOKS. We can go into this in a little more detail, but I believe that we have given you a misunderstanding. It is Mr. Pyke's systems that told us about the file. We have a better answer than we have given you, although not a perfectly satisfactory answer, but I really need to do this in closed session, sir.

MR. STUPAK. Okay.

MR. WHITFIELD. Mr. Burgess.

MR. BURGESS. Thank you, Mr. Chairman. I think we are probably all anxious to get to closed session now, so I'll be pretty brief. I wanted to ask a few more questions about the issues that came up to the previous panel on sequestration on the encryption.

Neither member of the other panel really could address what the cost would be for going to a fully sequestered and encrypted system. Does anyone on this panel have a concept of the cost involved, the budgetary requirement to go to a system that employs full encryption sequestration?

MR. PYKE. Mr. Burgess, segmentation of networks and sequestering data, if you like, as well as encryption are two techniques that are already being applied within the Department in protecting data as a part of the total package of cyber security projections. As you heard earlier, we make extensive use of encryption software appropriate for protecting information, and we do plan to expand that use. The issue here is not one of resources. In fact, in terms of resources, although we can always

use more in cyber security, it's a question of applying the resources in a prioritized way and smart way. We are expanding our use of encryption. We've already used some of it in terms of segmentation. We have taken significant steps to segment our networks in the last several months, and we are continuing to do even more of that.

MR. BURGESS. Are you satisfied that you are doing all you can to rapidly deploy encryption throughout your Department?

MR. PYKE. I am never satisfied, sir. We always are working, attempting to work faster and to get more protections in place as quickly as we can.

MR. BURGESS. Mr. Chairman, I think in the interest of going into closed session, I am going to yield back. I have some other questions.

MR. WHITFIELD. Ms. DeGette from Colorado.

Ms. DeGette. I'll be brief as well. I want to ask, Ambassador Brooks, you said you knew about this breach 8 months ago, correct?

MR. BROOKS. Yes, ma'am.

Ms. DeGette. Did you inform the 1,500 people who were targets of this breach that their data had been breached, their information had been breached?

MR. BROOKS. This is going to sound like a strange answer. I'd like to answer that in closed session. The answer is no. I'd like to answer why in closed session.

Ms. DeGette. I was going to say I don't think that's classified whether you informed them or not. And so you'll talk about why in the closed session.

Do you have concerns about the safety of those individuals?

MR. BROOKS. No, ma'am.

Ms. DeGette. And I suppose you'll tell me about that in closed session, too.

MR. BROOKS. Yes, ma'am. I will.

Ms. DeGette. I am going to wait until closed session.

MR. WHITFIELD. Mr. Inslee? No.

Mr. Walden is recognized.

MR. WALDEN. Thank you, Mr. Chairman.

Mr. Pyke, we've learned in testimony from the Inspector General's Office that as many as 50 percent of the cyber security incidents at DOE were not reported to law enforcement officials, which is a requirement. What's been done to ensure that all reportable cyber security incidents at DOE are reported to the authorities?

MR. PYKE. Mr. Walden, we have policies and procedures in place that require reporting of incidents and we have criteria that we apply, that are supposed to be applied, throughout the Department for determining which would be reported within the Department as well as to outside law

enforcement as necessary. Whenever anything happens like that, when we become aware of it as part of our compliance monitoring of our policies, we take action in order to shore it up. I've been pleased with the amount of incident reporting that I'm aware of, for example, in this fiscal year it--we have seldom learned of incidents after the fact that should have been reported.

MR. WALDEN. So what you're saying is what the Inspector General reported to us is no longer the case.

MR. PYKE. What I am saying is the trend is in the right direction, and I believe the people are being more diligent in reporting of incidents.

MR. WALDEN. So the Inspector General indicated 50 percent of the cyber security incidents were not reported to law enforcement. What would you say that percentage is today, then?

MR. PYKE. Sir, I have no idea. I am aware of only a very small number of cyber security incidents that we've learned about significantly after the fact, beyond the reporting requirements, and that have been entered in and reported at that time. It is hard to tell--it is hard to know what you don't know. And I am afraid--and I agree with the Inspector General that folks may have a tendency to try not to report things because they think there might be a stigma associated with reporting incidents. In a number of cases these incidents occurred despite all the proper protections being provided. I do not know how many incidents are not being reported.

MR. WALDEN. It could be the 50 percent the inspector references.

MR. PYKE. I believe based on the data I do have of what we've learned after the fact of incidents that should have been reported, I have seen a relatively small number of such incidents.

MR. WALDEN. The data on these individuals, 1,500 individuals who work for the Department of Energy, that was taken, can you describe for us the content of those data? Social Security numbers; were they personnel files, personal addresses?

MR. BROOKS. They did not have personal addresses. May I consult with somebody for a moment?

MR. WALDEN. Certainly.

MR. BROOKS. Name, Social Security number, a code which indicates who they worked for, a second code which indicates if they were a subcontractor, the majority of these are contractor employees; a code which either had the letter L or Q, the level of clearance, those are the two DOE clearances; and a column called status, which in every case said "continue." What this appears to have been was the list of routine people being processed for update of clearance.

There was no home information, there was no personnel file-type information, there was no health information. There was nothing that

would, from the paper, let you know where these people lived or worked. Although the particular code that is not particularly sensitive, it's just a way you put that in smaller boxes.

MR. WALDEN. With other search engines--

MR. BROOKS. That's the information.

Ms. DeGette. Will the gentleman yield?

Ambassador Brooks, if somebody got that information from your file; your name, your Social Security number, your security clearance, everything else, and Mr. Walden is right, you can just go on other search engines, but even if you didn't, wouldn't you be a little concerned if nobody told you that for 8 months?

MR. BROOKS. Of course I would.

Ms. DeGette. Thank you.

MR. WALDEN. Reclaiming my time.

What is the protocol for your agency where you have a breach of personnel records? Are you required to notify the individuals within a certain period of time, or do you have any rules or regulations?

MR. BROOKS. We have no formal rules. This is an issue of good management and our obligation to people. It's not an issue of regulation, as far as I can tell. I want to be very clear. There is a reason we have waited and I will talk about that more in closed session. I don't want to suggest, and I apologize to your colleague if I may have suggested, that I don't think this is important. We had a reason for doing what we have done.

MR. WALDEN. We look forward to hearing that, obviously, in the closed session.

I guess the other part of this though, does anybody get in contact with, for example, the credit agencies to make sure that these people's data, that somehow they aren't becoming victim of some sort of ID theft?

MR. BROOKS. The practice of the Federal government has been to notify individuals and provide them a mechanism for verifying that on their own. Individuals have certain legal rights, and the Department will follow the standard practice.

MR. WALDEN. I suppose, Mr. Garman, you are the Deputy Secretary, correct?

MR. GARMAN. No, sir. I am the Under Secretary for Energy and Environment.

MR. WALDEN. So do you have jurisdiction over the personnel side of this? Does anybody have jurisdiction over this issue?

MR. BROOKS. I think to the extent that anybody does, I do, although there are legal implications.

MR. WALDEN. I spent some time with the Secretary of Veteran Affairs listening to him describe what his agency went through, and how

he responded to protect the veterans, and the meeting with the security agencies, or, excuse me, the credit rating bureaus. His first goal, he told me, was to protect the veterans and their records.

MR. BROOKS. My understanding is that was somewhat more extensive data.

MR. WALDEN. Of course it was. In the millions, we know that.

MR. BROOKS. I mean, on each individual.

MR. WALDEN. I see what you're saying. But when it comes to in terms of identity theft, my name and my Social Security number gets somebody probably a cup of coffee or two and can really mess up my credit.

Given your cyber ability, do you have any knowledge that anybody has manipulated this data, or do you track that?

MR. BROOKS. To the best of my knowledge. I'd rather not go beyond what I'm about to say in open session. To the best of my knowledge, we have absolutely no evidence that anybody has done anything with this. I have a little bit of a basis for that statement, not a huge basis. I will talk more in closed session.

MR. WALDEN. Mr. Pyke, it's my understanding that many of the successful computer intrusions at DOE could have been avoided if they applied available network security patches and use of effective passwords. However, the failure to apply security patches and the use of common passwords continues to be a problem at the Department of Energy.

I understand 2 months ago several employees at DOE were targeted with an e-mail that successfully infected their computers with the Trojan Horse program that would have been prevented if DOE had provided current security patches. Can you tell us how you'll ensure that security patches and effective passwords will be implemented?

MR. PYKE. Mr. Walden, we are working to improve the way software patches are tested first and then distributed and applied to all systems, as I mention in my statement, and we learn from each incident, each experience that we have. Fortunately, the software patch protection is, again, one way of protecting systems, and in that particular case we were able to protect the systems and the data using other cyber security techniques that were applied at that time.

MR. WALDEN. In the Department of Interior a Federal judge has interceded because of the lack of security in some of their data files and has from time to time literally shut down the entire e-mail and network system for the Department of Interior. It seems to me the Department of Interior has far less critical data to the country's security perhaps in some areas than your agency.

MR. PYKE. Sir, you are right on target. System security configuration and system software patch management are key parts of cyber security.

MR. WALDEN. So you can understand our concern, and we share yours, and hopefully together we can get this cleaned up.

MR. WHITFIELD. Thank you, Mr. Walden.

Mr. Inslee.

MR. INSLEE. No questions.

MR. WHITFIELD. Mr. Barton.

CHAIRMAN BARTON. Thank you, Mr. Chairman. I apologize for having to leave. I had to go give a presentation at a conference, so I missed some of it. Some of what I say or ask I am sure is going to be redundant, but it probably won't hurt to have it said again.

Mr. Pyke, what are your duties as Chief Information Officer at the Department of Energy?

MR. PYKE. Mr. Chairman, I am responsible for the management of information technology throughout the Department, including ensuring that good management practices are provided, that standards are applied in the appropriate way, that capital investment decisions relative to information technology are being made in a systematic way, and using all necessary information.

I am responsible for operations of headquarters systems, and increasingly we are putting into place standardized systems with strong cyber security for everyone associated with headquarters, and, very importantly, I am responsible for cyber security for the Department.

CHAIRMAN BARTON. So even though it says information, you are not responsible for disseminating information, you are responsible for basically coordinating and protecting the information from falling into the wrong hands; that includes cyber security.

MR. PYKE. Yes, sir.

CHAIRMAN BARTON. What is the interrelationship with your position and the National Nuclear Security Administration and Mr. Brooks? Do you all have a co-equal, or is he in his own little sphere? How does that work?

MR. PYKE. If I may address that relative to cyber security. As a part of the revitalization effort I have led over this last 6 months, we have established a structure, working together with the under secretaries and with me, in which our office establishes top-level policy. We issue guidance, and we work with the under secretaries as they apply that policy and guidance in a way appropriate to each of the parts of the organization that they are responsible for.

They adapt it, they apply it. They are responsible to take into account the risk associated with each of their organizations in determining how best to apply the top-level guidance.

CHAIRMAN BARTON. In your conduct of your office, if you found something askance in Mr. Brooks' administration, can you tell him he has to do something? You can inform, advise, but I don't believe --

MR. PYKE. We are partners, for example, in the area of cyber security. We each have a part of the role to carry out, and I can certainly advise him if I learn of something.

CHAIRMAN BARTON. The short answer is no. You can't make him do anything.

MR. PYKE. No, sir.

CHAIRMAN BARTON. Mr. Brooks, how long have you been the Administrator in NNSA?

MR. BROOKS. Since 2003. I was acting as Administrator for several months before that.

CHAIRMAN BARTON. Now, my understanding is as Administrator, you are the number one manager at that agency; is that correct?

MR. BROOKS. Yes, sir.

CHAIRMAN BARTON. And you're supposed to know everything that's going on; is that correct?

MR. BROOKS. Conceptually, yes, sir.

CHAIRMAN BARTON. Conceptually. Who do you report to, if anybody?

MR. BROOKS. I report through the Deputy Secretary to the Secretary.

CHAIRMAN BARTON. Report through the Deputy Secretary to the Secretary.

MR. BROOKS. Yes, sir.

CHAIRMAN BARTON. How often do you meet with either or both of those gentlemen?

MR. BROOKS. Daily, every other day. It varies. The average is probably once or twice a day. Some days much more, some days not.

CHAIRMAN BARTON. When you are having these daily or every-other-day meetings, is there a formal agenda, kind of a routine agenda, and then special events? Is it informal, whatever you want to talk about or they want to talk about?

MR. BROOKS. Normally it's informal. Normally it's on a particular topic that one or the other of us wants to talk about. We also collectively, the leadership of the Department, meet with the Secretary every Monday morning, and that is a go-around-the-table. We also have another weekly meeting once again involving the leadership of the

Department with the Deputy Secretary that does have a structured agenda.

CHAIRMAN BARTON. Now, are there any classifications of information that you have access to that they don't? Are they cleared to know any and everything that you know?

MR. BROOKS. Yes. I am trying to think through some of the intelligence compartments. Yes, there is nothing that I am cleared to know that they are not cleared to know.

CHAIRMAN BARTON. Now, it is public knowledge, at least in this hearing room, unfortunately outside the hearing room, that back in September we know from the testimony of the prior witnesses that Mr. Podonsky and his group conducted a red team exercise that penetrated some of the security protections at the Department of Energy, and you were made aware of that at that time; is that not correct?

MR. BROOKS. That's correct.

CHAIRMAN BARTON. Now, we also know that subsequent to that there was a real penetration of your administration.

MR. BROOKS. That's correct.

CHAIRMAN BARTON. And you were informed of that in September.

MR. BROOKS. That's correct.

CHAIRMAN BARTON. And you meet with the Secretary or the Deputy Secretary almost every day, and yet apparently you didn't tell them about that.

MR. BROOKS. That's correct.

CHAIRMAN BARTON. Now, for probably the third or fourth time, why not?

MR. BROOKS. I'm choosing my words carefully, and we can expand on this in the closed session. The Department has treated these intrusions once they happen as counterintelligence issues. The Department has a fragmented counterintelligence organization which it has submitted legislation to correct. It appears that each side of that organization assumed that the other side had made the appropriate notification to the Deputy Secretary.

CHAIRMAN BARTON. That's hogwash. You report directly--

MR. BROOKS. Correct.

CHAIRMAN BARTON. --to the Secretary. You meet with him or the Deputy every day. You are the number one manager in the Department for these issues. You had a major breach of your own security in your own--I mean, I don't know how much we are supposed to say in public about this, and yet you didn't inform the Secretary. To say that somebody else is responsible begs the intelligence of this committee.

I mean, I don't know what to say other than it will be my strong recommendation after I have had a consultation with the Ranking

Member Mr. Dingell that you be removed from your office as expeditiously as possible. And I mean like 5:00 o'clock this afternoon if it's possible.

I don't see how you could meet with the Secretary every day for the last 7 or 8 months and not inform him of a serious, serious breach of security.

I'm going to ask you another question. Do you think the President of the United States knows? How would he know if you haven't told the Secretary?

MR. BROOKS. The Secretary was aware of the incident, but not of the specific content.

CHAIRMAN BARTON. The Secretary told me personally, personally, that he didn't know about this until 2 or 3 days ago.

MR. BROOKS. That's my understanding as well.

CHAIRMAN BARTON. We're going to go into closed session. I don't know how we can function in a democracy if those responsible as appointed by the President of the United States don't do their duty to report what's under their responsibility to the Presidential appointees that they are supposed to report to. I don't know how we function.

If I were you, sir, I would strongly consider your resignation being tendered to the President and Secretary of Energy today. Again, I haven't spoken yet directly with Mr. Dingell, so my official act, I am not sure what official--I am not going to do anything that he and I are not together on, but I think it's unconscionable that we have been operating since September with a security problem of this magnitude, and those responsible for protecting the integrity of the United States of America at the highest level haven't been notified, because if your explanation is to be believed, there was some sort of a mixup, and you weren't sure who was supposed to do it.

You should have at least notified the Secretary that somebody--what you knew, and then you should have worked to clear up any bureaucratic problems with these other officials.

MR. BROOKS. Yes, sir, I obviously should have done that. I thought he had been notified because of this confusion I referred to, and obviously I was wrong. I should have made sure he knew it himself as we gained the information which came to us over time.

CHAIRMAN BARTON. Mr. Garman, you are the Under Secretary. Do you have any direct report on this, or are you out of the chain of command on this one?

MR. GARMAN. I am out of the chain on this incident, and I would offer this--

CHAIRMAN BARTON. When did you find out about it?

MR. GARMAN. Two days ago. But having said that, let me add that I knew and the Secretary knew and a lot of people in this room knew that the Department faces the same endemic problem that every agency in the Government faces, and that is we are under attack in the cyber world on a daily basis, and that these attacks--

CHAIRMAN BARTON. Do you think the way to prevent future attacks is for somebody like Mr. Brooks to not inform the appropriate Presidentially appointed officials in the Department of Energy when an attack has been successful?

MR. GARMAN. I am not going to get drawn into that, Mr. Chairman.

CHAIRMAN BARTON. Your position is stick your head in the sand, don't worry about it. That's what you just said.

MR. GARMAN. No, sir. Let me be clear about this. I think one of the other elements that has not been vetted in this hearing is the change that is underway at the Department. By your line of questioning of Mr. Pyke, and I don't want anybody to leave this room with the impression, or the public, in the public session of this hearing, that the responsibility for cyber security rests on Mr. Pyke's shoulders alone. What we are doing is transitioning and making it crystal clear to every program manager, every office director and every under secretary that they are responsible. It is a line management responsibility for cyber security.

I would argue from my vantage point that this has not always been clear inside the Department of Energy, and that when I was a lower-level--

CHAIRMAN BARTON. But is the answer to not report when there is a breach? If something were to happen within your purview at the Department of Energy, you have jurisdiction or management responsibility for the National Laboratories, or some of them, if there were a security breach of this magnitude at Hanford, would you not report it to the Secretary of Energy if you knew?

MR. GARMAN. Sir, there is still, and let me--there is much I do not know about this incident.

CHAIRMAN BARTON. I'm not asking what you know right now, I'm asking just fundamental. If I am responsible for this committee, for the management of this committee as Chairman, and I know that something bad happens, one of my staffers embezzles money, somebody does something that's illegal, I do something about it and report it to the Speaker. I don't just stick my head in the sand.

MR. GARMAN. No, sir. That's not what I am suggesting.

CHAIRMAN BARTON. I am appalled that nobody seems too concerned about this but the Members of Congress. I mean, it's just another day at the office, I guess; luckily only 1,500 were stolen.

Mr. Chairman, we're going to be in Executive Session here quickly, I assume.

MR. WHITFIELD. Yes, sir, Mr. Chairman. As soon as you finish your line of questioning.

CHAIRMAN BARTON. I just want to reinforce, Mr. Brooks, I am going to recommend, subject to Mr. Dingell, that you be removed. I think you would do the country a service if you resigned before you have to be removed. You have no credibility with me; none.

With that, I yield back.

MR. WHITFIELD. The Chair would move at this time pursuant to clause 2(g) of rule 11 of the rules of the House the remainder of this hearing will be conducted in Executive Session to protect the information that might endanger national security.

Is there any discussion on the motion? If there is no discussion, pursuant to the rule, a recorded vote is ordered. Those who favor, say aye.

Those opposed, nay.

Ayes appear to have it. The ayes have it, and the motion is agreed to.

We will reconvene in just a few minutes in Room 2218, and that portion of our hearing will be closed to the public and open only to our witnesses, the Members and staff to such Members, and witnesses who have appropriate clearances.

The subcommittee will recess.

[Whereupon, at 1:06 p.m., the committee proceeded in closed session.]

RESPONSE FOR THE RECORD OF THOMAS N. PYKE, JR., CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF ENERGY

QUESTIONS FROM REPRESENTATIVE BLACKBURN SUBMITTED TO MR. PYKE

Q1. Has your office examined security systems that other countries use to protect critical information systems? If yes, how could we apply these systems to our networks?

A1. The Department of Energy relies on cyber security guidance issued by the National Institute of Science and Technology, which we are informed, includes the results of international collaboration by NIST through which best practices internationally are factored into NIST's guidance, which, in turn is applied to protect DOE systems and data.

Q2. In the hearings on the DATA bill, I discussed the practicality of the PGP program that was very effective, efficient, and freely distributed during the 1990s. Can this program or a similar one be used for password protection with DOE's systems?

A2. DOE uses several encryption techniques to protect passwords stored within DOE IT systems, consistent with NIST guidance. DOE also uses commercial encryption software to encrypt some emails and their attachments and, increasingly, to encrypt some files stored on laptop and other computers. DOE uses Pretty Good Privacy (PGP) as well to ensure the integrity of some information when it is stored or transmitted.

Q3. Although DOE has not inventoried all their information systems, can you give this committee an approximate number of types of existing systems?

A3. The Department's Program Offices report having a total of 827 information systems, of which 403 systems are classified systems.

Q4. Does any DOE facility have their computer system installed with EMP protection?

A4. The Department has no computer systems installed with EMP protection at this time.

RESPONSE FOR THE RECORD OF GLENN S. PODONSKY, DIRECTOR, OFFICE OF SECURITY AND SAFETY PERFORMANCE ASSESSMENT, U.S. DEPARTMENT OF ENERGY

QUESTIONS FROM REPRESENTATIVE BLACKBURN SUBMITTED TO MR. PODONSKY

Q1. How often do the different departments within DOE talk/work together on Cyber Security?

A1. The Office of Security and Safety Performance Assurance (SSA) provides comprehensive information and analysis regarding the effectiveness, vulnerabilities, and trends of DOE cyber security programs, primarily through its Office of Cyber Security Evaluations, within the Office of Independent Oversight. In so doing, SSA regularly works with the other programs within DOE on cyber security issues on a near continuous basis. In addition to participating in the Cyber Security Working Group (CSWG) at both the principals and guidance levels, the Office of Cyber Security Evaluations has daily contact with key OCIO cyber security staff members to support a number of initiatives, ranging from reviewing proposed policy and guidance to participating in reviews of technical proposals. In some instances, where SSA has unique technical capabilities, the OCIO has requested assistance in evaluating the effectiveness of network management tools associated with such matters as patch management, automated log reviews, and host based intrusion prevention systems. In these cases SSA has been able to support the OCIO without compromising its independent oversight role. With respect to the other program offices, the Office of Cyber Security Evaluations has routine contact with cyber security staff personnel due to the nature of planning, conducting, and reporting announced and unannounced inspections, Site Assistance Visits (SAVs), and other special reviews. Numerous other less formal contacts occur weekly with respect to requests for information, sharing of ideas and passing on of lessons learned. In carrying out its inspection role, SSA personnel also have routine contact with a wide variety of field personnel which enables sharing of important information.

The DOE CIO frequently meets with the Secretary and the Deputy Secretary and other senior management to discuss the Department's cyber security program and steps being taken to maintain a sound defense-in-depth risk managed posture for protecting the Department's information and computing systems. The CIO chairs the Cyber Security Executive Steering Committee, the members of which include the Under Secretaries and the Director of SSA. The CIO also has regular meetings with the Directors of the Office of Intelligence and SSA.

The cyber security staff in the DOE OCIO has routine and frequent interactions with the cyber security staff of each of the Under Secretary organizations, the Power Marketing Administrations, the Energy Information Administration, and elements of the Office of Intelligence. The OCIO cyber security staff also has routine interactions with representatives of the DOE laboratories and production facilities through the Cyber Security Working Group (CSWG).

Q2. How long will it be before the revitalization process is finished? How much will it cost to finish it?

A2. The DOE CIO reports that the implementation of the Department's Cyber Security Revitalization Plan is well underway, and much will be accomplished in FY 2006. Most of the longer term actions will have been substantially achieved by the end of FY 2007, although improving DOE's cyber security posture is a long term, continuing effort. The Department is covering the cost of revitalization through the current cyber security activities and funding embedded within each IT investment department-wide. These costs are estimated to be $295 million in FY 2007 as documented in the BY 2007 DOE Exhibit 53 IT Portfolio report.

Q3. How long did it take to do the Cyber Security Project Team Summary Report? How much of this report has been put into action? What is your timeline to address the concerns in the report?

A3. SSA was directed by the Deputy Secretary of Energy to lead a team to develop a plan of action to remedy existing unclassified cyber security problems throughout DOE on October 5, 2005. The Cyber Security Project Team (CSPT) was then formed with members drawn from SSA, the Office of the Chief Information Officer (OCIO), the National Nuclear Security Administration (NNSA), and the Office of the Undersecretary for Energy, Science, and Environment (ESE). The CSPT delivered the Summary report on November 7, 2005. On November 25, 2005, the Deputy Secretary of Energy issued a memorandum concurring with the recommendations and directing the development of implementation plans to address them.

The recommendations identified in the CSPT have been integrated into the Cyber Security Revitalization Plan, approved by the Deputy Secretary on March 6, 2006. The recommendations are being addressed in the guidance being issued as part of the revitalization effort and in the cyber security architecture and strategic plans being developed by the department-wide team participating in the development and deployment of the revitalization plan. The initial revitalization plan forecast completion of the policy, guidance, architecture elements within 12 months. However, the Department is working to accelerate this development and deployment. Many of the DOE sites have adopted many of the recommendations as best practices and have begun implementing them in a manner consistent with the revitalization plan.

RESPONSE FOR THE RECORD OF HON. GREGORY FRIEDMAN, INSPECTOR GENERAL, U.S. DEPARTMENT OF ENERGY

RESPONSE FROM THE DEPARTMENT OF ENERGY INSPECTOR GENERAL TO CONGRESSWOMAN MARSHA BLACKBURN

Question: You said that GAO was looking at the Oak Ridge Y-12 plant. Can you provide me an update on the evaluation of its safety systems to my office?

After speaking with Rodney Bacigalupo, a member of your staff, it was clarified that you were seeking an update on the Office of Inspector General's (OIG) 2006 Federal Information Systems Management Act evaluation, which includes a review of the Y-12 facility. The OIG's review is ongoing and we expect to complete our work in mid-September 2006. Following its completion, we will furnish you with a copy of our report and, if desired, can brief you or your staff on the results of our work at Y-12.