# Press Conference on the "Cyber Storm" Cyber Security Preparedness Exercise with Under Secretary for Preparedness George Foresman and Acting Director for the National Cyber Security Division Andy Purdy

Release Date: 02/10/06 00:00:00

For Immediate Release
Office of the Press Secretary
Contact: 202-282-8010
Washington,D.C.
February 10, 2006

**MODERATOR**: Speaking today will be Under Secretary for Preparedness, George Foresman, and Acting Director for the National Cyber Security Division, Andy Purdy.

Before we begin, I want to make sure that everyone is aware -- I believe there were some press releases passed out at the door.

**MR. FORESMAN**: Good afternoon, everybody, and thank you for joining us today. Today marks a pivotal point in our efforts to strengthen America's ability to be able to deal with a wide range of risks, including the risks to our information technology systems.

Today we are concluding Cyber Storm, the largest cyber security exercise ever conducted. Cyber Storm examined the preparedness, response and recovery capabilities for a significant cyber disruption within federal, state, local government, international partners, as well as the private sector.

This exercise was a significant accomplishment for the Department of Homeland Security, as well as all of our partners in both the public sector and the private sector.

And I want to take a moment to recognize those folks who have partnered with us with this exercise: The U.S. Department of Defense, U.S. Department of Justice, Department of Commerce, Department of Energy, Department of Transportation, Department of Treasury, the State Department, the Central Intelligence Agency, the National Security Agency, the National Security Council, and of course the Homeland Security Council.

We've been blessed to be joined by other key members of our coalition to strengthen the nation's preparedness, including some of our state partners, representatives from the State of New York. New York was an active partner. Michigan, Montana, as well as the multi-state Information Sharing and Analysis Center, our focal point for coordination of cyber incidents and response in all 50 states and the District of Columbia.

We're extremely pleased to be able to do this as a collaborative public sector and private sector partnership. We had major industry participation, including CA, Intel, McAfee, Microsoft, SIMTech and VeriSign.

As the owners of most of America's critical infrastructures are in the private sector, it is essential that as we do these exercises, that we do it from a national approach; local, state, federal and including our private sector partners.

And I would also like to acknowledge the fact that we had phenomenal international cooperation as we went about conducting the Cyber Storm exercise. Our international partners included Australia, Canada, New Zealand and the United Kingdom.

As we all well know, cyberspace has no borders, and it is vital that as we address these issues we address these issues in a comprehensive fashion, including our international partners.

In many ways, the way it's best described is DHS is the conductor of the orchestra, and all of these partners that have been with us through the Cyber Storm exercise are the various musicians playing beautiful music together to create a symphony of preparedness. And we've made great progress.

Cyber Storm exemplified the importance of public and private sector and international entities working together and in concert and in coordination to prepare and to protect our citizens, our businesses, and frankly, our national interests.

Hurricane Katrina reminded us that there is an urgent need to enhance preparedness for catastrophic events in this country, whether natural or man-made, whether it's technology or whether it's physical impacts.

Under the leadership of Secretary of Homeland Security Michael Chertoff, this Department is undertaking a risk management approach where we are prioritizing our efforts on events that pose the greatest potential consequences

to our communities and our homeland.

Our new Preparedness Directorate, which I'm pleased to be able to work with many dedicated men and women on day-to-day basis, is specifically focused on strengthening America's preparedness so that we are ready to meet any type of threat at any time, any place, in the right way, with the right resources, to do the right things.

Cyber security is an essential part of our preparedness efforts, because information technology systems can connect so many aspects of our economy and our society, including transportation, finance, telecommunications, health care, and most importantly, our national security.

Our cyber infrastructure is interwoven with our physical infrastructure, and we must protect all of our infrastructure with the utmost vigilance.

The completion of the Cyber Storm exercise represents a significant milestone for not only the Department of Homeland Security, but our efforts to better secure cyberspace. And it is a true, clear indication of the dedication of the public sector and the private sector to work together collaboratively and cooperatively to do this.

The lessons that we learn from Cyber Storm will help us enhance our overall preparedness in America, and it will help us be better capable of responding to and recovering from not only cyber attacks, but the wide range of threats and risks that we face on a day-to-day basis.

I'm extremely pleased to have joining me today Mr. Andy Purdy, who is our currently Acting Assistant Secretary for Cyber and Telecommunications Security. Andy has done a phenomenal job in this capacity. He's done a phenomenal job with the exercise. He has led a broad, wide-ranging effort to make sure that we are on a day-to-day basis focused holistically on managing our risks, including the cyber risk.

And it's more than just simply having a plan or getting people together; it's doing what we did with the Cyber Storm exercise. It's bringing all the partners to the table, looking at our processes, looking at our coordination and communication structures, and making sure that when the unthinkable happens, we are ready to react appropriately, quickly and effectively.

Andy, if you'd like to join me. Thank you.

**MR. PURDY**: Thank you. Although I appreciate the promotion, Mr. Secretary, I'm the Acting Director of the National Cyber Security Division. The mission of our division is to work collaboratively with public, private, and international entities to secure cyberspace and America's cyber assets.

To accomplish this mission, we have established two overarching priorities that guide our efforts and initiatives, including the Cyber Storm exercise: To build an effective national cyber security response system, and to implement a cyber risk management promotion for critical infrastructure protection.

Cyber Storm is part of an ongoing risk-based management effort to examine and improve rapid response, promote cyber security, and reduce cyber risk within all the levels of our government and among private sector partners.

Exercise control for Cyber Storm was based at Secret Service headquarters in Washington, D.C. One hundred and fifteen public, private and international organizations participated in the exercise, many from their regular places of business, in over 60 locations in the United States, Canada, Australia, New Zealand and the United Kingdom.

Cyber Storm included cyber attacks that disrupted or impacted energy and transportation infrastructure and targeted federal, state and international government with the intent of disrupting or impacting government operations and undermining public confidence.

The attack scenarios were developed with significant input from industry experts who participated as exercise planners. The scenarios were all pre-scripted and implemented in a closed and secure environment, eliminating any external distress or distraction to participants' real world systems. In other words, the exercise did not include any attacks against real world systems.

The scenarios were intended to exercise a number of communication paths and processes dealing with cyber incident response. This includes identification and utilization of all communication channels, and interaction between emergency readiness teams to enhance the coordination and response between public private sector partners.

My colleagues at the National Cyber Security Division will analyze the data from this exercise with participants. A full report will be released this summer, and the conclusions drawn from it will be shared with our partners and the public.

This data will also be used in our risk-based analysis to help identify where enhances are necessary to our responses and planning and response efforts, such as the national response plan and the national infrastructure protection plan.

Cyber Storm has assisted in the coordination and collaboration between federal, state and local, private sector firms

and international partners. We are increasingly prepared to communicate and coordinate our responses to a potential cyber attack.

Finally, I want to thank Secretary Chertoff and Under Secretary Foresman for their steadfast support of this exercise. And I want to introduce and thank my co-chairs of the National Cyber Response Coordination Group: Chris Painter from the Department of Justice, and Mark Hall from the Department of Defense. They will both be available for your questions following the conclusion of our part of the press conference.

I also want to acknowledge the tireless efforts of our exercise director, Jeffrey Wright, and his excellent team, and all of our interagency, private sector and international partners without whom this exercise would not have been possible.

Cyber Storm truly is a testament to the importance of preparedness, and the public and private sector collaboration necessary to protect all Americans.

We look forward to your questions at this time.

**MR. FORESMAN**: Yes, ma'am?

**QUESTION**: I know you said the report is coming out in the summer, but can you give us some idea of what you learned from this exercise?

**MR. FORESMAN**: Well, we will actually be conducting the hot wash over the course of the next several hours this afternoon and into next week, but it's difficult to presuppose the specific nature, because, frankly, we haven't done an exercise of this scale or scope. But clearly, the opportunity presents itself for us to strengthen, and irrespective of what comes out of the lessons learned, anytime you do an exercise, you strengthen yourself, you train yourself, you make yourself better.

So the after-action report is interesting as it will be. What's equally important if not more important is what has already happened during the past five days, with the fact that both the public sector and the private sector partners have had an opportunity to train and plan and communicate with one another.

Yes sir?

QUESTION: Mr. Secretary, I'm curious about the cyber response system that you're trying to set up, the capability. In the kind of attacks we've seen in the past, like denial of service attacks, or viruses or worms, there doesn't seem to be any single entity responsible for responding. The FBI tries to investigate to find out the source. You've got private organizations like CERT and Microsoft putting out data on patches. What is the response team -- what is your vision of the response system? And given that the Internet is so much in private hands and not government hands, how do you get your arms around what you respond to?

MR. FORESMAN: Well, let me begin, and then I'm going to ask Andy to chime in as well. Part of the challenge that we run into, and particularly in the post-9/11 environment, you know, our post-Y2K environment. I was a state official as we went through that in Virginia -- is many activities have been progressing independently, but in a concurrent and a somewhat coordinated fashion on a wide range of things, including cyber security.

We're at the point in our natural evolution of our nation's preparedness efforts in the post-9/11 environment, the better understanding that we've got to manage not against threats or hazards, but against a full continuum of risk, we're at the point where we can do a better job of integrating activities, synchronizing activities.

And the role of the Department of Homeland Security as the nation's incident manager is not to solve everything, but to make sure that we get all the right players at the table, we get all the right information to them, so that whether it's the private sector doing those things that it's best for them to do, whether it's governmental agencies, any level of government, they have the information to be able to take the actions that are necessary for them.

QUESTION: What is your role going to be, then, if somebody attacks the Internet or something, what is your role going to be that's different from what SIMTech or CERT or any of these organizations that are out there now are already doing? What do you bring to the table?

MR. FORESMAN: Well -- and I'm going to bring Andy over. But the key thing that you bring to the table is coordination. The value -- the sum total of all of these parts operating in a unified strategy is going to be better than any one entity operating independently without a broader vision of what is it that we need to accomplish from a security standpoint.

So we will bring the ability to leverage multiple people towards a common goal, towards a common solution set in order to deal with the problem, so that it's not a haphazard approach, it's not an independent approach, but it's an interdependent approach.

And, Andy, do you want add to --

And, Andy, do you want add to

QUESTION: I'm not sure I know what that means. Do you get on the phone and make sure people are already doing what they're supposed to be doing already? Do you tell them what -- I still don't get what you're going to do here.

MR. PURDY: Under the Presidential Directive, the Department of Homeland Security is designated as a focal point for the public and private sectors for issues related to the security of cyberspace.

Under the National Response Plan, Cyber Annex, the group that we co-chair, the National Cyber Response Coordination Group, is the principal interagency mechanism to prepare for and respond to cyber incidents of national significance, working with the private sector to do so.

Within the National Cyber Security Division, our U.S. CERT arm, our operational arm, works as the incident sharing for all the federal agencies. Under the Office of Management and Budget, we get all the incident information from all the federal agencies.

And we work on an ongoing basis, not just when there is an incident of national significance, but in day-to-day activities and malicious activities, to help supplement and work in partnership with the private sector, so that when things escalate to a higher level, we are ready to build the situational awareness and the responses that we provide.

So the National Cyber Response Coordination Group leverages the capabilities of the agencies of the United States government from a cyber defense perspective, so that we have the situational awareness to detect and recognize incidents of significance. We have the ability to attribute the source of attacks and malicious activity. We have the ability for coordinated response to those attacks, and we have the responsibility to help with the recovery of the disruptions that might be caused by those attacks.

So day in and day out, we are combining the intelligence function, the CERT, the computer emergency response function, the law enforcement functions, where we take information as a focal point and we make sure the right information is shared.

So there might be law enforcement sensitive information that the Department of Justice and the FBI and the Secret Service obtains. We use that information, and we provide alerts to the public and those who may be most at risk. So even though we can't identify where we got the information, we can help benefit the public and the private sector.

So we work with the anti-virus companies, the managed service providers, the major companies, so that when there are vulnerabilities that need to be communicated, we can help make sure that the protections are implemented, not just in alerts, but through the anti-virus vendors and the other protections.

So, our focus is really to help protect the United States from cyber attack. And as Secretary Foresman talked about, this effort under the National Infrastructure Protection Plan, this public-private partnership to assess the risks to the United States of physical and cyber attacks, is going to assess the risk and prioritize the risk mitigation measures.

So when President Bush yesterday said that America is at risk, we recognize and, under Secretary Chertoff's risk management framework, we are assessing and mitigating physical and cyber risks faced by the Nation.

But fundamentally, we're doing it in partnership with our state governments, with our private sector partners and with all the agencies of the Federal Government.

MR. FORESMAN: He did better.

MR. FORESMAN: Yes, sir?

QUESTION: I'd like to hear a little bit more about the INJAX or the scenarios that were used in the model. Did they -- how farfetched or how imaginative were they in terms of envisioning wide-scale disruptions beyond very limited geographical problems that we've actually seen in real life in the past?

And did anything surprise you -- I know the hot wash is still pending, but did anything fall over that you hadn't anticipated falling over?

MR. PURDY: Well, because we weren't impacting real systems, there weren't actual things that were going to happen that we didn't anticipate.

Though, as part of this effort, we are assessing the potential economic consequences from what was envisioned. And under Secretary Foresman's direction, we are going to be enhancing our modeling capabilities as to -- if certain things happen, what is the effect on the functionality of our critical infrastructures. What is the impact on the functioning of our economy.

One of the specific examples of -- that I wanted to mention, we simulated a cyber attack where a utility company's computer system is attacked, causing numerous disruptions in the power grid. We wanted to highlight the critical

nature of cyber security and its interconnectedness to physical infrastructure and exercise coordination and communication between public and the private sector.

The fact is, there's cyber risk out there. We as a nation have to prioritize resources. We cannot mitigate all cyber risks anymore than we can mitigate all physical risks. So, the exploitation of the vulnerabilities that you know too often occur in cyberspace, is a reality.

And so this exercise tried to use the kinds of vulnerabilities that exist in our past, and hypothesized malicious actors who, for their own gains, wanted to cause disruptions and have an impact on public confidence and those who use the Internet.

MR. FORESMAN: Yes, sir?

QUESTION: A couple of questions. One is that, the 2003 top-off, how to cyber exercise a national one, how did you build on that? Did you find any weaknesses? Did you incorporate that, build on that?

And the second question is that, two weeks ago, state CIOs released a survey saying that they're just not getting any help, or very little help, from the Federal Government in terms of building up their own capabilities and preparedness, and if you can address that as well.

MR. FORESMAN: I'm going to let Andy start, and then I'm going to finish up on that one.

MR. PURDY: We have been building, in the creation of Cyber Storm, and the enhancement of our cyber response system. We have been building on the Live Wire exercise in September '03.

We have had a number of tabletop exercise with this group. We had an international tabletop exercise. We have had tabletop exercise with this group, the Interagency Incident Management Group, the Homeland Security Operations Center.

So we have really been working those issues, and we have been providing the inputs on an ongoing basis to help make us better. Help make up communicate better. Help make us respond better.

So when you look at the results that will come out from this exercise, the sophisticated nature of the actual alerts that were created in the course of the exercise, and compare it to what was done in Live Wire in September of '03.

We are pleased at the robustness of that effort. The ability to quickly get targeted guidance to public and private sector partners who need it has increased dramatically.

MR. FORESMAN: And let me follow up with one additional piece with regard to the states. You know, one of the key pieces that the Department of Homeland Security and bring to the table, and we've seen it through out multi-state ISAC, is to give the tools to the states so that they can begin to take those actions that are necessary.

And I would clearly point out, I come from state government. I just recently came out of state government. And one of the things that we recognized is that we needed the Federal Government to help us articulate what is the end goal strategy.

We have been able to do that, in part through the National Infrastructure Protection Plan and a number of other initiatives. But it's ultimately up to the states and the communities, as part of that broader national strategy, to be able to push the ball down the road.

And in Virginia, we were emboldened by the fact that we had funding that was available through the Department of Homeland Security through the grants and training activities that allowed us to focus on cyber security. We had guidance that was coming out of Andy's shop and coming out of our infrastructure protection efforts.

So, part of it is, we've got to be the coach and the mentor, but it doesn't necessarily mean that the Federal Government is going to be doing every piece of the action.

MR. PURDY: Let me add that the work that Will Pelgram, heading up the multi-state ISAC, I encourage you to talk with him after the scenario. And the robust play of so many states in the exercise illustrates the work in the last year or two, that the MS ISAC has done, and the robustness of the state information systems leaders, in working to make sure that they can appropriately respond when they face incidents, share information through the multi-state ISAC to the Department of Homeland Security.

In addition, Secretary Foresman, together with the standup of the Preparedness Directorate, has asked us to work closely with the grants and training office to take a fresh look to make sure that the provisions that are available for grants from the states are robust and that cyber is appropriately included in that.

In addition, we will be working with our government and private sector partners to create cyber attack scenarios of the

type of the 15 that DHS has generally.

And we'll associate capabilities with those scenarios, so that then states have additional mechanisms to identify what capabilities they need that they don't have, and seek funding for those efforts.

MR. PURDY: Yes, sir?

QUESTION: Assuming you have found some problems in this exercise, how detailed will the results be when they come out this summer? Is some of that information -- end up not being public information because of the nature?

MR. FORESMAN: Well, I think -- yes. You have clearly pointed on it. But there are two pieces to it.

One, this is a department that is absolutely committed to learning from lesson learned and after-action reviews. Obviously, as we go through the process, the key to improving our capabilities is to be able to share with out local, our state, our private sector partners the lessons learned and we fully intend to do that.

If there are those things that are of a sensitive nature, that doesn't mean that it won't be shared with our local, state or other federal agency partners or our international partners. It means we'll just have to find a way to share it so that there is not broad distribution of it.

But at the end of the day, we are not going to get any stronger, we are not going to get any better, unless we capture these lessons learned, share them amongst the broadest possible audience, and make a full commitment to pushing improvement down the road.

This is a core tenet to everything that we will do in preparedness, whether it's cyber security, whether it's physical threats, whether it's chemical, biological, radiological, or nuclear, we've got to be able to move forward.

STAFF: I think we'll take one more question. Pete?

QUESTION: Can I go back to the example you mentioned in the question about specific scenarios you have. Okay. So somebody hacks into a utility computer and tries to shut down the power grid. What now is your role? You are the agency, then, that warns every other utility in America? Hey, look at what this hacker did in central Ohio. Here's the patch you need to install right now to make sure it doesn't happen to you. Is that what you do?

MR. FORESMAN: Pete, let me address this in two ways. I want Andy to address it. And this is actually good, because it will help very much humanize, if you will, the discussion.

Let him talk about the cyber piece of it. But then I'd like to talk in the broader aspect about overall incident management and the role of the department.

MR. PURDY: Yes, we do supply alerts and warnings. When there are vulnerabilities that are particularly focused on control systems. And many of the vulnerabilities that are exploited that could affect control systems affect others.

So our alert and warning system, our national cyber alert system that provides actionable guidance to technical and non-technical folks across the Nation helps in that.

We also have a major effort -- one of our major risk mitigation efforts that we have already identified in cyber -- those are Internet disruption, those are control systems, and software assurance.

Those are areas that we believe that fundamentally we have to, and we are committed to, and we put the resources into it, working in close partnership with government and the private sector, to help reduce those risks.

So we have a partnership through the national laboratories, partnering closely with DOE and the other agencies, for the control systems effort, where we are trying to work closely with the owners and operators and the vendors to understand the unique issues and problems that the control system community faces. And that's across all the infrastructures.

So we can help develop -- and we've come up with a security framework that gives guidance that we are testing now. To help those out there know what they need to do, and work with vendors of products that can help reduce the risks that those control systems owners and operators face.

QUESTION: So, specifically in that case, what does that mean? And what do you do? You actually -- I know in the scenario, I'm sure you had to play it out. Did you --

MR. PURDY: Yes. We provided guidance as to how the systems could protect themselves against an exploitation of the vulnerability that we were seeing in the real world.

And often you get that information from the FBI. Out in the real world when somebody complains that these kinds of things are happening.

That's why bringing everybody together and coordinating and sharing of critical information is so important and so beneficial.

MR. FORESMAN: And, Pete, let me just add to that. I mean, if we have a cyber event that manifests itself as a series of a single or even cascading problems, you have disruption of the electric grids in a portion of the country, that is going to precipitate a need for coordination among local, state, federal authorities, the public sector, the private sector. It's going to cause us to push forward aspects of our Federal Government response under the National Response Plan. And it will require some level, possibly with coordination with our international partners -- and that's really the genesis of what DHS does.

DHS is that crisis coordination point, and we have embedded within DHS certain expertises, whether it's cyber security, infrastructure protection, those are the people who help inform both the public sector and the private sector response.

So, we're really doing three roles. We are helping to detect and alert. We are helping to coordinate the response and recovery activities. And we are providing that technical assistance to states, communities and the private sector, as they go about doing that response and recovery.

QUESTION: To help visualize that you actually do, is there a room somewhere here? A sort of a national crisis readiness command center, with all sorts of monitors and you are seeing little blips and somebody reports a problem and you press a button and you've got all the utilities on the phone, or you've got all the telephone companies on the phone, or -- is that what you have, sort of a command center here, to be ready all the time?

MR. FORESMAN: Well, let me just give it to you in the most general of terms. It is not a single point. It is a system of systems. And it's interconnected centers that provide situational awareness on a wide range of hazards and threats that we face in America on a day-to-day basis.

It's a distributed network that allows us to collect information and intelligence from a wide range of resources. All of that is amalgamated on a day-to-day basis. And the center of the department's activities here at the NAC is the Homeland Security Operations Center. But the Homeland Security Operations Center is the hub activity of many other public sector, private sector, multi-levels of government operations centers around the country.

STAFF: Mr. Foresman, Mr. Purdy, thank you for your time. Thanks, everyone. I think we've got some of our partners that are going to be up front of you have additional questions.