Timeline	TGT	Type	JMET#	CND Events Timeline Remarks	Author	Inject Pt
D - 400 - D - 8						
			4/15/2007	[b4b2]. $1.86 plus fees Airfare		
	TSA		5/17/2005	Jet Diverted to Maine to Check Passenger		
			5/7/2005	[b4b2] down for 15 Minutes May 7		
				Calls for Hackers		
				Plane enters "No Fly Zone"		
			5/10/2005	White House and Capitol Evacuated Plane fly's though "NFZ"		
				"Hi-Tech Hate" slogans on 62 nations Web Sites		
				World Economic Forum Personal Information Stolen		
				Major Software Provider Systems Source code Stolen		
				Airport [b4b2] system vulnerabilities exploited		
				Airport Access Control Pilot Program (AACPP) offline (Orlandiris detection		
				TRANSFERRED TO OTHER AGENCY		
	U5	CNA		TRANSFER FOR DIRECT REPLY - DHS Response to Call for Hacker		
	General Internet Users			Trojan Horse E-mail	Patch and security companies pumping out patches/upd	
	DC Metro	CNA		DC Metro Shut Down		
	DC Metro	CNA		DC Metro Website Hacked and Posts Future Threats		
	US Military	CNA		Unusual Traffic at US Military Websites and NIPRNET		
	Port of Tacoma	CNA		Port Mainframe Shut Down	Military Sealift Command	
	Port Panama City	CNA		Port Mainframe Shut Down	Military Sealift Command	
	Port of San Diego	CNA		Port Mainframe Shut Down	Military Sealift Command	
	Burnside Bulk Marine Terminal (La	CNA		Port Mainframe Shut Down	Military Sealift Command	
	USTRANSCOM (GTN)	CNA		Unusual Login Activity		
	DoD	CNA		Trojan Horse E-mail		
	U.S.	CNA		Reports of Compromised Major Operating System Patches		
	USTRANSCOM (GTN)	CNA		Non-Working Password Issues		
	DHS all Nodes			Homeland Security Information Network Difficulties		
	US/Canada			Disruption in Montana Law enforcement Radio Networks (SummitNet)		
	U.S.	PSYOP		Media Reports 4 ports Security Screening Compromised		
	U.S.	PSYOP		Media Questioning DoD CND Efforts		
	Canada	PSYOP		U.S. Eliminating French Culture		
	U.S.	PSYOP		Hacker Precautions Taken		
	U.S.	PSYOP		Media Reports Global Capitalist Atrocities		
	US Military			US Military "Internet Café's" overloaded		
	USTRANSCOM (GTN)	CNA		SMTP Port Searches		
	USTRANSCOM (GTN)	CNA		SNMP Port Scans		
	USTRANSCOM (GTN)	CNA		USTRANSCOM Website Defacement		
	USTRANSCOM (GTN)	CNA		NGA Comercial Imagery Graphics Disrupted		
	U.S.	PSYOP		Sympathetic Anti-Global Protesting		
	STATE DEPARTMENT	PSYOP		U5 Experiencing Websight and Global Embassy Probes		
	U.S.	PSYOP		Media Questions on DoD Computer Security		
	DoT NC	PSYOP		Location of HAZMAT freight Cars sent to several Blog sites		
	FAA			Tower Disruption at Chicago and Philadelphia Airports		
	U.S.			Commercial Airline Computer Compromise		

b2

b5

CND Events Timeline

U.S.		Commercial Airline Computer Problems
U.S.		***Rail Switching Failures***
USTRANSCOM (GTN)	CNA	GTN Possible Compromise
USTRANSCOM (GTN)	CNA	GTN Compromise Confirmed
US Military	CNA	Hacker Claims received and posted on DoD sites
DoD Websites	CNA	Unusual E-mail being received
USTRANSCOM (GTN)	CNA	ASIM Reporting Extended Log-in Session
USTRANSCOM (GTN)	CNA	Windows NT Problems
USTRANSCOM	CNA	Surface Deployment & Distribution Command (SDDC) Map Found
Air Mobility Command	CNA	ACFP (Automate Computer Flight Plan) Compromised
USTRANSCOM	CNA	Confirms ACFP compromise is foreign and malicious
USTRANSCOM	CNA	E-mail Classification Problems
USTRANSCOM	CND	ASIM Monitoring Of Other Ports
Air Mobility Command	CNA	Unauthorized Login Attempts Detected
USTRANSCOM	CND	E-mail Rejection Problems
DoD	CNA	Classified Data In Unclassified E-mail
USTRANSCOM	CNA	Trojan Horse E-mail
London	PHYSICAL	Liquid Found in Subway
	CNA	DC, NC, NYC Yellow Bus Dispatch "Protect the Children" Post
White House	**CNA**	**Unidentified Aircraft has entered restricted Airspace**
DoT	**CNA**	**Alaska pipeline leak detection system compromised**
	CNA	**GPS Guided Systems experience abnormalities**
Local		DC, Miami, NYC area school delays and closures
		2nd Unidentified Aircraft has entered restricted Airspace
	PSYOP	**Detailed Plans of US Refinery Sites & NYC Tunnels Distributed**
General Public/Gov't Sites		Unable to Download Major Operating System Patches
Catskill Aqueduct		**Water Treatment Plant Computers Compromised**
Montana		**Water Treatment Plant Computers Compromised**
Chester Water Authority (PA)		**Water Treatment Plant Computers Compromised**
Los Angeles		**Water Treatment Plant Computers Compromised**
	PSYOP	Anti-Globalization Movement Denial of Water Tampering
U5	**CNA**	**Hundreds of "Watch List" and "No Fly" people flood U5 airports**
U5	PSYOP	Report of Watch List and No Fly Irregularities
		Federal Government enacts "Liberal Leave" policy for DC area
DC Metro		Metro systems on line. Physical threats still being investigated
DoT	CNA	Critical Infrastructure Remote Sensing Experiencing Attacks
DoT		Results of NCRST-H posted as "challenging" on Hacking Sites National Consortium on Safety, Hazards and Disaster A:
DoT Montana		**Highway Border Security checkpoint computers go offline**
		Report of Border Security Problems
	PSYOP	Report of Illegal Watch List Entries/Attempts
		Port Auth of NY & NJ "Spokesman" announce integrity of system
NYPA	CNA	Denial of Service attacks begin on Port Authority of NY & NJ
		Major News Network Will not reveal sources of reports
		Continued Background Noise

P3

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

Scenario Overview

Transportation

- **Aviation**
  - "Watch List" Irregularities
  - Tower Disruption
  - Security and Cargo
  - "No Fly Zones" Breached/Tested
  - GPS Guidance Systems
- **Waterborne Commerce**
  - Port Closures / Disruptions
  - Security and Cargo
  - GPS Guidance Systems
- **Rail**
  - SCADA Systems
  - HAZMAT

Homeland Security

Scenario Overview (Continued)

Transportation

- **Mass Transit**
  - DC Metro
  - NY/NJ Port Authority
  - NC/MT Disruptions
  - PSYOP Threats
  - Power Outages
- **Highways**
  - "Watch List" Border Issues
  - Oil and Commerce Transport
- **Pipelines (Cross Sector)**
  - SCADA Systems (flow and distribution)
  - Water Authority Disruptions

Homeland Security

Transportation Thread

- What indications would you have, if any, of an impending cyber attack?
  - Indication specifics (what is the indicator, when is it noticed, who is notified, etc…)

Homeland Security

Transportation Thread

- What level of attack would involve federal notification? Is this dependent upon the number of plants shut down? The area covered? Or is it because a group claims responsibility for the attack?

Homeland Security

Transportation Thread

- How would communications work once something has occurred?
  - When an incident occurs, who is notified? How?
  - Communication with Canada if cross-border? Who initiates? What is the chain?

Homeland Security

Transportation Thread

- Would you issue any RFIs? What would you request and who would you ask? What would the White Cell need to prepare ahead of time to be able to answer the RFIs coming into the White Cell? What would those requests and responses look like?

Homeland Security

Scenario Timeline

Major Events

DECISION POINTS

[redacted]

b 2

Activist Call to Hackers

Increased Protesting

Anti-Globalization Rally

Increased Probing / Testing of Networks and Security

Power plant shut downs / Blackouts

Port Disruptions

State and Local Attacks

Rail SCADA

Claims of Responsibility

Air Traffic Disruptions

Pipeline Disruptions

"Watch List" Irregularities

Continued Minor Cyber Activity (Copycat?)

Background Noise Throughout

Homeland Security

Scenario Overview (Continued)

Transportation (Monday)

b 2

Homeland Security

Scenario Overview (Continued)

Transportation (Tuesday)

b 2

Homeland Security

Scenario Overview (Continued)

Transportation (Wednesday – Thursday)

b 2

Homeland Security

Scenario Overview (Continued)

Transportation (Thursday)

b2

Homeland Security

Scenario Overview (Continued)

Transportation (Friday)

[b 2]

Homeland Security

Expected MPC Outcomes

Proposed final player list

Initial Communications Survey

Scenario framework complete; writing assignments identified

Action plans with milestones for scenario completion

Confirmed Final Planning Conference date

Homeland Security

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS P10.

[b6 b2]

From: [b6 b2]
Sent: Friday, September 23, 2005 2:20 PM
To: [b6 b2]
Cc:
Subject: Cyber Storm 2005: Data Call on IT Systems

I have had conversations with many of you concerning the participation of the IT infrastructure and incident response teams of your department or agency in the Cyber Storm Exercise. As part of the exercise, among the other scenario events we will be simulating cyber attacks directly on State and Federal Government IT Infrastructures. If this kind of direct attack falls within the training objectives of your organization, the Final Planning Conference will be one of the last times for you to indicate this requirement. Also, as part of the breakout sessions in next week's conference, we will be meeting to discuss these nature and extent of these simulated attacks. If your agency would like to participate in this portion of the exercise we will need some additional information in order to prepare the scenario. Please come to the FPC with answers to as many of these questions as possible in order to speed development process in this area.

I'm looking forward to meeting with all of you this coming Monday.

Thanks,
[b6 b2]
NCE Exercise Director
[b2]
In Support of DHS/NCSD
Office
Mobile [b2]
[b2 b6] dhs.gov

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

[b6, b2]

P/4.

From: [b6 b2]
Sent: Friday, October 07, 2005 11:14 AM
To: [b6 b2] v;

Subject: Corrected -- Cyber Storm National Cyber Exercise

On Behalf of Andy Purdy
Acting Director, National Cyber Security Division
Department of Homeland Security

Cyber Storm Stakeholders and Participants:

First, thank you for your contributions to a very successful planning conference two weeks ago. We made tremendous progress and the scenario is well in hand.

One fact of life is that the real world events of today take precedence over training for the events of tomorrow. Unfortunately, the recent hurricanes significantly impacted a number of our key federal and private sector players. As a consequence they have been forced to devote their energy toward recovery efforts and cannot fully participate in the Cyber Storm exercise. The absence of these stakeholders and participants would undoubtedly impact the ability of the exercise to meet all of its key objectives.

For this reason, we have decided to delay Cyber Storm until February 6-10, 2006. This will provide sufficient time to reprogram the resources and efforts required to make Cyber Storm a success for all participants.

In support of the new timeline, we will host an additional Scenario Planning Conference on November 15-16 at [b2] Our Final Master Scenario Event List (MSEL) Conference (a line by line walk through with exercise control cell and SMEs) will be held January 19-20, also at [b2] During the MSEL Conference we will also have the control cell training on NXMSEL system.

We appreciate your commitment to Cyber Storm and look forward to your continued participation.

TRANSFERRED TO OTHER AGENCY P15.
[b6 b2] TRANSFER FOR DIRECT REPLY - DHS

From: [b6 b2]
Sent: Wednesday, October 19, 2005 9:35 PM
To: [b6 b2]

Subject: Scenario Planning Conference Invitation

October 17, 2005

MEMORANDUM FOR: Exercise Cyber Storm Stakeholders

FROM: Andy Purdy, Acting Director, National Cyber Security Division

SUBJECT: Exercise Cyber Storm Scenario Planning Conference

You are invited to participate in the Scenario Planning Conference (SPC) for Exercise Cyber Storm, the National Cyber Exercise sponsored by the Department of Homeland Security – National Cyber Security Division (DHS-NCSD). The SPC will be held on November 15-16, 2005 at the [b2]

Exercise Cyber Storm is designed to exercise, evaluate, and improve communication, coordination, and procedures between DHS, other government agencies, the public and private sector, and with select foreign partners to gain an understanding of critical cyber security weaknesses and capabilities in the homeland security environment. Specifically, Exercise Cyber Storm will exercise and evaluate the National Cyber Alert System, coordinate Federal response under the Cyber Annex to the National Response Plan, emphasize public/private cooperation and communications, and examine mechanisms for intra-governmental coordination with state and international governments in a scenario of cyber incidents within the energy, information technology, telecommunications and transportation sectors. Exercise Cyber Storm, which will be based out of Washington, DC, will be held February 6-10, 2006. The current planning schedule is listed on the second page for your reference.

The primary goals of the SPC are to continue to refine the scenario timing and coordination of events developed during the September Final Planning Conference as well as to develop and provide the detailed scenario event implementers necessary to affect this scenario during the February exercise. This meeting will focus on scripting the particular implementers and should be attended by trusted agents for each participating organization and subject matter experts from key elements and organizations of the affected infrastructures. Discussions and products for this conference are designated For Official Use Only, and should not be distributed beyond those in attendance. The agenda and planning materials will be sent out prior to the planning conference.

Please RSVP using the event registration website [b2] no later than COB Thursday, November 10. Local lodging information is also posted at that site. If you have any questions, please [b6 b2]

Attachment: Exercise Cyber Storm Planning Schedule

EXERCISE CYBER STORM

PLANNING SCHEDULE

Shareholder input gathering	January – Early February 2005
Development of sector-specific scenario themes reflecting shareholder objectives	February 2005
Initial Planning Conference	March 1, 2005
Scenario development working group integrates draft detailed scenario	April 2005
Midterm Planning Conference	May 24-25, 2005
Final Planning Conference	September 7-8, 2005
First Dry Run	October 3-4, 2005
Scenario Planning Conference	November 15-16, 2005
MSEL Conference & Systems Test	January 19-20, 2006
Conduct Exercise	February 6-10, 2006
Develop After Action Report	March-April 2006

P19

Withheld in Full

b2 b5 b6

2 Pages

P26

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

December 12, 2005

MEMORANDUM FOR: Exercise Cyber Storm Stakeholders

FROM: Andy Purdy, Acting Director, National Cyber Security Division

SUBJECT: Exercise Cyber Storm Final MSEL Conference

Dear RECIPIENT,

You are cordially invited to participate in the Final MSEL Conference (FMC) for Exercise Cyber Storm, the National Cyber Exercise sponsored by the Department of Homeland Security – National Cyber Security Division (DHS-NCSD). The FMC will be held on January 19-20, 2006 at the [b2]

[b2] This is an **invitation-only event** and is intended for observer/controllers that will be working from the Exercise Control cell at [b2] or at their home organization location. If you cannot attend, please so advise and, if appropriate, include a nomination for your replacement.

Exercise Cyber Storm is designed to exercise, evaluate, and improve communication, coordination, and procedures between DHS, other government agencies, the public and private sector, and with select foreign partners to gain an understanding of critical cyber security weaknesses and capabilities in the homeland security environment. Specifically, Exercise Cyber Storm will exercise and evaluate the National Cyber Alert System, coordinate Federal response under the Cyber Annex to the National Response Plan, emphasize public/private cooperation and communications, and examine mechanisms for intra-governmental coordination with state and international governments in a scenario of cyber incidents within the energy, information technology, telecommunications and transportation sectors. Exercise Cyber Storm, which will be based out of Washington, DC, will be held February 6-10, 2006. The current planning schedule is listed on the second page for your reference.

The primary goals of the FMC are to continue to finalize the timing and coordination of the MSEL developed during the November Scenario Planning Conference. This meeting will focus on reviewing the particular implementers as well as conduct exercise controller training in advance of the exercise itself. Discussions and products for this conference are designated For Official Use Only, and should not be distributed beyond those in attendance. A detailed agenda will be posted on the Cyber Storm Portal for those who are attending the conference.

Please RSVP to [b6 b2] or [b2 b6].dhs.gov no later than COB Friday, January 13. A block of hotel rooms has been secured at the government per diem rate of $187 at the Embassy Suites, 900 10th Street, NW. To secure your room, you must call Embassy Reservations at 1-800-EMBASSY and mention 'National Cyber Exercise - Cyber Storm' by December 19, 2005. The block will be released after that date.

P22

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

Agenda for the NCRCG Preparation Exercise II
January 05, 2006

[b2]

0730: Participant check-in

[b2]

0800: Introductions and administrative remarks

0815: Exercise overview and review of SOP

0845: NCRCG stand-up triggers

0915: Break

0930: Begin Scenario 1

1100: Break

1115: Begin Scenario 2

1215: Break and working lunch service

1245: Begin Scenario 3

1330: Recap of exercise [b2]

1400: End of exercise

P228

Homeland Security

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

December 16, 2005

MEMORANDUM FOR:

National Cyber Response Coordination Group
Interagency Incident Management Group
Director, Homeland Security Operations Center

FROM: Jeff Wright, National Cyber Security Division Exercise Program

SUBJECT: Cyber Storm Preparation Exercise, January 05, 2006

This memorandum is to invite your organization to participate in the Cyber Storm Preparation Exercise II (PrepEx II), sponsored by the Department of Homeland Security – National Cyber Security Division (DHS-NCSD). This tabletop exercise (TTX) is the fifth exercise in the National Cyber Response Coordination Group (NCRCG) series and the second exercise specifically intended to serve as a building block for Cyber Storm full scale exercise (FSE) scheduled for February, 2006.

PrepEx II will be held on January 05 2006, from 8:00 a.m. to 2:00 p.m., at the Department of [b2] This TTX will be a joint exercise with the National Cyber Response Coordination Group (NCRCG) and US-Computer Emergency Readiness Team (US-CERT), as well as select representatives from the Interagency Incident Management Group (IIMG) and Homeland Security Operations Center (HSOC).

PrepEx II is focused on further development and coordination of the operational procedures and standard operating processes that will be exercised during the Cyber Storm FSE in February 2006. The TTX objectives are:

- Provide the NCRCG an opportunity to review and refine their initiation triggers and procedures
- Review the current Standard Operating Procedures (SOP)
- Execute and evaluate NCRCG stand-up and initial procedures
- Coordinate procedures with the IIMG and HSOC
- Identify specific actions required prior to Cyber Storm FSE

Please provide the name, phone number, and email address of the individual(s) who will represent your department or agency at the TTX to [b6 b2] no later than COB December 29, 2005.

Attachment:
Agenda

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

P 33K

CYBER STORM
EXERCISE QUICK START GUIDE
February 6–10, 2006

EXERCISE KICK-OFF TELECONFERENCE: Mon. Feb. 6 at 1140 EST (1640 GMT)
Call-In Number:
Participant ID: [b2]

DAILY SCHEDULE OF EXERCISE PLAY

	Mon. Feb. 6 Day 1	Tue. Feb. 7 Day 2	Wed. Feb. 8 Day 3	Thu. Feb. 9 Day 4	Fri. Feb. 10 Day 5
Observers / Controllers	[b2]				
Players/ Participants					

[b2]

Cyber Storm in the Media

An organization may respond to inquiries on their participation during the exercise. Responses should be channeled through the organization's public affairs office. All other media inquiries such as those pertaining to the exercise itself, other participants, or DHS role, *contact the* *DHS Press Office at 202-282-8010.*

CYBER STORM COMMUNICATIONS

1. The following should appear on all e-mail communications:
- Insert [b2] on all e-mail correspondence as a CC.
- Only send e-mail correspondence to or from Cyber Storm Exercise Control (ExCon) and between players and other organizations.
- Include the [b2] on all originals, replies, and forwarded correspondence.
1. [b2] users participating in the Cyber Storm exercise should include the following e-mail address in all correspondences: [b2]
2. Other communications such as phone, secure phones, faxes, CWIN, HSIN Portal, and US-CERT portal should be recorded by an observer/controller.
3. See the reverse side of this sheet for communications protocol and guidelines.

Using a Cyber Storm E-mail Account

1. Observer/Controller or Player: Use MS Outlook Web Access for all e-mail correspondence.
2. Web address: [b2]
3. Domain name: [b2]
4. User name: [b2]

NEED HELP? e-mail or call:	E-mail Address	Phone 202-406-xxxx
Exercise Help Desk	[b2]	
Technical Support	[b2]	

Exercise Status Hot Line: [b2]

Password

1. Participants staged at the [b2] in Washington, DC will receive a password at pre-STARTEX.
2. Participants staged at a location other than the Cyber Storm Exercise Control facility in Washington, DC, will receive a password provided to them either by personal e-mail account or by telephone call.
3. Users who have not received a password should contact the network support desk at [b2] or at [b2] beginning Monday, February 6, 2006 at 0600 EST.

Communications Guidelines

- ❑ At the official beginning of exercise play (STARTEX), ExCon will send the following e-mail:

  EXERCISE CYBER STORM HAS COMMENCED

- ❑ At each PAUSEX and RESTARTEX, ExCon will transmit a message:

  EXERCISE CYBER STORM HAS PAUSED, EXPECTED RESTART IS SET FOR (0000 hours) ..... EXERCISE CYBER STORM HAS RESUMED

- ❑ At end of active play (ENDEX 1630 EST), ExCon will send the message:

  EXERCISE CYBER STORM HAS CULMINATED AS OF (0000 hours)

- ❑ When contacting another party during exercise play:
  1. Locate the person's contact information provided in the exercise directory (by name, sector, and organization).
  2. To reach a party or organization outside of the exercise perimeter who is not listed in the directory, call [b2] Give the switchboard operator the name of the person and/or organization you would normally contact in a real event. Industry experts and agency representatives will be connected to simulate the requested organization's response within the context of the game.

- ❑ Include the following subject line in all e-mail correspondence:

  EXERCISE CYBER STORM

- ❑ Begin and end all text messages with the banner:

  EXERCISE EXERCISE EXERCISE

- ❑ Clearly mark all written communications, such as faxes, paper memos, presentation slides, etc., at beginning and end of each message with the ***EXERCISE EXERCISE EXERCISE*** banner.

- ❑ Start and end all phone conversations by saying:

  THIS CALL IS PART OF CYBER STORM EXERCISE PLAY .....
  THANK YOU AND THIS ENDS THE EXERCISE INJECT.

- ❑ For all communications, avoid the use of participating company/entity names in order to maintain anonymity, i.e., [b2]

- ❑ For technical support, call the Exercise Help Desk at [b2] or e-mail [b2]

- ❑ For questions about exercise rules, play, and protocol, call Network Support at [b2] or e-mail [b2]

P33

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

Primary Contact List

For the below organizations, please use the following information for their primary points of contact.

Organization	Name	Role	Phone	E-mail
American Red Cross	ARC Other	Subject Matter Expert		
[b2]	[b2]			
[b2]				
Communications ISAC				
Department of Homeland Security / National Communications System (NCS)	Manager NCC	MGR NCC		
Department of Homeland Security / National Cyber Security Division / US-CERT	Operations Center			
Information Technology ISAC*	SME	IT-ISAC Operations Center		
[b2]	[b6]	[b4 b2]		
	[b6]	Technical Operations Center	b2	b2 b6
	[b2]	Subject Matter Expert		
		Subject Matter Expert		
		Subject Matter Expert		
		Subject Matter Expert		
MS-ISAC*	Operations Center			
[b4 b2]	[b6]	[b2]		

P33C

NATIONAL CYBER EXERCISE
CYBER STORM
Player Directory

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

February 6–10, 2006

Department of Homeland Security
National Cyber Security Division

This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR EXERCISE USE ONLY

Cyber Storm Player Directory
By ORGANIZATION

* denotes CWIN capability

Organization	Name	Role	Phone	E-mail
[b2]	[b2]			
American Red Cross	ARC Other	Subject Matter Expert		
American Red Cross		Office of the Chief Information Security Officer		
American Red Cross	b6	Office of the Chief Information Security Officer		
American Red Cross		Manager, [b2]		
American Red Cross		System Admin		
American Red Cross		System Admin		
American Red Cross		NetOps Manager		
Australia	Operations Center			
Australia		All other roles		
[b2]	[b2]		b2	b2 b6
[b2]	[b2]			
[b2]				
[b2]	b6			
Canada		All other roles		
Canada, [b2] [b2]				

Organization	Name	Role	Phone	Email
Canada [b2]				
Canada [b2]				
Canada [b2]				
Canada [b2]				
Canada [b2]				
Canada [b2]				
Canada [b2]				
Canada [b2]				
Canada [b2]				
Canada [b2]				
Canada [b2]				
Canada [b2]				
Canada [b2]				
Canada [b2]				
Canada [b2]				

b6

b2

b2
b6

Organization	Name	Role	Phone	E-mail
Central Intelligence Agency / [b2]	[redacted] b6	NCRCG	[redacted]	[redacted]
Central Intelligence Agency / [b2]	[redacted]	NCRCG		
[b2]	[b2]			com
Communications ISAC				
[b4 b2]	[redacted]	Public Affairs		
[b2]		NCRCG		
		NCRCG		
		NCRCG		
Department of Commerce		NCRCG		
Department of Commerce / [b2]		Acting DPAS Program Manager		
Department of Commerce / [b2]	b6		b2	b2 b6 b4
Department of Commerce / [b2]		Senior Staff Officer		
Department of Commerce / NTIA		Chief, Emergency Planning & Policy (COOP Director)		
Department of Commerce / NTIA	[redacted]	NCRCG		
Department of Defense	DoD Other	Subject Matter Expert		
Department of Defense / OSD (NII)-IA	[b6]	NCRCG	[redacted]	[redacted]

Organization	Name	Role	Phone	E-mail
Department of Defense / JCS [b2]		NCRCG		
Department of Defense / JTF-GNO*	b6			
Department of Defense / JTF-GNO*		NCRCG		
Department of Defense / JTF-GNO*	[b2]			
Department of Defense / JTF-GNO* [b2]		NCRCG		
Department of Defense / JTF-GNO* [b2]		NCRCG		
Department of Defense / JTF-GNO* [b2]		NCRCG		
Department of Defense / OSD / NII	b6	NCRCG		
Department of Defense / OSD / NII		NCRCG	b2	b2 b6
Department of Defense / OSD / NII		NCRCG		
Department of Energy / [b2]	[b2] Hotline	[b2] Hotline		
Department of Energy [b2]				
Department of Energy [b2]	b6			
Department of Energy [b2]				

Organization	Name	Role	Phone	Email
Department of Energy [b2]	Network Security Team		[redacted]	[redacted]
Department of Energy [b2]	[b6]			
Department of Energy [b2]	Watch Officer			
Department of Energy [b2]	[b6]			
Department of Energy*	DOE Other	Subject Matter Expert		
Department of Energy*	[redacted]	NCRCG		
Department of Energy*		NCRCG		
Department of Health and Human Services		NCRCG		
Department of Health and Human Services		NCRCG	b2	
Department of Homeland Security / HSOC*		NSA Desk Officer		b2 b6
Department of Homeland Security / HSOC*	b6	NSA Desk Officer		
Department of Homeland Security / HSOC*		NSA Desk Officer		
Department of Homeland Security / ICE		NCRCG		
Department of Homeland Security / ICE		NCRCG		
Department of Homeland Security / Infrastructure Partnerships Division (IPD)*		IT, Telecom		gov
Department of Homeland Security / Infrastructure Partnerships Division (IPD)*	[redacted]	CWIN	[redacted]	[redacted]

Organization	Name	Role	Phone	E-mail
Department of Homeland Security / Infrastructure Partnerships Division (IPD)*		Hurricanes, NRCC, GIS POC		
Department of Homeland Security / Infrastructure Partnerships Division (IPD)*				
Department of Homeland Security / Infrastructure Protection Division / ICAO		Energy Sector Specialist		
Department of Homeland Security / Infrastructure Protection Division / ICAO		Aviation		
Department of Homeland Security / Infrastructure Protection Division / ICAO	b6	Financial	b2	
Department of Homeland Security / Infrastructure Protection Division / ICAO		IT, Telecom, NCRCG		b2 b6
Department of Homeland Security / National Communications System (NCS)		NCC		
Department of Homeland Security / National Communications System (NCS)	Manager NCC	MGR NCC		
Department of Homeland Security / National Communications System (NCS)	NCC Industry	NCC Industry		

Organization	Name	Role	Phone	Email
Department of Homeland Security / National Communications System (NCS)	NCC Watch	NCC Watch		
Department of Homeland Security / National Communications System (NCS)	NCC Watch			
Department of Homeland Security / National Communications System (NCS)	NCS Other	Subject Matter Expert		
Department of Homeland Security / National Communications System (NCS)		NCRCG		
Department of Homeland Security / National Communications System (NCS)		NCRCG	b2	b2 b6
Department of Homeland Security / National Cyber Security Division	b6	NCRCG		
Department of Homeland Security / National Cyber Security Division		NCRCG		
Department of Homeland Security / National Cyber Security Division		NCRCG		
Department of Homeland Security / National Cyber Security Division		NCRCG		

Organization	Name	Role	Phone	Email
Department of Homeland Security / National Cyber Security Division	[redacted]	NCRCG Support	[redacted]	[redacted]
Department of Homeland Security / National Cyber Security Division		NCRCG Support		
Department of Homeland Security / National Cyber Security Division		NCRCG		
Department of Homeland Security / National Cyber Security Division	b6	NCRCG		
Department of Homeland Security / National Cyber Security Division / O&A		NCRCG Support		b2
Department of Homeland Security / National Cyber Security Division / US-CERT		NCRCG	b2	b6
Department of Homeland Security / National Cyber Security Division / US-CERT	[redacted]	NCRCG		gov
Department of Homeland Security / National Cyber Security Division / US-CERT	Operations Center			
Department of Homeland Security / National Cyber Security Division / US-CERT	US-CERT Other	Subject Matter Expert		
Department of Homeland Security / National Cyber Security Division / US-CERT	[redacted] b6 [redacted]	NCRCG	[redacted]	[redacted]

Organization	Name	Role	Phone	E-mail
Department of Homeland Security / National Infrastructure Coordinating Center (NICC)*		Watch Supervisor		
Department of Homeland Security / National Infrastructure Coordinating Center (NICC)*		NICC Watch		
Department of Homeland Security / Office of Infrastructure Protection		Infrastructure Liaison (Day)		
Department of Homeland Security / Office of Infrastructure Protection		NCRCG		
Department of Homeland Security / Office of Infrastructure Protection / Contingency Planning & Support Division	b6	Senior Federal Official	b2	b2 b6
Department of Homeland Security / Office of Infrastructure Protection / Contingency Planning & Support Division		Senior Federal Official		
Department of Homeland Security / Office of Infrastructure Protection / HITRAC				
Department of Homeland Security / Office of Infrastructure Protection / HITRAC				

Organization	Name	Role	Phone	E-mail
Department of Homeland Security / Office of Infrastructure Protection / HITRAC				
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell		Director		
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell / Planning Cell		CNPPD (Alternate)		
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell / Planning Cell	b6	CNPPD	b2	b2 b6
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell / Planning Cell		RMD (Night)		
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell / Planning Cell		CNPPD (Alternate)		
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell / Planning Cell		RMD		

Organization	Name	Role	Phone	Email
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell / Planning Cell		HITRAC		
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell / Planning Cell		HITRAC		
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell / Planning Cell		CNPPD (Alternate)		
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell / Planning Cell	b6	RMD (Day)	b2	b2 b6
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell / Planning Cell		IPD		
Department of Homeland Security / Office of Infrastructure Protection / Risk Management Division		RMD Operations Cell (Day)		
Department of Homeland Security / Office of Infrastructure Protection / Risk Management Division		RMD Operations Cell (Night)		

Organization	Name	Role	Phone	E-mail
Department of Homeland Security / Office of Intelligence & Analysis		Portfolio Manager - Cyber Threat		
Department of Homeland Security / Office of Intelligence & Analysis		Cyber Analyst		v
Department of Homeland Security / Office of International Affairs	b6	Public Affairs		
Department of Homeland Security / Office of the General Counsel				
Department of Homeland Security / Protected Critical Infrastructure Information Program (PCIIP)			b2	b2
Department of Homeland Security / Public Affairs	DHS PA Ready Room			b6
Department of Homeland Security / Public Affairs	b6	NCRCG		
Department of Homeland Security / Transportation Security Administration		Public Affairs		ıv
Department of Homeland Security / Transportation Security Administration	Transportation Security Intelligence Service (TSIS)			
Department of Homeland Security / Transportation Security Administration	Transportation Security Operations Center (TSOC)			
Department of Homeland Security / Transportation Security Administration	TSA Other	Subject Matter Expert		

Organization	Name	Role	Phone	E-mail
Department of Homeland Security / United States Secret Service		Public Affairs		
Department of Homeland Security / United States Secret Service		NCRCG		
Department of Homeland Security / United States Secret Service		NCRCG		
Department of Homeland Security / United States Secret Service		CID		
Department of Homeland Security / United States Secret Service		NCRCG		
Department of Justice	b6	NCRCG	b2	
Department of Justice		Public Affairs		b2
Department of Justice / CCIPS		NCRCG		
Department of Justice / CCIPS		NCRCG		b6
Department of Justice / CCIPS		NCRCG		
Department of State		Public Affairs		
Department of State				
Department of State		NCRCG		
Department of State				
Department of State		NCRCG		
Department of State		NCRCG		

Organization	Name	Role	Phone	Email
Department of the Treasury*	[redacted]	NCRCG	[redacted]	[redacted]
Department of the Treasury*	b6	NCRCG		
Department of the Treasury*	[redacted]	NCRCG		
Department of Transportation [b2]	[redacted] b2	Help Desk and Developer		
Department of Transportation [b2]		IT Security Analyst		
Department of Transportation*	[b2]			b2
Department of Transportation*	DOT Other	Subject Matter Expert		b6
Department of Transportation*	[redacted]	NCRCG	b2	
Department of Transportation*		NCRCG		
Department of Transportation*	b6	NCRCG		
Department of Transportation*	[redacted]	NCRCG		
Department of Transportation*	[b2]			
Department of Transportation*	[b6]	NCRCG	[redacted]	[redacted]

Organization	Name	Role	Phone	Email
Director of National Intelligence / Intelligence Community Incident Response Center	[b6]	Acting Unit Chief		
Director of National Intelligence / Intelligence Community Incident Response Center	SIAO Watch Desk			
Director of National Intelligence / Intelligence Community Incident Response Center	[b6]	NCRCG		
[b4 b2] [b4 b2] [b2]	[b2]	[b4 b2]	b2	m
Electricity Sector Information Sharing Analysis Center (ESISAC)*	[b6]			
Electricity Sector Information Sharing Analysis Center (ESISAC)*	ESISAC Duty	Operations Center		b2 b6 b4
Electricity Sector Information Sharing Analysis Center (ESISAC)*				
Electricity Sector Information Sharing Analysis Center (ESISAC)*	b6			
Electricity Sector Information Sharing Analysis Center (ESISAC)*				
[b2]				

Organization	Name	Role	Phone	E-mail
[b2]	[b6]	[b2] Manager		
Federal Aviation Administration*	[b2]			
Federal Aviation Administration*	FAA Other	Subject Matter Expert		
Federal Aviation Administration*	[b2]			
Federal Aviation Administration*	[b6]	NCRCG		
Federal Aviation Administration*	[b2]			
Federal Aviation Administration [b2]		NCRCG		
Federal Bureau of Investigation (FBI)		NCRCG	b2	b2 b6
Federal Bureau of Investigation (FBI)		Field Offices		
Federal Bureau of Investigation (FBI)		Public Affairs		
Federal Bureau of Investigation (FBI)	b6	Analyst		
Federal Bureau of Investigation (FBI)		NCRCG		
Federal Deposit Insurance Corporation (FDIC)		Security Director		
Federal Deposit Insurance Corporation (FDIC)		Management Review		

Organization	Name	Role	Phone	E-mail
[b2]				
Federal Reserve Bank of NY				
Federal Reserve Bank of NY				
Federal Reserve Bank of NY		Subject Matter Expert		
Federal Reserve Bank of NY	b6			
Federal Reserve Bank of NY				
FS-ISAC		Security Operations Center		
FS-ISAC		Subject Matter Expert		
[b4 b2]				
[b2]	[b4 b2]			b2
Homeland Security Council		NCRCG		b6
[b2]	b6		b2	b4
Information Technology ISAC				
Information Technology ISAC*	IT-ISAC Operations Center			
Information Technology ISAC*	b6			
Information Technology ISAC				
Information Technology ISAC*	IT-ISAC Other	Subject Matter Expert		
[b2]		Information Technology Lead Technical Analyst		
	b6			
[b2]		[b2] Operator 1		

Organization	Name	Role	Phone	Email
	b6	[b2] Operator 2		
		[b2] Operations Center		
	[b2]	Subject Matter Expert		
		Response for [b2]		
		[b2] Operations Center		
		Response for [b2]		
	b6			
		[b2]		b2
b2		[b2] Public Affairs	b2	b6
		[b2] Public Affairs		
	[b2]	Subject Matter Expert		
		Public Affairs		
		[b2]		
	b6	Technical Operations Center		
		Information Security		
		Information Security		
	[b2]	Subject Matter Expert		

Organization	Name	Role	Phone	E-mail
	[b6]	Director [b2]		
	[b2]	Subject Matter Expert		
	[b6]	[b2] Center		
	[b2]	Subject Matter Expert		
		[b2] Center		
b2		[b2]		
	b6	Center		
		[b2] Center	b2	b2 b6
		[b2] Center		
	[b2]	Subject Matter Expert		
[b4 b2] [b2]	[b4 b2]			
Michigan	b6	Public Affairs		
Michigan		Public Affairs		
Michigan*	Operations Center			
Montana	[b6]	Public Affairs		
Montana*	Operations Center			

Organization	Name	Role	Phone	Email
MS-ISAC*	Operations Center			
[b2]	[redacted]	NCRCG	[redacted]	
National Security Agency / [b2]	b6			[redacted]
National Security Agency / NTOC		NCRCG		
National Security Agency / NTOC	[redacted]	NCRCG		
National Security Agency / NTOC	Senior Threat Watch Officer			
National Security Agency*	[redacted]	NCRCG		
National Security Council	b6	NCRCG	b2	
National Security Council / [b2]	[redacted]	NCRCG		
New York*	Operations Center			b2 b6
New Zealand	Operations Center			
New Zealand		All other roles		
NORTHCOM*	[b6]	Public Affairs		
NORTHCOM*	[b2]			
NORTHCOM*				
Office of Management and Budget [b2]	[b6]	NCRCG		
[b2]			[redacted]	[redacted]

Organization	Name	Role	Phone	E-mail
	[b2]	[b2] Coordinator 1		
		[b2] Coordinator 2		
		Information Technology		
b2	b6	Communications		
		Public Affairs		
		Public Affairs / Media Contact		
		Security		
	Media Relations			b2 b6 b4
	Operations Shift Supervisor		b2	
	[b2] Coordinator			
	b6			
	Operations Center			
	b6			
[b4] b2		[b2] Center		

Organization	Name	Role	Phone	E-mail
[b4 b2]		[b2] Center		
		Public Affairs		
		Operations		
	b6	Information Technology		b2
		Operations		b6
b2		Information Technology		
		Information Technology	b2	
		Security		
		Public Affairs		om
		Operations		n
		Operations		n
	[b2] Operator	Operations Center A		n
	[b2] Operator	Operations Center B		n
	[b6]	System Operations-TO		

Organization	Name	Role	Phone	E-mail
[redacted]	[b6]	System Operations-TO	[redacted]	[redacted]
b2	Emergency Command Center			
	[redacted]	[b2]		
	b6	[b2]		
	[redacted]	Security		
[redacted]				b2
United Kingdom		All other roles	b2	
United Kingdom [b2]	Analyst			b6
United Kingdom [b2]	Analyst b2			
United Kingdom / NISCC / [b2]	[redacted]			
[b2]		NCRCG		
[b2]	b6			
[b2]		[b2] Operations		
[b2]	[redacted]	Cyber Security Program Manager	[redacted]	[redacted]

FOR ~~EXERCISE USE~~ ONLY

Cyber Storm Player Directory
BY NAME

* denotes CWIN capability

Organization	Name	Role	Phone	E-mail
Australia		All other roles		
Canada		All other roles		
Canada / [b2]				
Canada [b2]				
Canada [b2]				
Canada [b2]				b2 b6
Canada [b2]				
Canada [b2]			b2	
Canada [b2]				
Canada [b2]				
Canada [b2]				
[b2]				
Communications ISAC				
[b4 b2]				

Organization	Name	Role	Phone	E-mail
[b2]				
[b2]				
[b4 b2]				
[b2]				
New Zealand		All other roles		
		[b2] Coordinator 2		
	b2	Information Technology	b2	b2
		Communications		b6
		Operations		b4
		Information Technology		
United Kingdom		All other roles		
[b2]				
Department of Homeland Security / Office of the General Counsel	[b6]			

Organization	Name	Role	Phone	E-mail
[b2]	[b2]			
[b2]	[b6]	System Operations-TO		
Information Technology ISAC*	IT-ISAC Operations Center			
[b4 b2]	[b6]	[b2] Center		
United Kingdom [b2]	Analyst [b2]			
United Kingdom [b2]	Analyst			
[b2]	[b6]	Public Affairs		b2
American Red Cross	ARC Other	Subject Matter Expert		
Department of Justice / CCIPS	[b6]	NCRCG	b2	b6
[b2]	[b2]			
National Security Council		NCRCG		
Information Technology ISAC				
American Red Cross	b6	Office of the Chief Information Security Officer		
Department of Defense / JTF-GNO* [b2]		NCRCG		
American Red Cross		Office of the Chief Information Security Officer		
Department of Commerce / NTIA		Chief, Emergency Planning & Policy (COOP Director)		

Organization	Name	Role	Phone	E-mail
[b2]		[b2] Coordinator 1		
Department of Energy [b2]				
Department of Homeland Security / HSOC*		NSA Desk Officer		
Federal Reserve Bank of NY				
Department of Homeland Security / ICE		NCRCG		
Federal Deposit Insurance Corporation (FDIC)		Security Director		b2
Federal Reserve Bank of NY	b6			b6
[b2]			b2	
Department of Homeland Security / Infrastructure Protection Division / ICAO		Energy Sector Specialist		
[b2]		NCRCG		
National Security Agency / [b2]				
[b2]		[b2]		
[b2]	[b2]			
Federal Bureau of Investigation (FBI)	b6	NCRCG		
Department of Homeland Security / United States Secret Service		Public Affairs		

Organization	Name	Role	Phone	E-mail
Department of Energy / [b2]	[b2] Hotline	[b2] Hotline		
[b4 b2]		[b2] Center		
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell / Planning Cell	b6	CNPPD (Alternate)		
Department of Commerce / NTIA		NCRCG		
Department of Homeland Security / Transportation Security Administration		Public Affairs		b2
Department of Defense / JTF-GNO*	Command Duty Officer		b2	b6
Department of Homeland Security / National Cyber Security Division	b6	NCRCG		
Electricity Sector Information Sharing Analysis Center (ESISAC)*				
Department of Transportation*	[b2]			
Federal Bureau of Investigation (FBI)	b6	Field Offices		
Department of Homeland Security / Office of Infrastructure Protection		Infrastructure Liaison (Day)		

Organization	Name	Role	Phone	Email
Federal Aviation Administration*	[b2]			
Department of Homeland Security / United States Secret Service	b6	NCRCG		
[b2]		NCRCG		
[b2]	[b2]			
Department of Commerce / [b2]	[b6]	Acting DPAS Program Manager		
[b4 b2]	[b2]	[b4 b2]		
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell / Planning Cell	[b6]	CNPPD	b2	b2
Department of Homeland Security / Public Affairs	DHS PA Ready Room			b6
[b2]	b6	System Operations-TO		b4
Department of Homeland Security / National Cyber Security Division / US-CERT		NCRCG		
Department of Defense	DoD Other	Subject Matter Expert		
Department of Energy*	DOE Other	Subject Matter Expert		
[b2]	b6	Information Technology Lead Technical Analyst		
Central Intelligence Agency / [b2]		NCRCG		

Organization	Name	Role	Phone	E-mail
Department of Transportation*	DOT Other	Subject Matter Expert		
[b2]		Public Affairs / Media Contact		
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell / Planning Cell	b6	RMD (Night)		
Department of Justice / CCIPS		NCRCG		
[b2]	Emergency Command Center			
Department of Homeland Security / Infrastructure Protection Division / ICAO	b6	Aviation	b2	
Department of Energy [b2]				b2
Electricity Sector Information Sharing Analysis Center (ESISAC)*	ESISAC Duty	Operations Center		b6
[b2]	[b6]	[b2] Center		m
Federal Aviation Administration*	FAA Other	Subject Matter Expert		
Department of Homeland Security / Infrastructure Partnerships Division (IPD)*	b6	IT, Telecom		gov
[b2]		[b2]		

Organization	Name	Role	Phone	E-mail
National Security Agency / NTOC		NCRCG		
Department of Energy [b2]				
Department of Homeland Security / National Cyber Security Division / O&A	b6	NCRCG Support		
Department of Homeland Security / Office of Infrastructure Protection / HITRAC [b2]		[b2]		
Department of Homeland Security / Office of Infrastructure Protection / Contingency Planning & Support Division		Senior Federal Official	b2	
[b2]	[b4 b2]			b2
[b2]				
[b2]	b6	NCRCG		b6
Federal Aviation Administration* [b2]		NCRCG		b4
Michigan		Public Affairs		
[b2]	[b2]			m
[b2]		Public Affairs		
Central Intelligence Agency / [b2]	b6	NCRCG		
[b2]		IT-Business		

Organization	Name	Role	Phone	E-mail
Federal Deposit Insurance Corporation (FDIC)		Management Review		
[b2]		[b2]		
		Operations		
Department of Energy Office of Energy Reliability				
[b2]				
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell		Director		
Department of Health and Human Services		NCRCG		
Department of Defense / OSD / NII		NCRCG		
National Security Agency / NTOC	b6	NCRCG	b2	
Department of Homeland Security / HSOC*		NSA Desk Officer		b2 b6
Department of State		Public Affairs		
Information Technology ISAC*				
Department of Homeland Security / Office of Intelligence & Analysis		Portfolio Manager - Cyber Threat		
[b2]		Security		
Department of Homeland Security / National Cyber Security Division / US-CERT		NCRCG		gov
[b2]				

Organization	Name	Role	Phone	E-mail
Department of Homeland Security / Protected Critical Infrastructure Information Program (PCIIP)				
National Security Council / [b2]		NCRCG		
Department of State [b2]				
Department of Homeland Security / United States Secret Service	b6	NCRCG		b2
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell / Planning Cell		CNPPD (Alternate)	b2	b6
Department of Commerce [b2]		NCRCG [b2] Manager		
Information Technology ISAC*	IT-ISAC Other	Subject Matter Expert		
Department of Transportation*		NCRCG		
Department of Defense / OSD / NII	b6	NCRCG		
Department of Commerce / [b2]				

Organization	Name	Role	Phone	E-mail
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell / Planning Cell		RMD		
Office of Management and Budget [b2]		NCRCG		
Electricity Sector Information Sharing Analysis Center (ESISAC)*				
Department of Energy*		NCRCG		
Department of Homeland Security / National Cyber Security Division	b6	NCRCG		
Canada [b2]			b2	
Department of Defense / JTF-GNO* [b2]		NCRCG		b2 b6
Electricity Sector Information Sharing Analysis Center (ESISAC)*				
[b2]		Public Affairs		
Department of Homeland Security / HSOC*		NSA Desk Officer		
[b2]		Information Technology		
[b2]		[b2] Center		

Organization	Name	Role	Phone	E-mail
Department of Homeland Security / Office of Infrastructure Protection / Contingency Planning & Support Division		Senior Federal Official		
[b2]		Public Affairs		
Information Technology ISAC				
Department of Health and Human Services		NCRCG		
Department of Homeland Security / National Cyber Security Division		NCRCG		
[b2]		[b2] Operations Center		b2
Department of Homeland Security / United States Secret Service	b6	CID	b2	b6
American Red Cross		Manager, [b2]		
Department of Justice		NCRCG		
[b2]		Information Technology		
Department of Homeland Security / Office of Infrastructure Protection / HITRAC				
Department of Homeland Security / National Communications System (NCS)		NCC		

Organization	Name	Role	Phone	E-mail
[b2]	[b6]	Director [b2]	[ ]	[ ]
Department of Homeland Security / Infrastructure Protection Division / ICAO		Financial		
Department of Homeland Security / National Communications System (NCS)	Manager NCC	MGR NCC		
Department of Defense / OSD (NII)-IA	[ ]	NCRCG		
Department of State [b4 b2]		NCRCG Public Affairs		
Department of Homeland Security / National Cyber Security Division		NCRCG		
Department of Defense / JTF-GNO*		NCRCG	b2	b2
Department of Transportation* [b2]	b6	NCRCG Security		b6 b4
Department of Homeland Security / National Cyber Security Division		NCRCG Support		
Department of Homeland Security / Office of Infrastructure Protection [b2]	[ ]	NCRCG	[ ]	[ ]

Organization	Name	Role	Phone	E-mail
Department of Commerce / [b2]	[b6]	Senior Staff Officer		
[b2]	[b2]	Subject Matter Expert		
[b2]	Media Relations			
[b4 b2]	[b4 b2]			
[b2]		Response for [b2]		
Director of National Intelligence / Intelligence Community Incident Response Center	b6	Acting Unit Chief		
[b2]	[b2]	Subject Matter Expert		b2
Federal Bureau of Investigation (FBI)		Public Affairs	b2	b6
Canada [b2]				
American Red Cross		System Admin		
[b2]	b6	[b2] Center		
[b2]				
FS-ISAC		Subject Matter Expert		
Department of Transportation*		NCRCG		
[b2]	[b2]	Subject Matter Expert		
		Subject Matter Expert		

Organization	Name	Role	Phone	E-mail
[b2]	[b2]	Subject Matter Expert		
		Subject Matter Expert		
NORTHCOM*	[b6]	Public Affairs		
Department of Transportation [b2]	[b2]	Help Desk and Developer		
Department of Homeland Security / National Communications System (NCS)	NCC Industry	NCC Industry		
Department of Homeland Security / National Communications System (NCS)	NCC Watch	NCC Watch		
Department of Homeland Security / National Communications System (NCS)	NCC Watch		b2	b2 b6
Department of Homeland Security / National Communications System (NCS)	NCS Other	Subject Matter Expert		
Department of Defense / JTF-GNO*	[b2]			
Department of Energy [b2]	Network Security Team			
National Security Agency*	b6	NCRCG		
Electricity Sector Information Sharing Analysis Center (ESISAC)*				

Organization	Name	Role	Phone	E-mail
[b2]	[redacted]	Public Affairs	[redacted]	[redacted]
Department of the Treasury*		NCRCG		
Department of Homeland Security / Office of Infrastructure Protection / Risk Management Division	b6 [redacted]	RMD Operations Cell (Day)		
Federal Reserve Bank of NY	NY FRB Other	Subject Matter Expert		
Canada [b2]	[redacted]			
Department of Homeland Security / National Cyber Security Division	b6	NCRCG Support		b2
Department of Homeland Security / National Communications System (NCS)	[redacted]	NCRCG		b6
Federal Aviation Administration*	[b2]		b2	
Department of Homeland Security / ICE	[b6]	NCRCG		
Australia	Operations Center			[redacted]
Department of Homeland Security / National Cyber Security Division / US-CERT	Operations Center			
Michigan*	Operations Center			
Montana*	Operations Center			
MS-ISAC*	Operations Center			
New York*	Operations Center		[redacted]	

Organization	Name	Role	Phone	E-mail
New Zealand	Operations Center			
[b2]	Operations Center			
[b2]	[b2]			
[b2]		[b2] Operations Center		
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell / Planning Cell		HITRAC		
Department of Justice / CCIPS		NCRCG		b2
[b2]		[b2]	b2	b6
United Kingdom / NISCC / [b2]	b6			
[b2]		NCRCG		
[b2]		Technical Operations Center		
Department of Energy [b2]				
Department of the Treasury*		NCRCG		
[b2]				
Department of Homeland Security / National Infrastructure Coordinating Center (NICC)*		Watch Supervisor		

Organization	Name	Role	Phone	E-mail
Department of Transportation [b2]	[b2]	IT Security Analyst		
Department of Homeland Security / Infrastructure Partnerships Division (IPD)*		CWIN		
[b2]		Public Affairs		
[b2]				
Federal Reserve Bank of NY				
Department of Homeland Security / National Cyber Security Division	b6	NCRCG		
Department of Homeland Security / Infrastructure Partnerships Division (IPD)*		Hurricanes, NRCC, GIS POC		
Canada [b2]			b2	b2
[b2]		Operations Information Security		b6
Department of Homeland Security / National Infrastructure Coordinating Center (NICC)*	[b2]	NICC Watch		
Department of State	b6			
Department of State		NCRCG		
Federal Aviation Administration*		NCRCG		
American Red Cross		System Admin		

Organization	Name	Role	Phone	E-mail
Federal Reserve Bank of NY				
American Red Cross		NetOps Manager		
[b2]		NCRCG		
Department of the Treasury*	b6	NCRCG		
Department of State		NCRCG		
[b2]		[b2] Center		n
[b2]		Information Security		
Canada / [b2]				
Homeland Security Council		NCRCG		b2
National Security Agency / NTOC	Senior Threat Watch Officer		b2	b6
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell / Planning Cell	b6	HITRAC		
Department of Homeland Security / Public Affairs		NCRCG		
Director of National Intelligence / Intelligence Community Incident Response Center	SIAO Watch Desk			
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell / Planning Cell	[b6]	CNPPD (Alternate)		

Organization	Name	Role	Phone	E-mail
Department of Homeland Security / Infrastructure Partnerships Division (IPD)*				
Canada [b2]				
Department of Homeland Security / United States Secret Service		NCRCG		
Department of Homeland Security / National Cyber Security Division		NCRCG		
Department of Defense / JTF-GNO* [b2]		NCRCG		
Department of Homeland Security / Office of International Affairs	b6	Public Affairs		b2
[b2]		Response for [b2]	b2	b6
Department of Homeland Security / Office of Infrastructure Protection / Risk Management Division		RMD Operations Cell (Night)		
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell / Planning Cell		RMD (Day)		
[b2]		Security		
Federal Bureau of Investigation (FBI)		Analyst		

Organization	Name	Role	Phone	E-mail
Director of National Intelligence / Intelligence Community Incident Response Center		NCRCG		
Department of Justice	b6	Public Affairs		
Department of Defense / JCS [b2]		NCRCG		
[b2]		[b2] Operations		
NORTHCOM*	[b2]			
NORTHCOM*				b2
Federal Bureau of Investigation (FBI)	b6	NCRCG		b6
Department of Transportation*	ark	NCRCG		
[b2]	[b2]	Operations Center A	b2	n
		Operations Center B		n
Department of Transportation*	[b2]			
Department of Homeland Security / Transportation Security Administration	Transportation Security Intelligence Service (TSIS)			
Department of Homeland Security / Transportation Security Administration	Transportation Security Operations Center (TSOC)			

Organization	Name	Role	Phone	E-mail
Department of Homeland Security / Transportation Security Administration	TSA Other	Subject Matter Expert		
Department of Homeland Security / National Cyber Security Division / US-CERT	US-CERT Other	Subject Matter Expert		
Department of Transportation*	n	NCRCG		
[b2]		[b2] Operator 1		
[b2]	b6	[b2] Operator 2		
Department of Homeland Security / Office of Infrastructure Protection / HITRAC				b2 b6
Federal Aviation Administration*	[b2]		b2	
Department of Energy [b2]	Watch Officer			
Department of Homeland Security / Infrastructure Protection Division / ICAO		IT, Telecom, NCRCG		
[b2]		[b2] Center		
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell / Planning Cell	b6	IPD		
[b2]		Cyber Security Program Manager		

Organization	Name	Role	Phone	E-mail
Michigan		Public Affairs		
Department of Homeland Security / National Communications System (NCS)		NCRCG		
[b2]		Operations		
Montana		Public Affairs		
[b2]				
FS-ISAC		Security Operations Center		
Department of Homeland Security / National Cyber Security Division / US-CERT	b6	NCRCG	b2	
Department of Homeland Security / Office of Intelligence & Analysis		Cyber Analyst		b2 b6
[b2]				
Department of Energy*		NCRCG		
Department of Defense / OSD / NII		NCRCG		
Canada [b2]				

Cyber Storm Player Directory
By SECTOR
* denotes CWIN capability

Organization	Name	Role	Phone	E-mail
		Energy		
[b2]				
[b2]				
[b2]	b6			
Electricity Sector Information Sharing Analysis Center (ESISAC)*				
Electricity Sector Information Sharing Analysis Center (ESISAC)*	ESISAC Duty	Operations Center		
Electricity Sector Information Sharing Analysis Center (ESISAC)*			b2	b2 b6
Electricity Sector Information Sharing Analysis Center (ESISAC)*				
Electricity Sector Information Sharing Analysis Center (ESISAC)*	b6			
[b2]				
[b2]				
[b2]				

Organization	Name	Role	Phone	E-mail
		Information Technology Lead Technical Analyst		
		[b2] Operator 1		
		[b2] Operator 2		
		[b2] Coordinator 1		
	b6	[b2] Coordinator 2		
		s Information Technology		b2
		Communications		b6
b2		Public Affairs		
		Public Affairs / Media Contact	b2	
		Security		
	Media Relations			
	Operations Shift Supervisor			
	[b2] Coordinator			
	b6			
	Operations Center			

FOR ~~EXERCISE USE~~ ONLY

Organization	Name	Role	Phone	E-mail
		Public Affairs		
		Operations		
b2	b6	Information Technology		b2 b6
		Operations	b2	
		Information Technology		
		Information Technology		
	k	Security		
		Public Affairs		m
		Operations		n
		Operations		n
	[b2] Operator	Operations Center A		n
	[b2] Operator	Operations Center B		n

Organization	Name	Role	Phone	E-mail
	b6	System Operations-TO		
		System Operations-TO		
	Emergency Command Center			
		IT-Corporate		
b2		IT-Business	b2	b2
	b6	Security		b6
		[b2] Operations		
		Cyber Security Program Manager		
Federal Departments & Agencies				
American Red Cross	ARC Other	Subject Matter Expert		
American Red Cross		Office of the Chief Information Security Officer		
American Red Cross		Office of the Chief Information Security Officer	b2	b2
American Red Cross	b6	Manager [b2]		b6
American Red Cross		System Admin		
American Red Cross		System Admin		

Organization	Name	Role	Phone	E-mail
American Red Cross		NetOps Manager		
Central Intelligence Agency / [b2]		NCRCG		
Central Intelligence Agency / [b2]		NCRCG		
[b2]		NCRCG		
[b2]		NCRCG		
[b2]		NCRCG		
Department of Commerce		NCRCG		
Department of Commerce / [b2]	b6	Acting DPAS Program Manager		
Department of Commerce / [b2]				
Department of Commerce / [b2]		Senior Staff Officer	b2	b2 b6
Department of Commerce / NTIA		Chief, Emergency Planning & Policy (COOP Director)		
Department of Commerce / NTIA		NCRCG		
Department of Defense	DoD Other	Subject Matter Expert		
Department of Defense / OSD (NII)-IA	b6	NCRCG		
Department of Defense / JCS [b2]		NCRCG		
Department of Defense / JTF-GNO*	Command Duty Officer			

Organization	Name	Role	Phone	E-mail
Department of Defense / JTF-GNO*	[b6]	NCRCG		
Department of Defense / JTF-GNO*	[b2]			
Department of Defense / JTF-GNO* [b2]		NCRCG		
Department of Defense / JTF-GNO* [b2]		NCRCG		
Department of Defense / JTF-GNO* [b2]	b6	NCRCG		
Department of Defense / OSD / NII		NCRCG		
Department of Defense / OSD / NII		NCRCG		b2 b6
Department of Energy / [b2]		NCRCG		
Department of Energy / [b2]	[b2] Hotline	[b2] Hotline	b2	
Department of Energy [b2]				
Department of Energy [b2]	b6			
Department of Energy [b2]				
Department of Energy [b2]	Network Security Team			
Department of Energy [b2]	[b6]			
Department of Energy [b2]	Watch Officer			

Organization	Name	Role	Phone	E-mail
Department of Energy Office of Energy Reliability	b6 2			
Department of Energy*	DOE Other	Subject Matter Expert		
Department of Energy*		NCRCG		
Department of Energy*		NCRCG		
Department of Health and Human Services		NCRCG		
Department of Health and Human Services		NCRCG		
Department of Homeland Security / HSOC*		NSA Desk Officer		
Department of Homeland Security / HSOC*		NSA Desk Officer		b2
Department of Homeland Security / HSOC*	b6	NSA Desk Officer	b2	b6
Department of Homeland Security / ICE		NCRCG		
Department of Homeland Security / ICE		NCRCG		
Department of Homeland Security / Infrastructure Partnerships Division (IPD)*		IT, Telecom		gov
Department of Homeland Security / Infrastructure Partnerships Division (IPD)*		CWIN		
Department of Homeland Security / Infrastructure Partnerships Division (IPD)*		Hurricanes, NRCC, GIS POC		

Organization	Name	Role	Phone	E-mail
Department of Homeland Security / Infrastructure Partnerships Division (IPD)*				
Department of Homeland Security / Infrastructure Protection Division / ICAO		Energy Sector Specialist		
Department of Homeland Security / Infrastructure Protection Division / ICAO	b6	Aviation		
Department of Homeland Security / Infrastructure Protection Division / ICAO		Financial		
Department of Homeland Security / Infrastructure Protection Division / ICAO		IT, Telecom, NCRCG		b2 b6
Department of Homeland Security / National Communications System (NCS)		NCC	b2	
Department of Homeland Security / National Communications System (NCS)	Manager NCC	MGR NCC		
Department of Homeland Security / National Communications System (NCS)	NCC Industry	NCC Industry		
Department of Homeland Security / National Communications System (NCS)	NCC Watch	NCC Watch		

Organization	Name	Role	Phone	E-mail
Department of Homeland Security / National Communications System (NCS)	NCC Watch			
Department of Homeland Security / National Communications System (NCS)	NCS Other	Subject Matter Expert		
Department of Homeland Security / National Communications System (NCS)		NCRCG		
Department of Homeland Security / National Communications System (NCS)		NCRCG		
Department of Homeland Security / National Cyber Security Division	b6	NCRCG	b2	b2 b6
Department of Homeland Security / National Cyber Security Division		NCRCG		
Department of Homeland Security / National Cyber Security Division		NCRCG		
Department of Homeland Security / National Cyber Security Division		NCRCG		
Department of Homeland Security / National Cyber Security Division		NCRCG Support		

Organization	Name	Role	Phone	E-mail
Department of Homeland Security / National Cyber Security Division		NCRCG Support		
Department of Homeland Security / National Cyber Security Division		NCRCG		
Department of Homeland Security / National Cyber Security Division	b6	NCRCG		
Department of Homeland Security / National Cyber Security Division / O&A		NCRCG Support		
Department of Homeland Security / National Cyber Security Division / US-CERT		NCRCG	b2	
Department of Homeland Security / National Cyber Security Division / US-CERT		NCRCG		b2 b6 ov
Department of Homeland Security / National Cyber Security Division / US-CERT	Operations Center			
Department of Homeland Security / National Cyber Security Division / US-CERT	US-CERT Other	Subject Matter Expert		
Department of Homeland Security / National Cyber Security Division / US-CERT	b6	NCRCG		
Department of Homeland Security / National Infrastructure Coordinating Center (NICC)*		Watch Supervisor		

Organization	Name	Role	Phone	E-mail
Department of Homeland Security / National Infrastructure Coordinating Center (NICC)*		NICC Watch		
Department of Homeland Security / Office of Infrastructure Protection		Infrastructure Liaison (Day)		
Department of Homeland Security / Office of Infrastructure Protection		NCRCG		
Department of Homeland Security / Office of Infrastructure Protection / Contingency Planning & Support Division	b6	Senior Federal Official		b2 b6
Department of Homeland Security / Office of Infrastructure Protection / Contingency Planning & Support Division		Senior Federal Official	b2	
Department of Homeland Security / Office of Infrastructure Protection / HITRAC				
Department of Homeland Security / Office of Infrastructure Protection / HITRAC				
Department of Homeland Security / Office of Infrastructure Protection / HITRAC				

Organization	Name	Role	Phone	E-mail
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell		Director		
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell / Planning Cell		CNPPD (Alternate)		
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell / Planning Cell		CNPPD		b2
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell / Planning Cell	b6	RMD (Night)	b2	b6
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell / Planning Cell		CNPPD (Alternate)		
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell / Planning Cell		RMD		
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell / Planning Cell		HITRAC		

Organization	Name	Role	Phone	E-mail
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell / Planning Cell		HITRAC		
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell / Planning Cell		CNPPD (Alternate)		
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell / Planning Cell		RMD (Day)		
Department of Homeland Security / Office of Infrastructure Protection / Incident Management Cell / Planning Cell	b6	IPD	b2	b2 b6
Department of Homeland Security / Office of Infrastructure Protection / Risk Management Division		RMD Operations Cell (Day)		
Department of Homeland Security / Office of Infrastructure Protection / Risk Management Division		RMD Operations Cell (Night)		
Department of Homeland Security / Office of Intelligence & Analysis		Portfolio Manager - Cyber Threat		
Department of Homeland Security / Office of Intelligence & Analysis		Cyber Analyst		

Organization	Name	Role	Phone	E-mail
Department of Homeland Security / Office of International Affairs		Public Affairs		
Department of Homeland Security / Office of the General Counsel	b6			
Department of Homeland Security / Protected Critical Infrastructure Information Program (PCIIP)				
Department of Homeland Security / Public Affairs	DHS PA Ready Room			
Department of Homeland Security / Public Affairs	b6	NCRCG		b2
Department of Homeland Security / Transportation Security Administration		Public Affairs		b6
Department of Homeland Security / Transportation Security Administration	Transportation Security Intelligence Service (TSIS)		b2	
Department of Homeland Security / Transportation Security Administration	Transportation Security Operations Center (TSOC)			
Department of Homeland Security / Transportation Security Administration	TSA Other	Subject Matter Expert		
Department of Homeland Security / United States Secret Service	b6	Public Affairs		
Department of Homeland Security / United States Secret Service		NCRCG		

Organization	Name	Role	Phone	E-mail
Department of Homeland Security / United States Secret Service		NCRCG		
Department of Homeland Security / United States Secret Service		CID		
Department of Homeland Security / United States Secret Service		NCRCG		
Department of Justice		NCRCG		
Department of Justice		Public Affairs		
Department of Justice / CCIPS		NCRCG		b2
Department of Justice / CCIPS	b6	NCRCG		b6
Department of Justice / CCIPS		NCRCG	b2	
Department of State		Public Affairs		
Department of State				
Department of State		NCRCG		
Department of State				
Department of State		NCRCG		
Department of State		NCRCG		
Department of the Treasury*		NCRCG		
Department of the Treasury*		NCRCG		
Department of the Treasury*		NCRCG		

Organization	Name	Role	Phone	E-mail
Department of Transportation [b2]		Help Desk and Developer		
Department of Transportation [b2]	b2	IT Security Analyst		
Department of Transportation*	Crisis Management Center (CMC)			
Department of Transportation*	DOT Other	Subject Matter Expert		
Department of Transportation*		NCRCG	b2	b2
Department of Transportation*		NCRCG		b6
Department of Transportation*	b6	NCRCG		
Department of Transportation*		NCRCG		
Department of Transportation*	Transportation [b2]			
Department of Transportation*	b6	NCRCG		
Director of National Intelligence / Intelligence Community Incident Response Center		Acting Unit Chief		b7v

Organization	Name	Role	Phone	E-mail
Director of National Intelligence / Intelligence Community Incident Response Center	SIAO Watch Desk			ov
Director of National Intelligence / Intelligence Community Incident Response Center	b6	NCRCG		
[b2]		EPA CSIRC Manager		
Federal Aviation Administration*	[b2]			
Federal Aviation Administration*	FAA Other	Subject Matter Expert		
Federal Aviation Administration*	[b2]		b2	b2
Federal Aviation Administration*	[b6]	NCRCG		b6
Federal Aviation Administration*	[b2]			
Federal Aviation Administration* [b2]		NCRCG		
Federal Bureau of Investigation (FBI)	b6	NCRCG		
Federal Bureau of Investigation (FBI)		Field Offices		
Federal Bureau of Investigation (FBI)		Public Affairs		

Organization	Name	Role	Phone	E-mail
Federal Bureau of Investigation (FBI)	[redacted]	Analyst	[redacted]	[redacted]
Federal Bureau of Investigation (FBI)		NCRCG		
Federal Deposit Insurance Corporation (FDIC)		Security Director		
Federal Deposit Insurance Corporation (FDIC)		Management Review		
[b2]				
Federal Reserve Bank of NY				
Federal Reserve Bank of NY				
Federal Reserve Bank of NY		Subject Matter Expert		
Federal Reserve Bank of NY	b6			b2 b6
Federal Reserve Bank of NY				
Homeland Security Council		NCRCG		
[b2]	el	NCRCG	b2	
National Security Agency / [b2]				
National Security Agency / NTOC		NCRCG		
National Security Agency / NTOC	[redacted]	NCRCG		
National Security Agency / NTOC	Senior Threat Watch Officer			
National Security Agency*	[b6]	NCRCG	[redacted]	[redacted]

Organization	Name	Role	Phone	E-mail
National Security Council		NCRCG		
National Security Council / [b2]	b6	NCRCG		
NORTHCOM*	les	Public Affairs		
NORTHCOM*				
NORTHCOM*	b2		b2	b2 b6
Office of Management and Budget [b2]	b6	NCRCG		
[b2]		NCRCG		
International				
Australia	Operations Center			
Australia		All other roles		
Canada		All other roles		
Canada [b2]				
Canada [b2]				
Canada [b2]	b6		b2	b2 b6
Canada [b2]				
Canada [b2]				

Organization	Name	Role	Phone	E-mail
Canada [b2]				
Canada [b2]				
Canada [b2]				
Canada [b2]				
Canada [b2]				
Canada [b2]	b6			
Canada [b2]				
Canada [b2]				
Canada [b2]			b2	b2 b6
Canada [b2]				
Canada [b2]				
New Zealand	Operations Center			
New Zealand		All other roles		
United Kingdom		All other roles		
United Kingdom [b2]	Analyst			
United Kingdom [b2]	Analyst b2			
United Kingdom [b2]	[b6]			

Organization	Name	Role	Phone	E-mail
Information Technology & Communications				
[b2]	[b2]			
[b2]				
Communications ISAC				
[b4 b2]	b6	Public Affairs		
Information Technology ISAC				
Information Technology ISAC*	IT-ISAC Operations Center			
Information Technology ISAC*	[b6]			
Information Technology ISAC*	IT-ISAC Other	Subject Matter Expert		
Information Technology ISAC	b6			
		[b2] Operations Center		
	[b2]	Subject Matter Expert		
		Response for [b2]	b2	
		[b2] Operations Center		
b2	b6	Response for [b2]		
		[b2]		
		[b2]		
		Public Affairs [b2]		

b2
b6

Organization	Name	Role	Phone	E-mail
	[b6]	Public Affairs		
	[b2]	Subject Matter Expert		
		Public Affairs		
	b6	[b2] Technical Operations Center		
		Information Security		
		Information Security		
	[b2]	Subject Matter Expert		b2 b6
b2	[b6]	Director, [b2]		
	[b2]	Subject Matter Expert		
	[b6]	[b2] Center	b2	n
	[b2]	Subject Matter Expert		
		[b2] Center		n
	b6	[b2] Center		
		[b2] Center		
		[b2] Center		

FOR ~~EXERCISE USE~~ ONLY

Organization	Name	Role	Phone	E-mail
[b2]	[b2]	Subject Matter Expert	b2	b2 b6 b4
b4 b2	b6	[b2] Center		
		[b2] Center		
Other Private Sector				
[b2] FS-ISAC	[b2] b6	Security Operations Center	b2	b4 b2 b6
FS-ISAC [b2] [b4 b2]	[b4 b2] [b4 b2]			
State & Local				
Michigan	[b6]	Public Affairs	b2	b2 b6
Michigan		Public Affairs		
Michigan*	Operations Center			
Montana	[b6]	Public Affairs		
Montana*	Operations Center			
MS-ISAC*	Operations Center			
New York*	Operations Center			
[b2]	[b2]			

Organization	Name	Role	Phone	E-mail
Transportation				
[b2]	[b2]		[ ]	[ ]
[b4 b2]	[b2]	[b4 b2]		
[b4 b2]			b2	b2 b6
[b2]				
[b2]			[ ]	[ ]

P34A

Withheld in Full

b2

4 Pages

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

[b6 b2]

P35

From: [b6 b2]
Sent: Monday, February 06, 2006 12:35 PM
To: [b2 b6]

Cc: [b2 b6]
Subject: Exercise Cyber Storm: Public announcements through open source

** EXERCISE Cyber Storm #9303 EXERCISE **

EXERCISE - EXERCISE - EXERCISE - EXERCISE - EXERCISE - EXERCISE

[b2]

iens

** EXERCISE Cyber Storm #9303 EXERCISE **

P36A

Withheld in Full

b2

5 Pages

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

[b6 b2] P37.

From: [b2 b6]
Sent: Tuesday, February 07, 2006 9:12 AM
To:

b2
b6

[b2 b6]

Cc: [b2 b6]

Subject: EXERCISE EXERCISE EXERCISE - Inject 9308 - 02

EXERCISE EXERCISE EXERCISE

[b2]

EXERCISE EXERCISE EXERCISE

P37A

Withheld in Full

b2

1 Page

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

[b6 b2]

P39.

From: [b2 b6]
Sent: Tuesday, February 07, 2006 9:37 AM
To: All Player; All OC
Subject: Please do not Act directly against Exercise IP Addresses.

To all players:
IMPORTANT!

[b2]

[b6]
Cyber Storm Exercise Director
CS-Control Voice [b2]
Mobile: [b2]

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

P40.

[b6 b2]

From: Media [b2]
Sent: Tuesday, February 07, 2006 11:21 AM
To: allplayer [b2] alloc [b2]
Cc: [b2]
Subject: Exercise Cyber Storm: [b2]

** EXERCISE Cyber Storm #7017 EXERCISE **

EXERCISE EXERCISE EXERCISE

[b2]

EXERCISE EXERCISE EXERCISE

** EXERCISE Cyber Storm #7017 EXERCISE **

Withheld in Full

b2

P41B

Withheld in Full

b2

1 Page

P42A

Withheld in Full

b2

4 Pages

P42B

Withheld in Full

b2

2 Pages

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

[b6 b2] P43

From: [b2 b6]
Sent: Tuesday, February 07, 2006 1:48 PM
To: allplayer [b2]
Cc: [b2]
Subject: FW: Exercise Cyber Storm: MSV A announces Security Advisory

** EXERCISE Cyber Storm #4011.3 EXERCISE **

** EXERCISE EXERCISE EXERCISE ** Cyber Storm Major SW Vendor A' Security Response Center has released a Security Advisory related to reported vulnerabilities

[b2]

** EXERCISE EXERCISE EXERCISE ** Cyber Storm

** EXERCISE Cyber Storm #4011.3 EXERCISE **

DISCLAIMER:
Exercise Exercise Exercise

Withheld in Full

b2

P44B

Withheld in Full

b2

1 Page

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

P45.

[b6 b2]

From: [b2 b6]
Sent: Tuesday, February 07, 2006 2:28 PM
To: All OC; All Player
Subject: Addendum Directory

EXERCISE Administrative update.

As many of you know there have been a variety of corrections, deletions and updates to the player contact data since STARTEX. The attached addendum is the latest update to the player directory. This addendum in conjunction with your original directory should now be considered the official player directory until the next addendum... or the ENDEX, which ever comes first.

Thank you.

[b6 b2]
Cyber Storm Exercise Director
CS-Control Voice: [b2]
Mobile: [b2]

-----Original Message-----
From: [b2 b6]
Sent: Tuesday, February 07, 2006 1:50 PM
To: [b2 b6]
Subject: addendum

Attached.

P45A

TRANSFERRED TO OTHER AGENC
TRANSFER FOR DIRECT REPLY - D

NATIONAL CYBER EXERCISE
CYBER STORM
Player Directory Addendum

February 6–10, 2006

Department of Homeland Security
National Cyber Security Division

This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR ~~EXERCISE~~ USE ONLY

Cyber Storm Player Directory
By ORGANIZATION

The below player directory entries have been added or edited since the Cyber Storm Player Directory distributed via e-mail on February 6.

* denotes CWIN capability

Organization	Name	Role	Phone	E-mail
Canada [redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Canada [redacted]				
Canada				
Canada				
Canada				
Canada				
Canada				
Canada				
Canada				
Canada				
[b2]				
Canada [b2]				
[b2]				
Canada [b2]				
[b2]				
Canada [redacted]				
Canada				
Canada				
Canada				
Canada				
Canada				
Canada				
Canada				
Canada				
Canada				

b2 b6 b2 b2 b6

Organization	Name	Role	Phone	E-mail
Canada /				
Canada /				
Canada /				
Canada /				
Canada /				
Canada /				
Canada /				
Canada /				
Canada /				
Canada /				
Canada /				
Canada /				
Canada /				
Canada /				
Canada /				
Canada /				
Canada /				
Canada /				
Canada /				
Canada /				
Canada /				
Canada /				
Canada /				
Canada /				
Canada /				
Canada /				
Canada /				
Department of Energy [b2]				
Department of Homeland Security / National Cyber Security Division / US- [b2]				

b2 b6 b2 b2 b6

Organization	Name	Role	Phone	E-mail
Department of Homeland Security / Office of Infrastructure Protection	[b6]	Infrastructure Liaison (Day)	[ ]	[ ]
Federal Aviation Administration*	[b2]		b2	b2 b6
United Kingdom [b2]	Analyst [b2]		[ ]	[ ] k

P46.

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

[b6 b2]

From: Media [b2]
Sent: Tuesday, February 07, 2006 3:42 PM
To: Allplayer [b2] alloc [b2]
Cc: [b2 b6]
Subject: Exercise Cyber Storm: Washington Daily News Report: Spouses of service members offended by posting on Tricare website

** EXERCISE Cyber Storm #7015 EXERCISE **

EXERCISE EXERCISE EXERCISE

[b2]

EXERCISE EXERCISE EXERCISE

** EXERCISE Cyber Storm #7015 EXERCISE **

TRANSFERRED TO OTHER AGENCY
[b6 b2] TRANSFER FOR DIRECT REPLY - DHS

P47

From: [b2 b6]
Sent: Tuesday, February 07, 2006 3:51 PM
To: allplayer [b2]
Cc: [b2]
Subject: Exercise Cyber Storm: DeepSight Analysis Report

From: [b2]
Sent: Tuesday, February 07, 2006 3:43 PM
To: allplayers [b2] alloc [b2]
Cc: [b2]
Subject: Exercise Cyber Storm: DeepSight Analysis Report

** EXERCISE Cyber Storm #4011.4 EXERCISE **

"THIS IS A MESSAGE FROM DEEPSIGHT" [

b2

b2

** EXERCISE Cyber Storm #4011.4 EXERCISE **

DISCLAIMER:
Exercise Exercise Exercise

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

[b6 b2]

P48

From: [b2 b6]
Sent: Tuesday, February 07, 2006 3:53 PM
To: allplayer [b2]
Cc: [b2]
Subject: FW: Exercise Cyber Storm: DeepSight Analysis Report

From: [b2]
Sent: Tuesday, February 07, 2006 3:44 PM
To: allplayers [b2]
Cc: [b2]
Subject: Exercise Cyber Storm: DeepSight Analysis Report

** EXERCISE Cyber Storm #4011.4-01 EXERCISE **

"THIS IS MESSAGE FROM DEEPSIGHT"

b2

** EXERCISE Cyber Storm #4011.4-01 EXERCISE **

DISCLAIMER:
Exercise Exercise Exercise

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

[b6 b2]

P49.

From: [b2 b6]
Sent: Tuesday, February 07, 2006 3:55 PM
To: allplayer [b2]
Subject: FW: Exercise Cyber Storm: DeepSight Analysis Report

From: [b2]
Sent: Tuesday, February 07, 2006 3:44 PM
To: allplayers [b2 b6]
Cc: [b2]
Subject: Exercise Cyber Storm: DeepSight Analysis Report

** EXERCISE Cyber Storm #4011.4-02 EXERCISE **

"THIS IS A MESSAGE FROM DEEPSIGHT"

b2

** EXERCISE Cyber Storm #4011.4-02 EXERCISE **

DISCLAIMER:
Exercise Exercise Exercise

DISCLAIMER:
Exercise Exercise Exercise

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

[b6 b2]

P50

From: [b2 b6]
Sent: Tuesday, February 07, 2006 3:56 PM
To: allplayers[b2]
Cc: [b2]

Subject: Exercise Cyber Storm: In response to 3016 - Media response to anonymous threat posting on US DoD mail website

---

From: [b2]
Sent: Tuesday, February 07, 2006 3:52 PM
To: allplayers [b2]
Cc: [b2]

Subject: Exercise Cyber Storm: In response to 3016 - Media response to anonymous threat posting on US DoD mail website

** EXERCISE Cyber Storm #7043 EXERCISE **

EXERCISE EXERCISE EXERCISE February 7, 2006

b2

EXERCISE EXERCISE EXERCISE

** EXERCISE Cyber Storm #7043 EXERCISE **

DISCLAIMER:
Exercise Exercise Exercise

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

P51

[b6 b2]

From: [b2 b6]
Sent: Tuesday, February 07, 2006 3:58 PM
To: allplayer [b2]
Subject: FW: Exercise Cyber Storm: DeepSight Analysis Report

From: [b2]
Sent: Tuesday, February 07, 2006 3:44 PM
To: allplayers [b2]
Cc: [b2]
Subject: Exercise Cyber Storm: DeepSight Analysis Report

** EXERCISE Cyber Storm #4011.4-03 EXERCISE **

"THIS IS A MESSAGE FROM DEEPSIGHT" EXERCISE EXERCISE EXERCISE Technical Cyber Security Alert EXERCISE [

b2

b2

Technical Staff EXERCISE EXERCISE EXERCISE

** EXERCISE Cyber Storm #4011.4-03 EXERCISE **

DISCLAIMER:
Exercise Exercise Exercise

DISCLAIMER:
Exercise Exercise Exercise

TRANSFERRED TO OTHER AGENCY P52.
[b6 b2] TRANSFER FOR DIRECT REPLY - DHS

From: [b2 b6]
Sent: Tuesday, February 07, 2006 4:04 PM
To: [b2] All Player
Cc: [b2 b6]
Subject: RE: Exercise Cyber Storm: DeepSight Analysis Report

EXERCISE EXERCISE EXERCISE

[b2 b6]

[b2]

[b2 b6]
Major Hardware Vendor Z

EXERCISE EXERCISE EXERCISE

-----Original Message-----
From: [b2 b6]
Sent: Tue 2/7/2006 3:53 PM
To: All Player
Cc: [b2]
Subject: Exercise Cyber Storm: DeepSight Analysis Report

From: [b2]
Sent: Tuesday, February 07, 2006 3:43 PM
To: allplayers [b2]
Cc: [b2]
Subject: Exercise Cyber Storm: DeepSight Analysis Report

** EXERCISE Cyber Storm #4011.4 EXERCISE **

"THIS IS A MESSAGE FROM DEEPSIGHT"

b2

b2

[b2]

** EXERCISE Cyber Storm #4011.4 EXERCISE **

DISCLAIMER:
Exercise Exercise Exercise

[b6 b2] TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

P54.

From: [b2]
Sent: Tuesday, February 07, 2006 5:16 PM
To: [b2]
Cc: allplayer [b6 b2]
Subject: Re: Exercise Cyber Storm: DeepSight Analysis Report

** EXERCISE Cyber Storm #4011.4 EXERCISE **

Based upon the email bellow the FAA CSIRC did the following steps:

CSIRC Actions:

[b2]

** EXERCISE Cyber Storm #4011.4 EXERCISE **

Very Respectfully
[b6]
FAA CSIRC Response Group
[b2] (PH)
(FAX)
(STU)

[b2]

Sent by: [b6 b2]

02/07/2006 03:53 PM

To <allplayer@cs-control.com>
cc [b2]
Subject Exercise Cyber Storm: DeepSight Analysis Report

From: [b2]
Sent: Tuesday, February 07, 2006 3:43 PM
To: allplayers [b2]
Cc: [b2]

[b2]

Subject: Exercise Cyber Storm: DeepSight Analysis Report

** EXERCISE Cyber Storm #4011.4 EXERCISE **

"THIS IS A MESSAGE FROM DEEPSIGHT"

b2

** EXERCISE Cyber Storm #4011.4 EXERCISE **

DISCLAIMER:
Exercise Exercise Exercise

DISCLAIMER:
Exercise Exercise Exercise

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

P55

[b6 b2]

From: Control [b2]
Sent: Wednesday, February 08, 2006 8:15 AM
To: allplayer [b2]
Cc: [b2 b6]

Subject: [b2] Meetings Open

** EXERCISE Cyber Storm #2022 EXERCISE **

[b2]

** EXERCISE Cyber Storm #2022 EXERCISE **

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

[b6 b2]

P56.

From: [b2]
Sent: Wednesday, February 08, 2006 8:18 AM
To: All OC; All Player
Cc: csemail
Subject: EXCERCISE CYBER STORM. DeepSight Increased ThreatCon from [b2]

EXERCISE EXERCISE EXERCISE

THIS IS A MESSAGE FROM DEEPSIGHT

-----BEGIN PGP SIGNED MESSAGE-----

[b2]

CYBERSTORM

-----END PGP SIGNATURE-----

EXERCISE EXERCISE EXERCISE

P57

Withheld in Full

b2

2 Pages

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

[b2 b6]

P58.

From: [b2]
Sent: Wednesday, February 08, 2006 8:38 AM
To:

b2
b6

Cc:

Subject: 199.2 FM Washington D.C. Hourly traffic report

** EXERCISE Cyber Storm #7006 EXERCISE **

EXERCISE EXERCISE EXERCISE Traffic on the hour report

[b2

EXERCISE EXERCISE b2 EXERCISE

** EXERCISE Cyber Storm #7006 EXERCISE **

P59.

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

[b6 b2]

From: [b2 b6]
Sent: Wednesday, February 08, 2006 8:39 AM
To: allplayer[b2]
Cc: [b2]
Subject: Exercise Cyber Storm: Major Hardware Vendor A Announces Major Vulnerability

** EXERCISE Cyber Storm #4531 EXERCISE **

b2

b2

** EXERCISE Cyber Storm #4531 EXERCISE **

DISCLAIMER:
Exercise Exercise Exercise

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

P60.

[b6 b2]

From: [b2 b6]
Sent: Wednesday, February 08, 2006 8:55 AM
To:

b2
b6

Cc:
Subject: SITRep EXERCISE

EXERCISE EXERCISE EXERCISE

DHS-NCSD/US-CERT will be proposing on 9 am Co-Chair Conference Call that a NCRCG meeting be convened this morning.

Please stay tuned for more details. SITREP from US-CERT below.

EXERCISE EXERCISE EXERCISE

-----Original Message-----
From: [b2]
To: [b2 b6]
Sent: Wed Feb 08 08:04:17 2006
Subject: SITRep EXERCISE

Federal Space / GFIRST

Co-Chair conference call

b2

b 5

b 2

PAGES

2 - 16

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

P61

[b6 b2]

From: [b2]
Sent: Wednesday, February 08, 2006 9:01 AM
To: allplayer [b2]
Cc: [b2]
Subject: Exercise Cyber Storm: Washington Daily Media Report - Report extortion of [b4 b2]

** EXERCISE Cyber Storm #7011 EXERCISE **

EXERCISE EXERCISE EXERCISE

[b2 b4]

EXERCISE EXERCISE EXERCISE

** EXERCISE Cyber Storm #7011 EXERCISE **

[b6 b2] TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

P62

From: [b2 b6]
Sent: Wednesday, February 08, 2006 9:27 AM
To:

b2
b6

Cc:
Subject: RE: SITRep EXERCISE

Importance: High

EXERCISE EXERCISE EXERCISE

ALL NCRCG MEMBERS CALL INTO CONFERENCE CALL AT 9:30.

CALL-IN INFO:
[b2]

EXERCISE EXERCISE EXERCISE

[b2 b6]

-----Original Message-----
From: [b2 b6]
Sent: Wednesday, February 08, 2006 8:55 AM
To:

[b2 b6]

b2
b6

Subject: SITRep EXERCISE

EXERCISE EXERCISE EXERCISE

DHS-NCSD/US-CERT will be proposing on 9 am Co-Chair Conference Call that a NCRCG meeting be convened this morning.

Please stay tuned for more details. SITREP from US-CERT below.

EXERCISE EXERCISE EXERCISE

-----Original Message-----
From: [b2]
To: [b2 b6]
Sent: Wed Feb 08 08:04:17 2006
Subject: SITRep EXERCISE

Federal Space / GFIRST

b2

b5

b2

PAGES
3 - 17

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS P63

[b6 b2]

From: [b2]
Sent: Wednesday, February 08, 2006 9:29 AM
To: all players; All OC
Cc: [b2]
Subject: RE-SEND: Exercise Cyber Storm: Major Hardware Vendor Z Announces Major Vulnerability

Exercise Exercise Exercise

b2

Respectfully yours,

[b2]

** EXERCISE Cyber Storm #4531 EXERCISE **

Exercise Exercise Exercise

P63A

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

EXERCISE Hardware Vendor "Z" Security Advisory: Mishandled Evil Bit Denial of Service
EXERCISE Document ID: 65537 Revision 1.0
EXERCISE For Public Release 2006 February 08 08:00 AM US/Eastern

Summary

b2

b2

b2

End of Notice

EXERCISE Hardware Vendor "Z" Security Advisory: Mishandled Evil Bit Denial of Service
EXERCISE Document ID: 65537 Revision 1.0
EXERCISE For Public Release 2006 February 08 08:00 AM US/Eastern

TRANSFERRED TO OTHER AGENCY P65
[b6 b2] TRANSFER FOR DIRECT REPLY - DHS

From: [b2 b6]
Sent: Wednesday, February 08, 2006 9:36 AM
To: [b2] All Player
Cc: [b2 b6]

Subject: RE: Exercise Cyber Storm: Major Hardware Vendor Z Announces Major Vulnerability

EXERCISE EXERCISE EXERCISE

[b2]

Sorry for any inconvenience,

[b6]
Major Hardware Vendor Z PSIRT

EXERCISE EXERCISE EXERCISE
-----Original Message-----
From: [b2 b6]
Sent: Wed 2/8/2006 8:41 AM
To: All Player
Cc: [b2 b6]
Subject: Exercise Cyber Storm: Major Hardware Vendor A Announces Major Vulnerability

** EXERCISE Cyber Storm #4531 EXERCISE **

EXERCISE Hardware Vendor "Z" Security Advisory:

[b2]

b2

** EXERCISE Cyber Storm #4531 EXERCISE **

DISCLAIMER:
Exercise Exercise Exercise

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

[b6 b2]

P66

From: [b2 b6]
Sent: Wednesday, February 08, 2006 9:40 AM
To: [b2]
Cc: [b2 b6]
Subject: Re: EXCERCISE CYBER STORM. DeepSight Increased ThreatCon from [b2]

Exercise Exercise Exercise

So is Dept. Of Commerce claiming that they have control systems or operator control panels as it relates to OPC protocol on your networks?

Please reply to US-CERT [b2]

Exercise Exercise Exercise
[b2 b6]
US CERT Operations
[b2 b6]
Incident Hotline: [b2]
[b2]

ThumbTyped from my BlackBerry

-----Original Message-----
From: [b2 b6]
To: [b2 b6]
Sent: Wed Feb 08 09:25:05 2006
Subject: Re: EXCERCISE CYBER STORM. DeepSight Increased ThreatCon from [b2].

EXERCISE EXERCISE EXERCISE

The Dept of Commerce acknolwedges receipt and has taken the following actions:

[b2]

Action coordinated through DoC Federation of [b2]

EXERCISE EXERCISE EXERCISE

>>> [b2] 2/8/2006 8:14 AM >>>
EXERCISE EXERCISE EXERCISE

THIS IS A MESSAGE FROM DEEPSIGHT

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Name: Increased ThreatCon from [b2]
Location:
https:// [b2]

Summary:
The DeepSight Threat Analyst Team is elevating the ThreatCon to [b2] in response to multiple unspecified vulnerabilities that are reported to exist in various client and server implementations of OPC protocols.The exact nature of these vulnerabilities have not been publicized at the time of writing, customers are recommended to review the following alert.

OPC Protocols Alert
[b2]

View public key at:
[b2]

-----BEGIN PGP SIGNATURE-----
Version: [b2]

CYBERSTORM

-----END PGP SIGNATURE-----

EXERCISE EXERCISE EXERCISE

DISCLAIMER:
Exercise Exercise Exercise

DISCLAIMER:
Exercise Exercise Exercise

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

Cyber Storm Tabletop Exercise

August 9, 2005

Homeland Security

P84

Cyber Storm Tabletop Exercise

Table of Contents

P84A

Agenda

Overview

List of Players

Exercise Slides

Reference Material

Homeland Security Presidential Directives

1. HSPD-5: Management of Domestic Incidents
2. HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection

National Security Documents

3. National Strategy for Homeland Security - Executive Summary
4. National Strategy to Secure Cyberspace
5. Interim National Infrastructure Protection Plan

National Response Information

6. National Response Plan – Front pages, and Cyber Incident Annex
7. National Incident Management System (NIMS) - extract of general slides
8. Interagency Incident Management Group (IIMG) Overview
9. National Cyber Response Coordination Group (NCRCG) Overview
10. Draft Cyber Incident Response Flow Chart

Concepts of Operations

11. U.S.-Computer Emergency Readiness Team (US-CERT) Concept of Operations for Federal Cyber Security Incident Handling

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

Homeland Security

12. National Cyber Response Coordination Group (NCRCG) Concept of Operations

Standard Operating Procedures

13. Homeland Security Operations Center (HSOC) Standard Operation Procedures

14. Interagency Incident Management Group (IIMG) Standard Operating Procedures

Glossary of Terms Used in the Exercise

After Action Report (for future use)

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

P84B

Cyber Storm Tabletop Exercise Player Book

August 9, 2005

Homeland Security

FOR OFFICIAL USE ONLY

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS P84C

Cyber Storm Tabletop Exercise

August 9, 2005

Agenda

0730	Registration
0830	Opening Remarks and Exercise Overview
0845	Move 1: Intelligence and Threat Assessment
0945	Break
1000	Move 2: Incident Response
1130	Working Lunch
1200	Move 3: Recovery
1300	[b2]
1400	ENDEX

Homeland Security

Cyber Storm Tabletop Exercise
Overview

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

P84D

1. **Background**

The National Cyber Response Coordination Group (NCRCG) will hold a Cyber Storm Tabletop Exercise (TTX) to enhance its overall preparedness and response capabilities in the event of a potential or actual Incident of National Significance involving the Nation's critical cyber infrastructure. This exercise is the fourth in a series of building block exercises leading to Cyber Storm 05, the national full-scale cyber exercise (FSE) scheduled for November 14-18, 2005. The FSE will require activation of all Federal departments and agencies having responsibility to respond to a cyber Incident of National Significance.

2. **Purpose**

The purpose of Cyber Storm TTX is to enhance the operational framework of the NCRCG with its supporting U.S. Computer Emergeny Response Team (US - CERT), and mutual interaction with the InteragencyIncident Management Group (IIMG) and the Homeland Security Operations Center (HSOC) in the event of a Cyber Incident of National Significance potentially or actually affecting the U.S. critical cyber infrastructure. In addition, the exercise will provide insight into required NCRCG operational capabilities for efficient and effective response to a cyber incident of national significance.

The exercise is scheduled for August 9, 2005, [redacted] b2

3. **Scope**

The tabletop discussion will involve the full membership of the NCRCG and IIMG, relevant participants from the HSOC and the US-CERT, and select key organizations under the National Response Plan and National Infrastructure Protection Plan.

The exercise will focus on managing the consequences of a cyber attack while providing appropriate coordination with the IIMG and other operational entities.

This is an unclassified exercise.

4. Exercise Objectives

The objectives of this exercise are to:

- Establish operational linkages between and requirements in support of the NCRCG and IIMG
- Establish communication protocols between the IIMG, NCRCG, US-CERT and HSOC
- Validate the current NCRCG concept of operations
- Establish a process for Federal departments and agencies to support the NCRCG mission
- Determine the lateral linkages to other interagency activities and operations/incident response centers (e.g., National Infrastructure Coordination Center, National Response Coordination Center) under the National Response Plan framework

By meeting the above objectives, the organizations involved in this exercise will be better prepared to participate in Cyber Storm 05 FSE in November.

b2
b5

Cyber Storm Tabletop Exercise
Overview

b2
b5

Cyber Storm Tabletop Exercise
Overview

b2
b5

Cyber Storm Tabletop Exercise
Overview

b2
b5

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

Cyber Storm Tabletop Exercise Participants
As of Friday, August 05, 2005
Alphabetical Listing

P84E

Name	Organization
[redacted]	DHS
	DOJ/CCIPS
	NSC
	DHS
	DoD/JTF-GNO
	[b2]
	DoD/OASDNII
	DOT
	HSOC
	DHS
	HSOC
	USSS
b2	DoD/JTF-GNO [b2]
	DOJ [b2]
b6	FBI
	DoD/JTF-GNO
	DOJ/CCIPS
	DHS
	HSOC
	NCSD/US-CERT
	DHS/NCS
	NRC
	DHS
	DOJ/CCIPS
	DHS/NCSD [b2]
	DoD/JTF-GNO [b2]
	DHS
	HHS
	[b2]
	DHS
	DHS/EPR/FEMA
	DOJ/ [b2]
	DoD/NORTHCOM
[redacted]	[b2]
	DHS

Cyber Storm Tabletop Exercise Participants
As of Friday, August 05, 2005
Alphabetical Listing

Name	Organization
[redacted]	NCSD/US-CERT
	CIA
	[b2]
	[b2]
	NCSD/Cyber Storm Exercise/[b2]
	USCG
	Commerce/NTIA [b2]
	DHS
	DoD/OASDNII
	DHS
	DHS
	Commerce [b2]
	OMB
	[b2]
b2	DHS/NCSD/[b2]
	NCSD/Cyber Storm Exercise/[b2]
b6	DOE
	DHS/NCSD
	DHS/NCSD/NSA
	DHS
	DHS/OGC
	DHS
	[b2]
	DHS/USSS
	[b2]
	DHS
	DHS
	DHS
	DoD/JTF-GNO/[b2]
	[b2]
	DoD/OASDNII
	DHS
	DOS
	DHS/NCSD/LE
	DOT TCIRC
	DHS/NCSD [b2]

Cyber Storm Tabletop Exercise Participants
As of Friday, August 05, 2005
Alphabetical Listing

Name	Organization
	[b2]
	DHS
	[b2]
	[b2]
	DHS/NCSD/LE
	[b2]
	[b2]
	[b2]
	NCSD/US-CERT
	DOJ/CCIPS
	DHS
	DoD/STRATCOM
	Treasury
b2	DoD/NORTHCOM
	[b2]
b6	DHS
	[b2]
	DHS
	DOE
	DHS/NCSD
	[b2]
	NCSD/US-CERT
	DOD
	DHS
	FBI
	DHS/USSS
	DOS
	[b2]
	[b2]
	DOS
	DHS
	FEMA
	[b2]
	DHS/NCS
	DoD/JTF-GNO [b2]
	DHS

Cyber Storm Tabletop Exercise Participants
As of Friday, August 05, 2005
Alphabetical Listing

Name	Organization
b2 b6	DHS
	DoD/JTF-GNO [b2]
	[b2]
	DoD/JCS [b2]
	DHS
	DoD/JTF-GNO [b2]
	DHS/USSS
	[b2]
	[b2]
	DHS/NCSD
	DHS/USSS
	HSOC
	NCSD/US-CERT
	DHS/IP/NCSD
	DOE

Cyber Storm Tabletop Exercise Participants
As of Friday, August 05, 2005
Interagency Incident Management Group (IIMG)

Organization	Name
ARC	
DHS	
DHS	
DHS	
DHS	
DHS	
DHS	
DHS	
DHS	
DHS	
DHS	
DHS	
DHS	b2
DHS	
DHS	b6
DHS	
DHS	
DHS	
DHS	
DHS	
DHS	
DHS	
DHS	
DHS	
DHS/OGC	
DOD	
DOE	
DOI	
DOJ [b2]	
DOJ [b2]	
[b2]	
DOT	
[b2]	
[b2]	

Cyber Storm Tabletop Exercise Participants
As of Friday, August 05, 2005
Interagency Incident Management Group (IIMG)

Organization	Name
FBI	
FEMA	
[b2]	
HHS	
b2	
Treasury	
USCG	
[b2]	
[b2]	
USSS	
[b2]	
[b2]	

b2
b6

Cyber Storm Tabletop Exercise Participants
As of Friday, August 05, 2005
National Cyber Response Coordination Group (NCRCG)

Organization	Name
CIA	
Commerce/NTIA [b2]	
Commerce/OCIO	
DHS/NCS	
DHS/NCS	
DHS/NCSD	
DHS/NCSD [b2]	
DHS/NCSD [b2]	
DHS/NCSD [b2]	b2
DHS/NCSD/LE	
DHS/NCSD/LE	b6
DHS/NCSD/NSA	
DHS/USSS	
DHS/USSS	
DHS/USSS	
DHS/USSS	
[b2]	
[b2]	
DoD [b2]	
DoD/JCS [b2]	
DoD/JTF-GNO	
DoD/JTF-GNO [b2]	
DoD/JTF-GNO [b2]	
DoD/JTF-GNO [b2]	
DoD/JTF-GNO [b2]	
DoD/JTF-GNO [b2] [b2]	
DoD/JTF-GNO [b2]	
DoD/JTF-GNO [b2]	
DoD/NORTHCOM	
DoD/NORTHCOM	
DoD/OASDNII	

Cyber Storm Tabletop Exercise Participants
As of Friday, August 05, 2005
National Cyber Response Coordination Group (NCRCG)

Organization	Name
DoD/OASDNII	[redacted]
DoD/OASDNII	
DoD/STRATCOM	
DOE	
DOE	
DOJ/CCIPS	
DOJ/CCIPS	
DOJ/CCIPS	b2
DOJ/CCIPS	
DOS	b6
DOS	
DOS	
DOT TCIRC	
FBI	
[b2]	
[b2]	
NSC	
[b2]	
OMB	

Cyber Storm Tabletop Exercise Participants
As of Friday, August 05, 2005
Others

Organization	Name
HSOC	
US-CERT	
	b2
	b6
Other	
DHS	
DHS	
DHS	
DHS	
DHS/EPR/FEMA	
DHS/IP/NCSD	
DHS/NCSD	
DHS/NCSD	
[b2]	
NCSD [b2]	
NCSD [b2]	
[b2 b4]	

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

P84F

Cyber Storm Tabletop Exercise

9 August 2005

Homeland Security

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

Cyber Tabletop Exercise (TTX) Overview

Agenda

0730	Registration
0830	Opening Remarks and Exercise Overview
0845	Move 1: Intelligence and Threat Assessment
0945	Break
1000	Move 2: Incident Response
1130	Working Lunch
1200	Move 3: Recovery
1300	[b2]
1400	ENDEX

Homeland Security

FOR OFFICIAL USE ONLY

2

Purpose

- The purpose of the Cyber Storm TTX is to enhance the overall preparedness and response capabilities of the federal government in the event of a potential or actual Cyber Incident of National Significance.
- Key organizations involved in preparedness, response and recover from a cyber incident include:
  - National Cyber Response Coordination Group (NCRCG)
  - Interagency Incident Management Group (IIMG)
  - Homeland Security Operations Center (HSOC)
  - U.S. Computer Emergency Readiness Team (US-CERT)

Objectives

- Establish operational linkages between and requirements in support of the NCRCG and IIMG.
- Establish communications protocols between the IIMG, NCRCG, HSOC and US-CERT.
- Validate the current NCRCG Concept of Operations.
- Establish a process for Federal departments and agencies to support the NCRCG mission.
- Determine lateral linkages to other sector interagency activities and operations/incident response centers under the National Response Plan (NRP) framework.

Key Players' Responsibilities

- IIMG: Federal headquarters-level multi-agency coordination entity that facilitates strategic Federal domestic incident management for Incidents of National Significance.
- NCRCG: Principal federal interagency mechanism for managing cyber incidents of National Significance and other cyber related issues affecting national interests.
- HSOC: Primary national hub for domestic incident management, operational coordination and situational awareness. Standing 24/7 interagency organization fusing law enforcement, national intelligence, emergency response and private sector reporting.
- US-CERT: Coordinates cyber warning among Federal departments and agencies. Maintains 24/7 operations center with connectivity to Federal cyber operations centers, internet service providers and private sector IT vendors. In concert with HSOC, acts as focal point to collect and disseminate cyber related information. Provides technical and operational support to the IIMG.

Exercise Presumptions

- The sequence of events may include exercise artificialities.
- Events may occur simultaneously, but the discussion of those events may need to be sequenced.
- Response to Cyber Incidents of National Significance will be based upon the NRP, National Incident Management System (NIMS), and the Cyber Incident Annex.
- The cyber threat scenario will be discussed in the NRP taxonomy of prevention, preparedness, response, and recovery.
- Recognizing that cyberspace is largely owned and operated by the private sector, the authority of the Federal government to exert direct control over activities in cyberspace is limited.

Guiding Authorities

- Homeland Security Presidential Directives (HSPDs)
  - HSPD-5: Management of Domestic Incidents
  - HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection
- National Strategy Documents
  - National Strategy For Homeland Security, July, 2002
  - National Strategy To Secure Cyberspace, February 2003
  - Interim National Infrastructure Protection Plan, February 2005
- NRP, December 2004
  - Cyber Incident Annex
- NIMS, March 1, 2004 (Slide extract)
- Standard Operating Procedures
  - IIMG: Interagency Integrated Standard Operating Procedures, IIMG Activation and Operations, March 2005
  - HSOC: Standard Operating Procedures, April 2005
- Concept of Operations
  - US-CERT: Concept of Operations for Federal Cyber Security Incident Handling, April 2005
  - NCRCG: NCRCG Concept of Operations, June 2005

*All are included in the player book, reference section

Homeland Security

b2

Homeland Security

b2

b2

Move 1: Intelligence/Threat Assessment

Thursday, 4 August 2005

b2

b2

b2

Move 2: Incident Response

Tuesday, 9 August 2005

b2

b2

b2

b2

b2

Move 3: Recovery and Reconstitution

Friday, 12 August 2005

b2

b2

ENDEX --- [b2]

Homeland Security

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

P84G

References for Cyber Storm Tabletop Exercise

Homeland Security Presidential Directives

1. HSPD-5: Management of Domestic Incidents
2. HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection

National Security Documents

3. National Strategy for Homeland Security - Executive Summary
4. National Strategy to Secure Cyberspace
5. Interim National Infrastructure Protection Plan

National Response Information

6. National Response Plan – Front pages, and Cyber Incident Annex
7. National Incident Management System (NIMS) - extract of general slides
8. Interagency Incident Management Group (IIMG) Overview
9. National Cyber Response Coordination Group (NCRCG) Overview
10. Draft Cyber Incident Response Flow Chart

Concepts of Operations

11. U.S.-Computer Emergency Readiness Team (US-CERT) Concept of Operations for Federal Cyber Security Incident Handling
12. National Cyber Response Coordination Group (NCRCG) Concept of Operations

Standard Operating Procedures

13. Homeland Security Operations Center (HSOC) Standard Operation Procedures
14. Interagency Incident Management Group (IIMG) Standard Operating Procedures

P84V

Withheld in Full

b2

4 Pages

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

[b6 b2]

P85

From: [b2 b6]
Sent: Thursday, August 04, 2005 9:30 PM
To: [b2 b6]

Cc: [b2 b6]
Subject: NCRCG TTX: Advance packet for Cyber Storm Tabletop Exercise, 9 Aug 05

All,

Please see the message below and attachments for additional information concerning the 9 August NCRCG TTX.

Thanks,
[b2 b6]

From: [b2 b6]
Sent: Thursday, August 04, 2005 7:06 PM
To: [b2 b6]

Cc: [b2 b6]
Subject: Advance packet for Cyber Storm Tabletop Exercise, 9 Aug 05

Thank you in advance for your participation in the Cyber Storm Tabletop Exercise (TTX), scheduled for Tuesday, August 9th. The TTX will involve members of the Interagency Incident Management Group (IIMG), National Cyber Response Coordination Group (NCRCG), U.S. Computer Emergency Readiness Team (US-CERT), and the Homeland Security Operations Center (HSOC). Please find attached:

- TTX overview
- overviews of the IIMG and NCRCG
- NRP Cyber Incident Annex
- seating arrangement
- player book Table of Contents
- directions to the Transportation Security Operations Center [b2]

In addition to the attachments mentioned above, a DRAFT flow chart depicting the response and information sharing process during a cyber related Incident of National Significance has been developed and is provided as another tool to assist in the TTX discussion.

As a reminder, the exercise is for the principal representative of your Department/Agency to the IIMG and NCRCG, along with other specifically invited offices/personnel. If additional attendance or representation is desired, please send your request to your group POC in order to coordinate available space. Requests will be

considered on a space available basis.

Although the exercise is unclassified, the [

b2]

The schedule is as follows:

7:30	Check-in (for 100+ people) will begin - YOU MUST BE PRE-REGISTERED! Additional security staff will be added, but they advise arriving at least 20 minutes early. Morning refreshments will also be available beginning at 7:30 a.m.
8:30	STARTEX
11:30	Working lunch
2:00	ENDEX

Thank you and we look forward to your participation in the Cyber Storm TTX.

rl

Jeffrey H. Wright
Director, Exercise Program
National Cyber Security Division
US Department of Homeland Security
[b2] (office)
(mobile)
(fax)

P92

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

b5

Cyber Storm 2005
Final Planning Conference
September 26-27, 2005
U.S. Department of Homeland Security
National Cyber Security Division

[b2]

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

Agenda
Day 1

0730-0830	Sign-in	
0830-0845	Welcome & Opening Remarks	Mr. Andy Purdy Acting Director, NCSD
0845-0850	Conference Overview	Mr. Jeff Wright Exercise Program Director, NCSD
0850-1000	Exercise Design & Policy Update Introductions and Logistics Brief Overview of the Exercise Exercise Update ▪ Participation/Scope Management ▪ Information Protection & Security ▪ Public Affairs ▪ After Action Review ▪ White Cell Composition ▪ Communications Support	[b6] Cyber Storm Exercise Director b6 b2
1000-1015	*Break*	
1015-1130	Scenario Overview [b6] MSEL Management (NXMSEL) Breakout Group Plan	
1130-1215	*Lunch*	
1230-1600	Scenario Development & Inject Building Breakout Teams ▪ Intelligence/Law Enforcement ▪ Information Technology/Telecommunications ▪ Energy Infrastructure ▪ Transportation Infrastructure	Team Leads
1615-1630	Wrap-Up *(all assemble)*	Mr. Jeff Wright

FPC Agenda *(continued)*

Day 2

0730-0830	*Arrival*	
0830-0945	Breakout Teams Inject Development Completion *(team rooms)*	Team Leads
0945-1000	*Break*	
1000-1130	Team Composite Scenario Review *(team rooms)*	Team Leads
1130-1230	*Lunch*	
1230-1415	Plenary Composite Scenario Review	[b6 b2]
1415-1430	*Break*	
1430-1530	Plenary Composite Scenario Review	
1530-1600	Wrap-Up/Way Ahead	Mr. Jeff Wright

P 93

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

National Cyber Security Division

National Cyber Exercise: Cyber Storm 2005

Final Planning Conference

September 26-27, 2005

Homeland Security

FOR OFFICIAL USE ONLY
Exercise Sensitive, Pre-Decisional Material, Not for Dissemination

Cyber Storm 05 Overview

Exercise Objectives

- **Exercise the national cyber incident response community with a focus on:**
  - Interagency Coordination through the Interagency Incident Management Group (IIMG) and National Cyber Response Coordination Group (NCRCG)
  - Intergovernmental coordination and incident response vertically (Federal-State) and horizontally (international)
  - Identification of policies/issues that hinder effective cyber response & recovery
  - Identification of critical information sharing paths and mechanisms;
  - Identification and improvement of public-private collaboration, procedures and processes for:
    - Establishing situational awareness
    - Supporting critical and time sensitive decision making
    - Communicating appropriate information to key stakeholders and the public
    - Planning and implementing appropriate response and recovery activities in conjunction with the private sector
- **Highlight available tools and analytical capability that can be employed for cyber incident response and recovery**

[b2 b5]

- **Raise awareness of the economic and national security impacts associated with a significant cyber incident**

Homeland Security

Cyber Storm 05 Overview

Exercise Design

- **CYBER STORM 2005 will be:**

b2
b5

Homeland Security

Cyber Storm 05 Overview

Context and Scope

- **Large-scale cyber incident affecting multiple critical infrastructure sectors:**

  [b2 b5]

  - IT and Telecommunications
  - Transportation
  - Energy

- **Cyber Storm 2005 WILL include:**
  - Cyber attacks and potentially complimentary physical attacks disrupting transportation and energy infrastructure elements
  - Cyber attacks targeted at the IT infrastructure of State, US Federal and other national Government agencies intended to degrade government operations/delivery of public services, diminish the ability to remediate impacts on other infrastructure sectors, and undermine public confidence

- [b2]

Homeland Security

Cyber Storm 05 Overview

Scenario Elements

- **Adversary: Non-terrorist, politically motivated "hack-tivist"**
- **Coordinated, Campaign-Level Cyber Attack to achieve a specific political agenda (economic and public trust impact)**

b2

b5

Homeland Security

Cyber Storm 05 Overview

Exercise Timeline

[b5]

[b2]

- Will include build-up, crisis, and response/recovery phases
- Exercise play in real-time with time jumps to allow full crisis lifecycle
- Five-day phased, distributed exercise that includes a 36-hour period of 24x7 play

Homeland Security

Cyber Storm 05 Overview

Stakeholders and Participants

- **Department of Commerce**
  - National Telecommunications & Information Administration
  - Bureau of Industrial Standards
- **Department of Defense**
  - OASD NII
  - Joint Staff
  - NORTHCOM
  - STRATCOM
  - Joint Force Component Command – Net Warfare
  - Joint Task Force – Global Network Operations
- **Department of Energy**
  - Office of Energy Reliability

  [b2 b5]
- **Department of Justice**
  - Computer Crime and Intellectual Property Section
  - Federal Bureau of Investigation
- **Department of State**
  - Bureau of Diplomatic Security

  [b2 b5]
- **Department of Transportation**
  - Crisis Management Center Federal Aviation Administration
- **Department of Treasury**

  [b2 b5]
- **Central Intelligence Agency**
- **National Security Agency**
  - National Threat Operations Center/ National Security Incident Response Center
- **Federal Deposit Insurance Corporation**
- **Office of Management & Budget**
- **National Security Council**
- **Homeland Security Council**
- **American Red Cross**
- **Multi-State ISAC**
- **Michigan** [b5]
- **Montana** [b5]
- **New York** [b5]
- **Information Technology ISAC**
  - Microsoft [b4] Symantec, McAfee, [b2] and others
- **Telecommunications ISAC**

  [b2]
- [b2]
  - Electric Sector ISAC

  [b2 b4]
- **Transportation Private Sector**

  [b2 b5]
- **International Participants**
  - Canada – Public Safety and Emergency Preparedness Canada
  - UK – National Infrastructure Security Co-Ordination Centre
  - Australia – Attorney General's Office
  - New Zealand – Centre for Critical Infrastructure Protection
- **Interagency**
  - National Cyber Response Coordination Group
  - Interagency Incident Management Group

Homeland Security

Cyber Storm 05 Overview

Stakeholders and Participants

- **Department of Homeland Security**
  - National Cyber Security Division/US-Cyber Emergency Response Team
  - National Communications Service
  - Transportation Safety Agency/Transportation Safety Operations Center
  - US Secret Service
  - Homeland Security Operations Center
  - Homeland Security Information Network
  - Protected Critical Infrastructure Information Program
  - Infrastructure Coordination Division
  - Information Analysis
  - Protective Services Division
  - Immigration and Customs Enforcement (Customs and Border Protection)
  - Science & Technology
  - Integration - Staff/Incident Management Division
  - Office of Legislative Affairs
  - Office of Public Affairs
  - Office of International Affairs
  - Office of General Counsel
  - Office of State and Local Government Coordination and Preparedness

Homeland Security

Cyber Storm 05 Overview

Planning Schedule

b5

Homeland Security

Information and Security Policy and Procedures

FOR OFFICIAL USE ONLY
Exercise Sensitive, Pre-Decisional Material, Not for Dissemination

b2 b5

Pages 10-11

DHS Office of Public Affairs (OPA)

FOR OFFICIAL USE ONLY
Exercise Sensitive, Pre-Decisional Material, Not for Dissemination

b2 b5

Public Affairs Working Group (PAWG)

- DHS Public Affairs will establish a Public Affairs Working Group (PAWG) to assure that all participating offices/organizations are prepared together to work and function as a team during the exercise. Activities include but are not limited to:

b5

- The PAWG will include public affairs representatives from all exercise counterparts, including International, interagency, State, and private sector
- The PAWG will meet as coordinated by OPA.

b5

- Anticipated first meeting / teleconference NLT Oct. 14

Homeland Security

Public Affairs Pre-Exercise Effort

- OPA will coordinate and execute a pre-exercise public affairs incident communications rehearsal for all participants' public affairs representatives. This rehearsal will:
  - Identify communications methods and channels
  - Define roles and responsibilities at all levels
  - Develop a cooperative public affairs team effort among International, Federal, State and private sector participants
  - Refine public affairs coordination processes
- Anticipated date: first week of November (Proposed ~Nov 2)

Homeland Security

b2 b5

VIP Observer Program Overview

- The VIP Observer Program will provide an opportunity to
  - Observe the Cyber Storm exercise
  - Understand how it will further the public and private sectors' ability to more effectively and efficiently respond to a cyber attack
- Any Stakeholder or Player organization may sponsor VIP visitor(s)

[b5]

Homeland Security

Areas for Consideration

b5

Homeland Security

b2 b5

Pages 19 - 22

After Action Review

Homeland Security

b2 b5

Pages 24 - 28

Final After Action Report

- Final Report will cover all aspects of exercise development and design, execution, findings and recommendations

[b5]

- DHS-specific findings and recommendations will be reviewed

[b5]

Homeland Security

FOR OFFICIAL USE ONLY
Exercise Sensitive, Pre-Decisional Material, Not for Dissemination

White Cell Composition & Requirements

Functions

- ▸ Provide response for simulated offices/exercise control
  - National (POTUS, SecDHS) [b5]
  - Sector (ISACs, Threads)
  - SMEs (IT, States, Foreign)
- ▸ Guide agency participation to meet specific Goals & Objectives
- ▸ Scenario Injects
- ▸ Respond to Requests For Information (RFI)

Homeland Security

White Cell Composition

Homeland Security

White Cell Composition & Requirements

Composition

[b2 b5]

ion,

Homeland Security

FOR OFFICIAL USE ONLY
Exercise Sensitive, Pre-Decisional Material, Not for Dissemination

White Cell Structure

[redacted]

b2
b5

Homeland Security

FOR OFFICIAL USE ONLY
Exercise Sensitive, Pre-Decisional Material, Not for Dissemination

White Cell Structure

b2
b5

Homeland Security

White Cell Composition & Requirements

Mechanics

[b2 b5]

Homeland Security

Communications Support

Homeland Security

FOR OFFICIAL USE ONLY
Exercise Sensitive, Pre-Decisional Material, Not for Dissemination

b2 b5

Pages 37 - 38

Scenario Overview

Homeland Security

FOR OFFICIAL USE ONLY
Exercise Sensitive, Pre-Decisional Material, Not for Dissemination

b2 b5

Pages 40 - 45

MSEL Management

Homeland Security

b2 b5

Pages 47 - 56

POINTS OF CONTACT

Jeff Wright
Exercise Program Director, NCSD
[b2 b6]

[b6 b2]
Exercise Program Coordinator, NCSD
[b2 b6]

[b2 b6]
Cyber Storm Exercise Director
[b2 b6]

[b2 b6]
Cyber Storm Program Manager
[b2 b6]

Homeland Security

FOR OFFICIAL USE ONLY
Exercise Sensitive, Pre-Decisional Material, Not for Dissemination

P94

Withheld in Full

b2 b4 b5 b6

10 Pages

Pg 6

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

Department of Commerce

- National Telecommunications & Information Administration
- [b2]

Department of Defense

- OASD NII
- Joint Staff
- NORTHCOM
- STRATCOM
- Joint Force Component Command - Net Warfare
- Joint Task Force - Global Network Operations

Department of Energy

- Office of Energy Reliability

Department of Justice

- Computer Crime and Intellectual Property Section
- Federal Bureau of Investigation

Department of State

- [b2]
- Bureau of Diplomatic Security

Department of Transportation

- Crisis Management Center Federal Aviation Administration

Executive Office of the President

- Office of Management and Budget
- National Security Council
- Homeland Security Council

Interagency

- National Cyber Response Coordination Group
- Interagency Incident Management Group

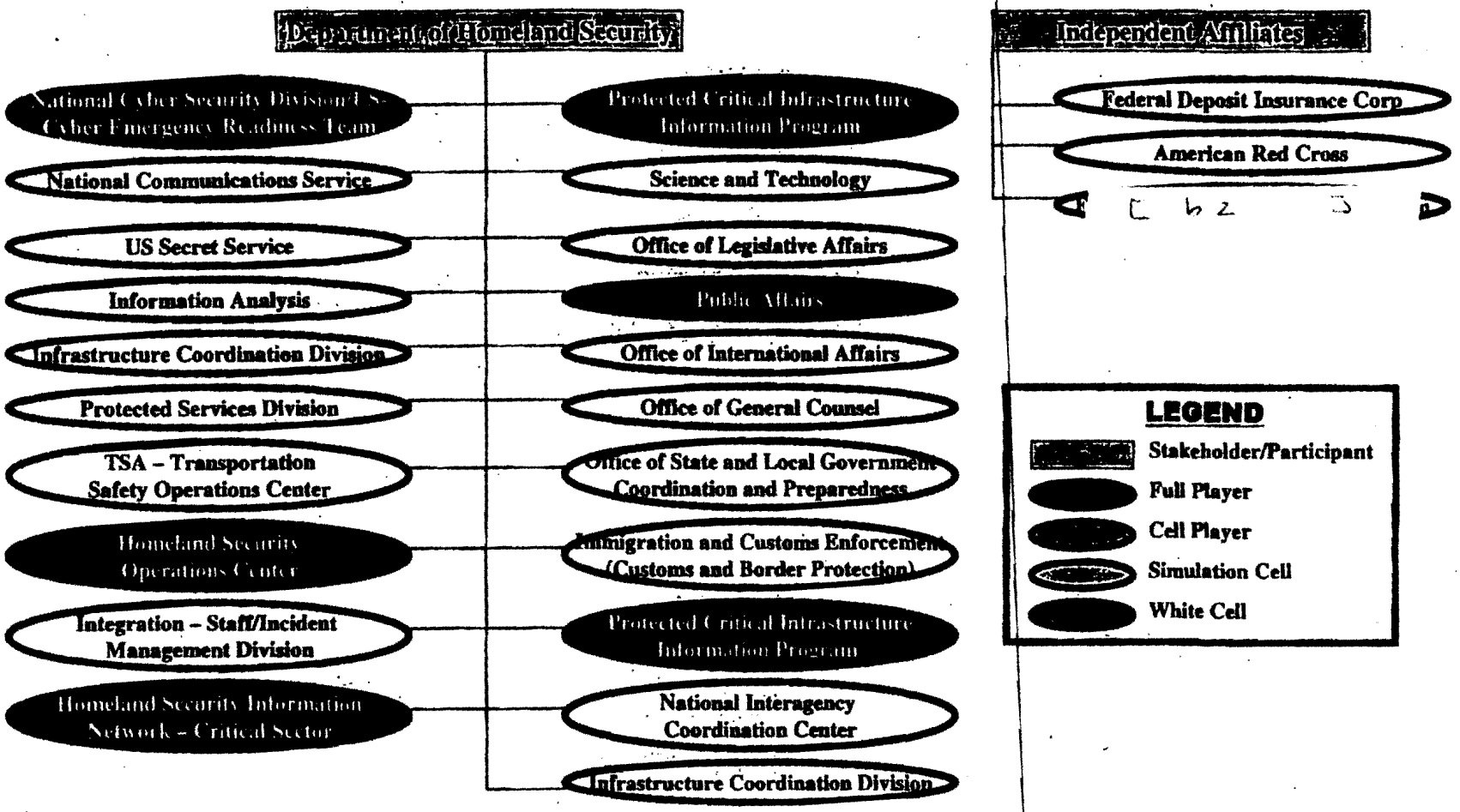
North American Electric Reliability Council

- Electric Sector ISAC
- [b2]

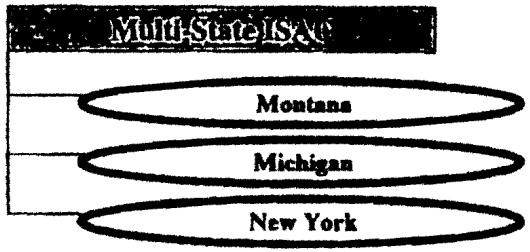
LEGEND

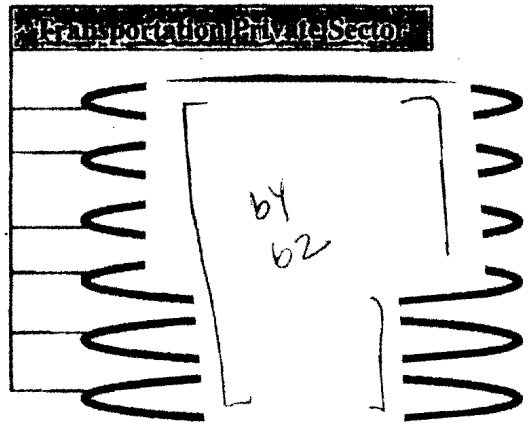
- Stakeholder/Participant
- Full Player
- Cell Player
- Simulation Cell
- White Cell

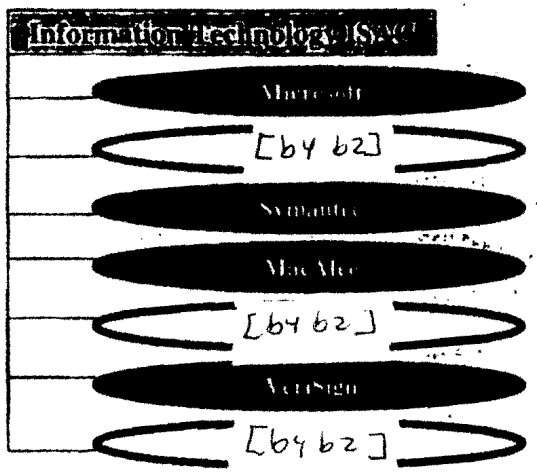
Homeland Security

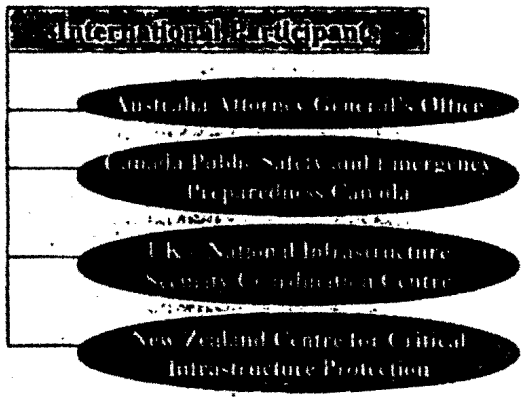


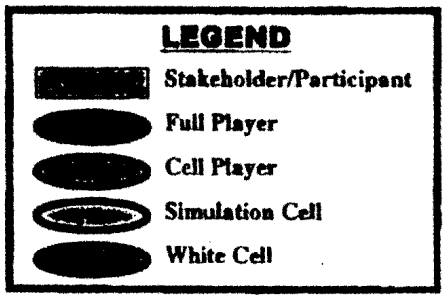
Homeland Security











Homeland Security

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

P97.

Cyber Storm 2005

Stakeholders and Participants

- **Department of Commerce**
  - o National Telecommunications & Information Administration
  - [b2]
- **Department of Defense**
  - o OASD NII
  - o Joint Staff
  - o NORTHCOM
  - o STRATCOM
  - o Joint Force Component Command – ~~Net Warfare~~
  - o Joint Task Force – Global Network Operations
- **Department of Energy**
  - o Office of Energy Reliability
  - [b2]
- **Department of Justice**
  - o Computer Crime and Intellectual Property Section
  - o Federal Bureau of Investigation
- **Department of State**
  - o Bureau of Diplomatic Security
  - [b2]
- **Department of Transportation**
  - o Crisis Management Center
  - o Federal Aviation Administration
- **Department of Treasury**
  - [b2]
- **Central Intelligence Agency**
- **National Security Agency**
  - o National Threat Operations Center/ National Security Incident Response Center
- **Federal Deposit Insurance Corporation**
- **Office of Management & Budget**
- **National Security Council**
- **Homeland Security Council**
- **American Red Cross**
- **Multi-State ISAC**
- **Michigan**
- **Montana**
- **New York**
- [b2]
- **Information Technology ISAC**
  - [b4 b2]
- **Telecommunications ISAC**
  - [b2]
  - [b2]
  - o Electric Sector ISAC
  - [b2]
- **Transportation Private Sector**
  - [b4 b2]
- **International Participants**
  - o Canada – Public Safety and Emergency Preparedness Canada
  - o UK – National Infrastructure Security Co-Ordination Centre
  - o Australia – Attorney General's Office
  - o New Zealand – Centre for Critical Infrastructure Protection
- **Interagency**
  - o National Cyber Response Coordination Group
  - o Interagency Incident Management Group
- **Department of Homeland Security**
  - o National Cyber Security Division/ US-Cyber Emergency Response Team
  - o National Communications Service
  - o Transportation Safety Agency / Transportation Safety Operations Center
  - o US Secret Service
  - o Homeland Security Operations Center
  - o Homeland Security Information Network
  - o Protected Critical Infrastructure Information Program
  - o Infrastructure Coordination Division
  - o Information Analysis
  - o Protective Services Division
  - o Immigration and Customs Enforcement (Customs and Border Protection)
  - o Science & Technology
  - o Integration - Staff / Incident Management Division
  - o Office of Legislative Affairs
  - o Office of Public Affairs
  - o Office of International Affairs
  - o Office of General Counsel
  - o Office of State and Local Government Coordination and Preparedness

Points of Contact

[b2 b6]
Exercise Program Director, NCSD
[b2 b6]

[b2 b6]
Cyber Storm Exercise Director
[b2 b6]

P98

Homeland Security

National Cyber Exercise - Cyber Storm 2005

Final Planning Conference

September 26-27, 2005

Conference Objectives

- ~~Finalize and Integrate Scenario~~
- Finalize Player List and Level of Play
- Identify Trusted Agents

Monday, September 26	Tuesday, September 27
0730-0830 Registration	
0830-0850 Welcome and Opening Remarks	**0730-0830 Arrival**
0850-1130 Exercise Update	**0830-1130 Breakout Groups**
1130-1215 Lunch	b2 b5
1230-1600 Breakout Groups	
b2 b5	**1130-1230 Lunch**
	1230-1530 Scenario Review
	1530-1600 Closing Remarks
1615-1630 Day 1 Wrap-Up	

b2 b5

Pages 2 - 3

P101

Withheld in Full

b2 b5

1 Page

P10L

Homeland Security

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

December 16, 2005

MEMORANDUM FOR:

National Cyber Response Coordination Group
Interagency Incident Management Group
Director, Homeland Security Operations Center

FROM: Jeff Wright, National Cyber Security Division Exercise Program

SUBJECT: Cyber Storm Preparation Exercise, January 05, 2006

This memorandum is to invite your organization to participate in the Cyber Storm Preparation Exercise II (PrepEx II), sponsored by the Department of Homeland Security – National Cyber Security Division (DHS-NCSD). This tabletop exercise (TTX) is the fifth exercise in the National Cyber Response Coordination Group (NCRCG) series and the second exercise specifically intended to serve as a building block for Cyber Storm full scale exercise (FSE) scheduled for February, 2006.

PrepEx II will be held on January 05 2006, from 8:00 a.m. to 2:00 p.m., at the Department of Homeland Security National Cyber Security Division, [b2] This TTX will be a joint exercise with the National Cyber Response Coordination Group (NCRCG) and US-Computer Emergency Readiness Team (US-CERT), as well as select representatives from the Interagency Incident Management Group (IIMG) and Homeland Security Operations Center (HSOC).

PrepEx II is focused on further development and coordination of the operational procedures and standard operating processes that will be exercised during the Cyber Storm FSE in February 2006. The TTX objectives are:

- Provide the NCRCG an opportunity to review and refine their initiation triggers and procedures
- Review the current Standard Operating Procedures (SOP)
- Execute and evaluate NCRCG stand-up and initial procedures
- Coordinate procedures with the IIMG and HSOC
- Identify specific actions required prior to Cyber Storm FSE

Please provide the name, phone number, and email address of the individual(s) who will represent your department or agency at the TTX to [b2 b6] no later than COB December 29, 2005.

Attachment:
Agenda

P104A

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

Agenda for the NCRCG Preparation Exercise II
January 05, 2006

[b2]

0730: Participant check-in

[b2]

0800: Introductions and administrative remarks

0815: Exercise overview and review of SOP

0845: NCRCG stand-up triggers

0915: Break

0930: Begin Scenario 1

1100: Break

1115: Begin Scenario 2

1215: Break and working lunch service

1245: Begin Scenario 3

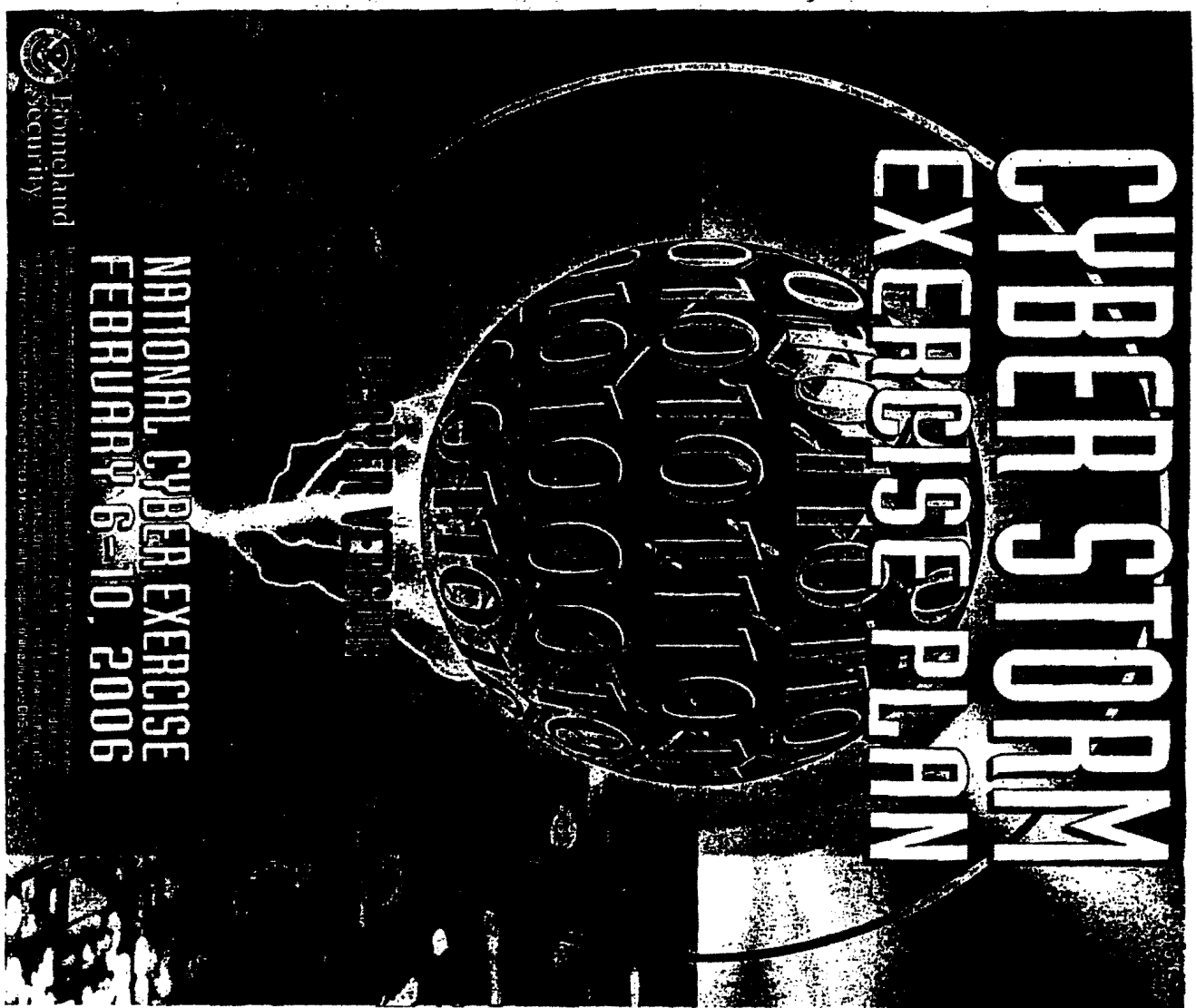
1330: Recap of exercise and [b2]

1400: End of exercise

b5
b2

P113

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS



CYBER STORM
EXERCISE QUICK START GUIDE
February 6–10, 2006

EXERCISE KICK-OFF TELECONFERENCE: Mon. Feb. 6 at 1140 EST (1640 GMT)
Call-in Number: [b2]
Participant ID: [b2]

DAILY SCHEDULE OF EXERCISE PLAY

	Mon. Feb. 6 Day 1	Tue. Feb. 7 Day 2	Wed. Feb. 8 Day 3	Thu. Feb. 9 Day 4	Fri. Feb. 10 Day 5
Observers / Controllers	[b2]				
Players/ Participants					

[b2]

Cyber Storm in the Media

An organization may respond to inquiries on their participation during the exercise. Responses should be channeled through the organization's public affairs office. All other media inquiries such as those pertaining to the exercise itself, other participants, or DHS role, *contact the DHS Press Office at* 202-282-8010.

Cyber Storm Communications

1. The following criteria should appear on all email communications:
   - Insert [b2] on all email correspondence as a CC.
   - Email shall be sent only to or from Cyber Storm ExCon and between players and other organizations.
   - The [b2] email should be included on all original emails, replies and forwarded email correspondence.
2. [b2]) users participating in the Cyber Storm exercise should include the following email address in all correspondences: [b2]
3. Other communications such as phone, secure phones, faxes, CWIN, HSIN Portal, and US-CERT portal should be recorded by an observer/controller.
4. See the back of this sheet for communications protocol and guidelines.

Using a Cyber Storm Email Account

1. Observer/Controller or Player: Use MS Outlook Web Access for all email correspondence.
2. Web address: [b2] [b2]
3. Domain name:
4. User name: [b2] id

NEED HELP? Email or call:	Email address	Telephone
Exercise Help Desk	[b2]	[b2]
Technical Support	[b2]	[b2]
Exercise Status Hot Line: [b2]		

Password

1. Participants staged at the [b2] in Washington, DC will receive a password at pre-STARTEX.
2. Participants staged at a location other than the Cyber Storm Exercise Control facility in Washington, DC, will receive a password provided to them either by personal email account or by telephone call.
3. Users who have not received a password should contact the network support desk at [b2] or at [b2] beginning Monday, February 6, 2006 at 0600 EST.

Exercise Participant General Guidelines

- You will receive an official message from ExCon indicating that the exercise has begun. The text of that message will read:
  - ***EXERCISE CYBER STORM HAS COMMENCED.***
- At each PAUSEX and RESTARTEX you will receive a message:
  - ***EXERCISE CYBER STORM HAS PAUSED, EXPECTED RESTART IS SET FOR .....***
  - ***EXERCISE CYBER STORM HAS RESUMED.***
- ENDEX for active play is scheduled for .... and you will receive a message from ExCon that includes the text:
  - ***EXERCISE CYBER STORM HAS CULMINATED AS OF (TIME)***
- When exercise play dictates the need to contact another party, the player should
  1) Look in the directory to se if there is a listing for that party or organization in the directory. If so, contact that person using the contact information provided in the directory
  2) If that party or organization is not listed in the exercise directory, that indicates they are outside the exercise perimeter.
     a. Contact [b2] and tell the switchboard operator the name and organization of the party that you would have contacted if the event is real.
     b. Exercise control using industry experts and agency representatives will simulate that party's response to the best of their ability within the context of the game.
- All e-mails must have a subject line that begins with .EXERCISE CYBER STORM.
- The text message must begin and end with the words: EXERCISE EXERCISE EXERCISE
- Any other written communications (FAX, paper memo's, presentation slides, etc.) should also be clearly marked at the beginning and end of the communication with the EXERCISE EXERCISE EXERCISE banner.
- All phone conversations must begin and end with the words, "This call is part of Cyber Storm Exercise Play."
- The Exercise Help Desk can be reached at [b2] or email [b2] [b2]
- For questions about exercise rules, play , and protocol, please call [b2], or e-mail [b2]

For Injects Originating from Exercise Control the following protocol will be used:

- Phone ***"This is your name from "Cyber Storm"/ "National Cyber Exercise" and this is an inject for the exercise..... Thank you and this ends the exercise inject"***
- Fax Top and Bottom ***EXERCISE EXERCISE EXERCISE***
- Email Top and Bottom ***EXERCISE EXERCISE EXERCISE***
- Simulated Reports Top and Bottom ***EXERCISE EXERCISE EXERCISE***
- For all communications, avoid the use of participating company/entity names in order to maintain anonymity, i.e., Major Software Vendor
- Simulated if a player is not part of the exercise or listed in the directory, do not choose the next best option. Contact Exercise Control (email, phone, etc.), state who you are trying to contact and ExCon will simulate the role

Department of Homeland Security

CYBER STORM
Exercise Plan (EXPLAN)

Player Version

February 6–10, 2006

Department of Homeland Security
National Cyber Security Division

This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

Contents

EXECUTIVE SUMMARY 1
1. INTRODUCTION 5
2. PURPOSE OF THE EXERCISE 6
3. CYBER STORM OBJECTIVES 6
4. SCOPE 7
5. SCENARIO 8
6. ASSUMPTIONS 9
6.1 EXERCISE PLAY 9
6.2 EXERCISE ATTACKER 10
6.3 TARGETED RANGE OF RESPONSE 10
7. INTERAGENCY ROLES AND RESPONSIBILITIES 11
7.1 DEPARTMENT OF HOMELAND SECURITY 11
7.2 STAKEHOLDERS 13
7.3 STATE GOVERNMENT 13
7.4 PRIVATE SECTOR ORGANIZATIONS 13
7.5 INTERNATIONAL SECTOR 13
8. EXERCISE STRUCTURE 14
8.1 EXERCISE MANAGEMENT TEAM 14
8.2 PLAYERS 14
8.3 EXERCISE CONTROL CELL 14
8.4 MASTER SCENARIO EVENTS LIST (MSEL) MANAGEMENT 15
8.5 AFTER ACTION REVIEW AND ANALYSIS 15
8.6 COMMUNICATIONS AND NETWORK DESIGN 15
9. SECURITY GUIDELINES AND SAFETY MEASURES 16
9.1 SECURITY GUIDELINES 16
9.2 SAFETY MEASURES 16
9.3 OPERATIONAL CONTINGENCIES 16
10. AUTHORITIES AND REFERENCES 18
11. ACRONYMS AND ABBREVIATIONS 19
12. GLOSSARY OF TERMS 23
13. KEY MILESTONES 27

ANNEXES

A Cyber Storm Concept of Operations A-1

B Participating Stakeholders and Organizations B-1

C Public Affairs C-1

D Data Collection Process and After Action Review D-1

E Security Policy and Procedures E-1

Executive Summary

The Department of Homeland Security (DHS)/National Cyber Security Division (NCSD) has been central in sponsoring the National Cyber Exercise (NCE) Cyber Storm. Congress has provided specific directions for implementation of Fiscal Year 2005 appropriations for full execution of this program in coordination with the DHS National Exercise Program implementers. To this end, Cyber Storm, a large-scale, functionally based exercise is scheduled to take place at [b2] on February 6–10, 2006.* Cyber Storm draws participation from a multitude of organizations within public, private and international sectors.

The NCE Cyber Storm is mandated under authorities and references as provided within this document. In addition, the exercise will emphasize and provide necessary enhancements to the Cyber Incident Annex of the National Response Plan (NRP) as a result of policy determinations on preparedness and protection of critical cyber infrastructures across all sectors.

Stakeholders and participants will gain a necessary understanding of critical cyber security response and recovery processes and the cyber response community's coordination, communications, and cooperation capabilities through a controlled environment as provided by Cyber Storm. Participants, i.e., players and planners, include a range of subject matter experts and staff from Federal departments/agencies (D/A), including defense, civil, intelligence and law enforcement communities; State governments; private industry; and select international partners. This document includes a listing of participating organizations.

Further, several DHS organizations have been integrally involved in the coordination and implementing of policy and planning, as well as assuming the role of exercise control support and exercise players. Through stakeholder interviews and several planning conferences and meetings, planners have developed the necessary strategies, methodology, and operational processes and procedures in preparation for Cyber Storm's execution.

The Cyber Storm Exercise Plan (EXPLAN) is the principal planning document and guide for government, public, and private sector personnel who will participate in Cyber Storm. Collaboration of leadership, stakeholders, planners, players, and controllers is essential to achieve a common baseline in execution of homeland security cyber response and recovery mechanisms. The EXPLAN annexes serve both as a resource and information guide required to carry out all the technical, operational and logistical aspects of the exercise.

---

* NCSD has been preparing and coordinating efforts for this international and national exercise since August 2004. The Cyber Storm exercise was originally scheduled for November 2005; however, the devastating events of the hurricane season prompted exercise participants and stakeholders from private and government sectors to request a postponement until February 6–10, 2006.

GOALS AND OBJECTIVES

As identified in the Concept of Operations (CONOPS), the primary goal of Cyber Storm as articulated by its governing leadership and identified stakeholders is to:

> Exercise, within the context of a cyber incident of national significance, the national cyber incident response community's policy; information sharing mechanisms; and its procedures and processes for establishing situation awareness, supporting public and private sector decision making, communicating appropriate information to the public, and planning and implementing appropriate response and recovery activities.

Secondary goals of the exercise are to:

- Identify and publicize specific tools and analytical capability that the cyber community as a whole can take advantage of in the preparation for and response to incidents; and
- Raise awareness, both inside and outside of the cyber community, the national security and economic impacts associated with a cyber incident of national significance.

EXERCISE SCOPE

Cyber Storm is an objectives-driven, no-fault exercise.

b2

Cyber Storm's scope is sector-focused. The scenario involves actual participation by a wide range of organizations. By definition at the highest level, the exercise will concentrate exclusively on the cyber implications of incidents occurring within the sectors: energy, information technology (IT)/telecommunications (combined for purpose of this exercise only) and transportation.

b2

The Cyber Storm scenario is inject-driven. The exercise is based on plausible, real-world attacks and has been limited to four distinct attack vectors that (1) target and disrupt the cyber and physical critical infrastructure of the sectors; (2) reduce and degrade public confidence in State and Federal government and their operations; (3) reduce ability of local governments to remediate impacts of specific attacks. The DHS Office of Public Affairs will have a key role in formulating responses to the injects as they evolve during the exercise.

EXERCISE STRUCTURE

b2

This page intentionally left blank.

CYBER STORM EXPLAN

1. Introduction

The Department of Homeland Security (DHS)/National Cyber Security Division (NCSD) has by congressional mandate been tasked and funded to develop and conduct the National Cyber Exercise (NCE) Cyber Storm. The National Cyber Exercise, Cyber Storm, is being planned in accordance with authorities mandated under Homeland Security Presidential Directive 8 (HSPD-8), the National Response Plan (NRP), and the President's Strategy to Secure Cyber Space (National Cyberspace Strategy), as well as by several government authorities and regulations, as listed in Section 10 of this document, and draws participation from public, private and international sectors.[2]

b2

As stated within the DHS/NCSD Cyber Storm Concept of Operations (CONOPS) (see Annex A), the primary goal for Cyber Storm is to exercise, within the context of a cyber incident of national significance,

- National policies relating to cyber incident response
- Information sharing mechanisms
- Procedures and processes for establishing situation awareness
- Public and private sector decision making
- Communication of appropriate information to the public
- Response and recovery activities.

Secondary goals of the exercise are to:

- Identify, publicize, and capitalize on specific tools and analytical capabilities for the community as a whole
- Raise the community's awareness on national security and economic impacts associated with a cyber incident of national significance.

This approach will help stakeholders and participants to gain a necessary understanding of critical cyber security response and recovery processes and the cyber response community's coordination, communications, and cooperation capabilities. Participants include Federal departments/agencies (D/A), including defense, civil, intelligence and law enforcement communities; state agencies; private industry; and select international partners. Annex B contains the current listing of D/As, private sector organizations, state and international participants.

[2] Originally scheduled for execution in November 2005, the events of Hurricanes Katrina and Rita prompted the decision by key Federal and private sector players to postpone Cyber Storm to February 6-10, 2006.

The Cyber Storm Exercise Plan (EXPLAN) is the principal planning document and guide for government, public, and private sector personnel who will participate in Cyber Storm. This document also serves as a resource outlining objectives, roles and responsibilities, schedule, exercise management organization of various constituents within the interagency cyber community, and other pertinent information required to ensure the success of the exercise. The EXPLAN will be distributed to exercise leadership, stakeholders, planners, players, and controllers to ensure a common baseline is met to exercise homeland security cyber response and recovery mechanisms. The EXPLAN contains resource annexes relevant to the execution of Cyber Storm.

2. Purpose of the Exercise

The public and private sector's increasing reliance on cyber infrastructure has increased the risk of a potential attacker conducting cyber-based attacks with impacts on our national defense and economy.

[b2]

A key purpose of Cyber Storm is to exercise and evaluate policy and procedures in response to these attacks, and identify where further planning and process improvement may be needed. It will exercise key organizations within the Federal response infrastructure by activating both the National Cyber Response Coordination Group (NCRCG), comprised of senior representatives from Federal agencies; and the Interagency Incident Management Group (IIMG) per their standard operating procedures and as called for under the NRP and its Cyber Incident Annex.

[b2]

3. Cyber Storm Objectives

Cyber Storm is an objectives-driven, no-fault exercise. Exercise parameters and scenario details are based on

[b2]

b2

Achievement of exercise objectives and goals will be measured objectively through observations, lessons learned, and examination of policy and procedures

b2

4. Scope

Cyber Storm implementers will simulate a large-scale cyber incident affecting or disrupting multiple critical infrastructure elements primarily within the energy, information technology (IT) and transportation sectors, and secondarily within telecommunications.

b2

The adversary(ies) will stage *primary cyber attacks* and, in certain circumstances, may include complementary physical attacks against energy, transportation, and IT/telecommunications sectors. These attacks are intended to disrupt certain elements of critical infrastructure, potentially leading to cascading effects within other facets of the nation's economic, societal, and governmental structures. Cyber attacks will also be levied simultaneously against Federal, state, and international government infrastructure as a means to disrupt government operational capabilities, hinder their ability to respond to the impact of the primary attacks, and, subsequently, undermine public confidence in the government(s).

b2

5. Scenario

The design of sector-specific scenario injects will enable the testing, evaluation, and ultimately, the improvement of the ability to respond effectively to a cyber attack. The scenario design also allows public and private sectors to participate in simulated attack scenarios. Each scenario will compel exercise players to notify government authorities as appropriate, provide and/or receive guidance, activate and deploy interagency/private sector coordination groups, and respond to and recover from the simulated cyber attacks. Stakeholders will gain an understanding of critical cyber security weaknesses and the homeland security community's cyber response and recovery capabilities, underlining policy and resource requirements.

b2

The scenario timeline is in real-time with exercise play over a five-day period. The approach is implemented within three phases: (1) build-up, (2) crisis, and (3) response/recovery.

b2

b2

Figure 1. Exercise Scenario Timeline

The start of exercise (STARTEX) is on Monday, Feb. 6, 2006 at [b2]. The end of exercise or end of active play (ENDEX) is Thursday, Feb. 9, 2006 at [b2 GMT). "Full-stop" ENDEX (i.e., immediately after the scheduled tabletop exercise) occurs at] on Friday, Feb. 10, 2006. [b2]

6. Assumptions

6.1 Exercise Play

Cyber Storm, per its goals, objectives, and guiding authorities, will focus exclusively on the cyber implications which arise from a cyber incident.

b2

b2

7. Interagency Roles and Responsibilities

The interagency cyber response and recovery community will share responsibilities for the development, execution, and assessment of Cyber Storm within the framework of the purpose and objectives identified in this EXPLAN. Roles and responsibilities are described within the following sections as well as identified in the CONOPS.

7.1 Department of Homeland Security

7.1.1 NATIONAL CYBER SECURITY DIVISION

As the exercise sponsor, NCSD will develop, implement, and coordinate all aspects of Cyber Storm, including the creation of exercise policies in compliance with Federal and DHS exercise guidelines to protect stakeholders and national security interests.

b2

7.1.2 OFFICE OF PUBLIC AFFAIRS

The DHS Office of Public Affairs (OPA) will ensure proper coordination of pubic affairs aspects for the exercise by working closely with international, Federal, state, and private sector counterparts.

b2

Annex C provides additional details on the handling of public affairs by agencies.

b2

7.1.3 OFFICE OF LEGISLATIVE AFFAIRS

DHS Office of Legislative Affairs (OLA) will serve as the Department's primary interlocutor with Congressional members and entities as well as coordinate with the Office of Public Affairs.

b2

[b2]

[b2]

[b2]

7.1.7 US-CERT

The focal point within the Federal government for the National Cyberspace Security Response System under the National Cyberspace Strategy, US-CERT manages the National Cyber Alert System by relaying cyber security update and warning information to users across the public and private sectors. The system provides all citizens with free, timely, actionable information to better secure their computer systems. Office of Management and Budget (OMB) Memorandum M-04-25 identifies US-CERT as the Federal Information Security Incident Center for Federal agencies. In addition, US-CERT provides direct input to the Homeland Security Operations Center (HSOC) and the Homeland Security Advisory System (HSAS) for cyber-related issues. US-CERT is the operational arm for the Federal government that deals with cyber vulnerabilities and threat warnings, as well as protection, detection, response and recovery actions for cyber incidents.

[b2]

7.2 Stakeholders

The exercise stakeholders include those from Federal, State, private and international sectors.

[b2]

7.3 State Government

The NCSD is working collaboratively with the States of Michigan, Montana, and New York within the construct of Cyber Storm to enhance collective performance in protecting the nation's critical infrastructure. The Cyber Storm exercise will be conducted in coordination with members of the Multi-State Information Sharing and Analysis Center (MS-ISAC), sector-specific Information Sharing and Analysis Centers (ISAC), and state offices of homeland security.

7.4 Private Sector Organizations

Private sector participation is in targeted infrastructure sectors and is being coordinated through sector-specific departments and industry associations.

[b2]

7.5 International Sector

International play will revolve around cyber incident response organizations in the public and private sector. The Department of State has invited and confirmed participation of Australia, Canada, New Zealand (NZ), and the United Kingdom (UK) in Cyber Storm.

[b2]

8. Exercise Structure

Several teams of individuals are required for the maintenance and execution of Cyber Storm. The following sections describe the overall team structure and composition.

8.1 Exercise Management Team

The Cyber Storm Exercise Management Team (EMT) has the chief responsibility for defining, designing, planning, and implementing all aspects of this exercise. Through the planning of several information gathering conferences, the team has worked closely with the Cyber Storm stakeholders to define their requirements and establish an overarching purpose, concept, structure, and objectives and goals. The preliminary knowledge gained from these efforts was used to build a framework, design the scenario, and establish an exercise observation and data collection process. The team is also responsible for fulfilling the exercise's administrative, logistical, safety, and security needs.

8.2 Players

[b2] Participants will take part in the Cyber Storm scenario experience and respond to scenario injects through the course of the exercise.

[b2]

Players are practitioners and experts who understand the interdependence of cyber systems and the negative impact that cyber attacks can release upon critical infrastructure.

[b2]

[b2]

b2

Pages 15 - 17

10. Authorities and References

The development of the Cyber Storm exercise is mandated within the following authorities and references as identified below:

- Department of Homeland Security, *National Strategy to Secure Cyberspace,* February 2003.
- DHS, Homeland Security Act of 2002.
- DHS Infrastructure Analysis Information Protectorate (IAIP), National Cyber Security Division, *Concept of Operations (CONOPS),* Aug. 15, 2005.
- DHS Interagency Incident Management Group (IIMG), *Interagency Integrated Standard Operating Procedures,* Mar. 14, 2005.
- DHS, Interim National Infrastructure Protection Plan (NIPP), v.1, February 2005.
- DHS, Livewire Baseline Exercise After Action Report: An Assessment by the IAIP Exercise Management Program, June 18, 2004.
- DHS, National Response Plan (NRP), Essential Support Function (ESF) 1, Transportation; ESF 2, Communications; ESF 5, Emergency Management; ESF 12, Energy; ESF 15, Emergency Public Information and External Communications, and Cyber Incident Annex, June 30, 2004.
- DHS, National Strategy for Homeland Security, 2003.
- DHS, National Cyber Response Coordination Group (NCRCG) Concept of Operations (CONOPS), v.3.0, February 2005.
- DHS *NCRCG Standard Operating Procedures* (SOPS), v.4.0, December 2005.
- DHS IAIP, National Cyber Security Division, CONOPS, Aug. 15, 2005.
- Federal Information Security Management Act of 2002, Public Law 107-347, December 2002. http://csirc.nist.gov/policies/FISMA-final.pdf
- Homeland Security Presidential Directive (HSPD) 5, *Management of Domestic Incidents,* Feb. 28, 2003.
- HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection, Dec. 17, 2003.
- National Institute of Standards and Technology (NIST) 800-34 (draft), *Guide to Single Organization IT Exercises,* 2005.
- OMB Memorandum M-04-25, Federal Information Security Incident Center, Aug. 23, 2004.
- U.S. Computer Emergency Readiness Team (US-CERT), Concept of Operations for Federal Cyber Security Incident Handling, v.2.4, February 2005.

b2

Pages 19 - 26

13. Key Milestones

Several conferences and key activities have been instrumental in the development and structuring of the Cyber Storm exercise. Collaboration among stakeholders, planners, participants, and potential players was a key issue in establishing exercise structure, policy, and procedures.

Event / Activity	Date
Initial Planning Conference	Mar. 1, 2005
Mid-term Planning Conference	May 23-24, 2005
NCRCG / IIMG Tabletop Exercise	Aug. 9, 2005
International Planning Conference	Sept. 7-8, 2005
NCRCG / DOD Tabletop Exercise	Sept. 20, 2005
Requirements and Scope Lock-Down Date	Sept. 27, 2005
State participation finalized • Private sector participation finalized • Participant objectives and expected outcomes complete	Continuous
Final Planning Conference	Sept. 26-27, 2005
First Dry Run (Exercise Staff Internal)	Oct. 3-4, 2005
Scenario Planning Conference	Nov. 15-16, 2005
VIP Invitations	Jan. 10, 2006
Final Master Scenario Event List Conference	Jan. 19-20, 2006
Exercise Cyber Storm	Feb. 6-10, 2006
After Action Report Conferences	Feb. 2006
Final After Action Report Published	Apr. 28, 2006

Annex A: Concept of Operations

This annex contains the approved version of the Concept of Operations (CONOPS) for the NCE Cyber Storm exercise. This document was drafted and approved in coordination with DHS executive leadership and defines the scope, objectives, and participants (see Annex B for current listing), as well as provides the baseline design concept and plan of action leading to the development of Cyber Storm.

This page intentionally left blank.

Department of Homeland Security
Preparedness Directorate
National Cyber Security Division

Concept of Operations (CONOPS)

National Cyber Exercise:
Cyber Storm

December 7, 2005

b2

Pages A-4 through A-27

Annex B: Participating Stakeholders and Organizations (as of 27 Jan 2006)

Department of Commerce

- National Telecommunications & Information Administration
- Bureau of Industrial Standards

Department of Defense

- Joint Staff
- National Military Command Center
- U.S. Northern Command
- U.S. Strategic Command
- Joint Force Component Command – Net Warfare
- Joint Task Force – Global Network Operations

National Security Agency

- National Threat Operations Center/National Security Incident Response Center

Department of Energy

- Office of Electricity Delivery and Energy Reliability
- Office of the Chief Information Officer
- Regional Power Administrations

Department of State

- Bureau of Diplomatic Security
- Bureau of Political-Military Affairs

Department of Transportation

- Crisis Management Center
- Federal Aviation Administration
- Transportation Cyber Incident Response Center
- Pipeline and Hazardous Materials Safety Administration

Department of Treasury

Department of Homeland Security

- National Cyber Security Division/US Computer Emergency Readiness Team
- National Communications System
- Transportation Security Administration/Transportation Security Operations Center
- U.S. Secret Service
- Homeland Security Operations Center
- Protected Critical Infrastructure Information Program
- Homeland Security Information Network
- Immigration and Customs Enforcement (Customs and Border Protection)
- Infrastructure Protection Division (NICC, CWIN)
- Information Analysis
- Science & Technology (DETER Testbed)
- Integration-Staff/Incident Management Division
- Office of Legislative Affairs
- Office of Public Affairs
- Office of International Affairs
- Office of General Counsel
- Office of State and Local Government Coordination and Preparedness

Department of Justice

- Computer Crime and Intellectual Property Section
- Federal Bureau of Investigation

Director for National Intelligence

- Central Intelligence Agency
- Intelligence Community Incident Response Center

Federal Deposit Insurance Corporation

Federal Reserve Bank of New York

Office of Management & Budget

National Security Council

Homeland Security Council

American Red Cross

Multi-State ISAC

State Government of Michigan

State Government of Montana

State Government of New York

[b2]

Information Technology ISAC

Microsoft Corporation

[b4 b2]

Symantec Corporation

McAfee Inc.

[b4 b2]

VeriSign, Inc.

Intel Corporation

Telecommunications ISAC

[b2]

Energy Private Sector

[b4 b2]

Electric Sector ISAC

[b4 b2]

Transportation Private Sector

[b4 b2]

International Lead Participants

Canada – Public Safety and Emergency Preparedness Canada

UK – National Infrastructure Security Co-Ordination Centre

Australia – Attorney General's Office

New Zealand – Centre for Critical Infrastructure Protection

Interagency

National Cyber Response Coordination Group

Interagency Incident Management Group

Annex C: Office of Public Affairs

This annex provides guidance for public affairs personnel, specifically their interaction with the media before and during the exercise. The release of information about the exercise to the media and general public will be coordinated by or through OPA. This office will distribute guidance on/procedures for the handling and release of information to the media to all participating D/As.

Overview of Public Affairs Activities

b2

Cyber Storm Public Affairs Working Group

OPA will establish the Public Affairs Working Group (PAWG) to ensure that all participating organizations and representatives are prepared to work and function as a team. The PAWG will

b2

b2 b6

Pages C-2 through C-3

Press Office
U.S. Department of Homeland Security
Homeland Security

Fact Sheet

Contact: Press Office 202-282-8010

Cyber Storm Exercise

Cyber Storm is a nationwide cyber security exercise that is expected to take place in early February 2006, to assess preparedness capabilities in response to a cyber incident of national significance. Cyber Storm is the Department's first cyber exercise testing response across the private sector as well as international, federal, and state governments. The exercise is an initiative that meets Homeland Security Presidential Directive 8 "*National Preparedness*" requirements found in Homeland Security Presidential Directive 8, is coordinated under the DHS National Exercise Program, and is in accordance with Congressional appropriations to conduct exercises that test response to cyber attacks on critical infrastructures. Cyber Storm is intended to act as a catalyst for assessing communications, coordination and partnerships across critical infrastructure sectors.

Goals and Objectives

Within the context of a large-scale cyber incident affecting the energy, information technology (IT), telecommunications, and transportation critical infrastructure sectors, the goal of Cyber Storm is to exercise the national cyber incident response community with focus on:

- Interagency coordination through the National Cyber Response Coordination Group (NCRCG) pursuant to the *Cyber Annex* to the *National Response Plan;*
- Identification of policy issues that affect response and recovery;
- Identification of critical information sharing paths and mechanisms among public and private sectors; and
- Identification, improvement and promotion of public and private sector interaction in processes and procedures for:
    - Establishing situational awareness;
    - Supporting public and private sector decision making;
    - Communicating appropriate information to key stakeholders and the public; and
    - Planning and implementing appropriate response and recovery activities.

Secondary goals of the exercise include:

- Highlighting specific tools and analytical capability that may be used in preparation for, response to, and recovery from cyber incidents; and
- Raising awareness of the economic and national security impacts associated with a significant cyber incident.

Participants

- Participants include members of the public sector (federal and state agencies), the private sector (IT, telecommunications, energy and transportation), and international government partners.

- Participants provided additional support staff to help plan and control the exercise to ensure it meets their organizations' training needs and supports the interests of their constituents.

The Scenario

Cyber Storm simulates a sophisticated cyber attack scenario. All "attacks" are pre-scripted and executed in a closed and secure environment, eliminating any external distress to participants' day-to-day systems during the exercise.

Scenarios may include:
- Cyber attacks disrupting energy and transportation infrastructure elements; and
- Cyber attacks targeted at federal, state and international governments with the intent of disrupting government operations and degrading public confidence.

Scenarios to generate participant actions through:
- Identification and efficient use of all communications channels;
- Escalation to a series of interrelated incidents that, combined, represent a significant enough threat to require (per the terms of the *Cyber Annex*) the stand-up and operation of the NCRCG ;
- The stand-up and operation of Interagency Incident Management Group (IIMG) while testing the communication relationship between the NCRCG and the IIMG; and
- Continued coordination of all public and private participants through the planning and recovery activities.

b2

b5

Pages C-6 through C-8

b2

Pages D-1 through D-10

b2

Pages E-1 through E-6

P114

Department of Homeland Security

TRANSFERRED TO OTHER AGENCY
TRANSFER FOR DIRECT REPLY - DHS

CYBER STORM
Exercise Directory

February 6–10, 2006

Department of Homeland Security
National Cyber Security Division

This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

Cyber Storm Participant Directory

By Organization

Note: This directory will be expanded, and an update version will be provided via electronic mail the morning of Monday, February 6, 2006.

Organization	Name	Role	Phone	E-mail
[b2]	[b2]			
Australia	[b2]			
Australia		All other roles		
[b2]	[b2]			m
[b2]	[b2]			
[b2]	[b6]			
[b2]	[b6]			
Canada		All other roles	b2	b2 b6 b4
[b2]	[b2]			
CIA [b2]		NCRCG		
CIA [b2]		NCRCG		
Citadel Security Software/IT ISAC				
Communications Industry	b6			om
[b2]				
[b4 b2]		Public Affairs		
		NCRCG		
[b2]		NCRCG		

Organization	Name	Role	Phone	E-mail
[b2]		NCRCG		
Department of Commerce		NCRCG		
Department of Commerce / [b2]	b6	[b2] Manager		
Department of Commerce / [b2]				
Department of Commerce / [b2]		Sr Staff Officer		
Department of Defense	DoD Other	Subject Matter Expert		
Department of Energy	DOE Other	Subject Matter Expert		b2 b6
Department of Energy	[b6]	NCRCG		
Department of Energy		NCRCG		
Department of Energy / [b2]	[b2] Hotline	[b2] Hotline	b2	
Department of Energy [b2]				
Department of Energy [b2]	b6			
Department of Energy [b2]				
Department of Energy [b2]	Network Security Team			
Department of Energy [b2]	[b6]			
Department of Energy [b2]	Watch Officer			

Organization	Name	Role	Phone	E-mail
Department of Energy Office of Energy Reliability				
Department of Health and Human Services		NCRCG		
Department of Health and Human Services		NCRCG		
Department of Homeland Security / Infrastructure Partnerships Division (IPD)				
Department of Homeland Security / Infrastructure Partnerships Division (IPD)		CWIN		b2
Department of Homeland Security / Infrastructure Partnerships Division (IPD)	b6	Hurricanes, NRCC, GIS POC		b6
Department of Homeland Security / International Civil Aviation Organization (ICAO)		Energy Sector Specialist	b2	
Department of Homeland Security / International Civil Aviation Organization (ICAO)		Aviation		
Department of Homeland Security / International Civil Aviation Organization (ICAO)		Financial		
Department of Homeland Security / International Civil Aviation Organization (ICAO)		IT, Telecom, NCRCG		

Organization	Name	Role	Phone	E-mail
Department of Homeland Security / International Civil Aviation Organization (ICAO)	[b6]	Transportation Sector Specialist		
Department of Homeland Security / National Communications System (NCS)	Manager NCC	MGR NCC		
Department of Homeland Security / National Communications System (NCS)	NCC Industry	NCC Industry		
Department of Homeland Security / National Communications System (NCS)	NCC Watch	NCC Watch		
Department of Homeland Security / National Infrastructure Coordinating Center (NICC)		Watch Supervisor		b2 b6 gov
Department of Homeland Security / National Infrastructure Coordinating Center (NICC)		NICC Watch	b2	v
Department of Homeland Security / Office of Intelligence & Analysis	b6	Portfolio Manager - Cyber Threat		
Department of Homeland Security / Office of Intelligence & Analysis		Public Affairs		
Department of Homeland Security / Office of Intelligence & Analysis		Cyber Analyst		

Organization	Name	Role	Phone	E-mail
Department of Homeland Security / Protected Critical Infrastructure Information (PCIIP)				
Department of Homeland Security/ICE		NCRCG		
Department of Homeland Security/ICE		NCRCG		
Department of Homeland Security/NCS		NCRCG		
Department of Homeland Security/NCS		NCRCG		
Department of Homeland Security/NCSD		NCRCG		b2 b6
Department of Homeland Security/NCSD		NCRCG		
Department of Homeland Security/NCSD	b6	NCRCG	b2	
Department of Homeland Security/NCSD/BAH		NCRCG		
Department of Homeland Security/NCSD/BAH		NCRCG		
Department of Homeland Security/NCSD/BAH		NCRCG		
Department of Homeland Security/NCSD/BAH		NCRCG		
Department of Homeland Security/NCSD/O&A		NCRCG		
Department of Homeland Security/NCSD/US-CERT		NCRCG		

Organization	Name	Role	Phone	E-mail
Department of Homeland Security/NSCD		NCRCG		
Department of Homeland Security/PA		NCRCG		
Department of Homeland Security/USCERT		NCRCG		
Department of Homeland Security-IP		NCRCG		
Department of Justice		NCRCG		
Department of Justice		Public Affairs		
Department of Justice/CCIPS		NCRCG		b2 b6
Department of Justice/CCIPS		NCRCG		
Department of Justice/CCIPS	b6	NCRCG	b2	
Department of State		Public Affairs		
Department of State		NCRCG		
Department of State		NCRCG		
Department of State		NCRCG		
Department of the Treasury		NCRCG		
Department of the Treasury		NCRCG		
Department of the Treasury		NCRCG		
Department of Transportation	[b2]			
Department of Transportation	DOT Other	Subject Matter Expert		

Organization	Name	Role	Phone	E-mail
Department of Transportation	[redacted]	NCRCG	[redacted]	[redacted]
Department of Transportation	b6	NCRCG		
Department of Transportation		NCRCG		
Department of Transportation	[redacted]	NCRCG		
Department of Transportation	[b2]			
Department of Transportation	[b6]	NCRCG		
Department of Transportation [b2]	[b2]	Help Desk and Developer		b2 b6
Department of Transportation [b2]	[b2]	IT Security Analyst	b2	
DOD/ OSD (NII)-IA	[redacted]	NCRCG		
DOD/JCS [b2]		NCRCG		
DOD/JTF-GNO		NCRCG		
DOD/JTF-GNO		NCRCG		
DOD/JTF-GNO	b6	NCRCG		
DOD/JTF-GNO		NCRCG		
DOD/OSD/NII		NCRCG		
DOD/OSD/NII	[redacted]	NCRCG	[redacted]	[redacted]

Organization	Name	Role	Phone	E-mail
DOD/OSD/NII	[b6]	NCRCG	[redacted]	[redacted]
[b4 b2]				
[b4 b2]	[b2]	[b4 b2]		
[b2]				
Electricity Sector Information Sharing Analysis Center (ESISAC)	[b6]			
Electricity Sector Information Sharing Analysis Center (ESISAC)	ESISAC Duty	Operations Center		
Electricity Sector Information Sharing Analysis Center (ESISAC)	[redacted]			b2 b6 b4
Electricity Sector Information Sharing Analysis Center (ESISAC)	b6		b2	
Electricity Sector Information Sharing Analysis Center (ESISAC)	[redacted]			
Federal Aviation Administration	[b2]			
Federal Aviation Administration	FAA Other	Subject Matter Expert		
Federal Aviation Administration	[b2]			
Federal Aviation Administration	[b6]	NCRCG	[redacted]	[redacted]

Organization	Name	Role	Phone	E-mail
Federal Aviation Administration	[b2]			
Federal Aviation Administration [b2]		NCRCG		
Federal Bureau of Investigation		Public Affairs		
Federal Bureau of Investigation		NCRCG		
Federal Bureau of Investigation (FBI)		NCRCG		
Federal Bureau of Investigation (FBI)		Field Offices		
Federal Bureau of Investigation (FBI)	b6	Player		b2 b6
Federal Deposit Insurance Corporation (FDIC)		Security Director		
Federal Deposit Insurance Corporation (FDIC)		Management Review	b2	
[b2]				
Federal Reserve Bank of NY				
Federal Reserve Bank of NY				
Federal Reserve Bank of NY	NY FRB Other	Subject Matter Expert		
Federal Reserve Bank of NY				
Federal Reserve Bank of NY	b6			

Organization	Name	Role	Phone	E-mail
FS-ISAC	FS-ISAC			
FS-ISAC	[b6]			
[b4 b2]				
[b2]	[b4 b2]			
Homeland Security Council		NCRCG		
[b4 b2]	b6			
[b2]		Acting Unit Chief		
	SIAO Watch Desk			
		NCRCG		b2 b6
[b2]				
Information Technology ISAC	b6			
Information Technology ISAC				
Information Technology ISAC	IT-ISAC Other	Subject Matter Expert	b2	
American Red Cross	ARC Other	Subject Matter Expert		
American Red Cross		Office of the Chief Information Security Officer		
American Red Cross	b6	Office of the Chief Information Security Officer		
American Red Cross		Manager [b2]		
American Red Cross		NetOps Manager		

Organization	Name	Role	Phone	E-mail
American Red Cross		System Admin		
American Red Cross	b6	System Admin		
[b4 b2]				
JTF-GNO	Command Duty Officer			
JTF-GNO	[b2]			
		Information Technology Lead Technical Analyst		
		[b2]		
	b6	Operator 1		b2
		[b2] Operator 2		b6
		[b2] Operations Center		b4
	[b2]	Subject Matter Expert	b2	
		[b2] Operations Center		
b2				
	b6	[b2]		
		[b2]		
		Public Affairs		
		[b2]		
		Public Affairs		
	[b2]	Subject Matter Expert		
	b6	Public Affairs		
		[b2]		

Organization	Name	Role	Phone	E-mail
	b6	TAC		
	b2	Subject Matter Expert		
	b6			
b2	b2	Subject Matter Expert		
	b6			
	b2	Subject Matter Expert		
	b6 y			b2 b6 b4
	b2	Subject Matter Expert	b2	
	b6			
b4 b2	b4 b2			
b2				
Michigan	b6	Public Affairs		
Michigan	Operations Center			
Michigan	b6	Public Affairs		
Montana	Operations Center			
Montana	b6	Public Affairs		
MS-ISAC	Operations Center			

Organization	Name	Role	Phone	E-mail
[b2]	[b6]	NCRCG		
[b2]	[b2] ther	Subject Matter Expert		
National Security Agency		NCRCG		
National Security Agency/NTOC		NCRCG		
National Security Council	b6	NCRCG		
NCRCG		NCRCG		
NCRCG		NCRCG		
[b2]/Comm ISAC	[b2] Watch			
New York	Operations Center			
New Zealand		All other roles		
New Zealand	Operations Center			
NORTHCOM	[b2]		b2	b2 b6
NORTHCOM	[b2]			
NSA NTOC		NCRCG		
NSA/NTOC/NCRCG				
NSC/[b2]		NCRCG		
NTIA	b6	Chief, Emergency Planning & Policy (COOP Director)		
NTIA		NCRCG		
OMB/[b2]		NCRCG		
[b2]	[b2]			

Organization	Name	Role	Phone	E-mail
		[b2] Coordinator 1		
		[b2] Coordinator 2		
		Information Technology		
	b6	Public Affairs / Media Contact		
		Security		
	Media Relations			
b2	Operations Shift Supervisor			b2 b6 b4
	[b2] Coordinator			
	b6			
	Operations Center		b2	
b4				
	b6			
		Operations		n
		Information Technology		

Organization	Name	Role	Phone	E-mail
		Operations		
	b6	Information Technology		
		Information Technology		
	k	Security		
		Operations		
b2		Operations		
	[b2]	Operations Center A		b2 b6
	[b2]	Operations Center B		
	n	System Operations-TO		
	b6		b2	
		System Operations-TO		
	Emergency Command Center			
		IT-Corporate		
		[b2]		
	b6	Security		
Transportation Security Administration		Public Affairs		
Transportation Security Administration	Transportation Security Intelligence Service (TSIS)			

Organization	Name	Role	Phone	E-mail
Transportation Security Administration	Transportation Security Operations Center (TSOC)			
Transportation Security Administration	TSA Other	Subject Matter Expert		
United Kingdom		All other roles		
United Kingdom [b2]	Analyst			
United Kingdom [b2]	Analyst			
[b2]				
United Kingdom [b2]	[b6]			b2 b6
United States Secret Service	[b6]	Public Affairs		
United States Secret Service		NCRCG	b2	
United States Secret Service		NCRCG		
United States Secret Service	b6			
United States Secret Service		NCRCG		
US-CERT		NCRCG		gov
US-CERT	Operations Center			
US-CERT	US-CERT Other	Subject Matter Expert		
[b2]	[b6]	NCRCG		
[b2]				

Organization	Name	Role	Phone	E-mail
[b2]	[b6]	[b2] Operations	[b2]	
[b2]		Cyber Security Program Manager		

Cyber Storm Participant Directory

By Sector

Note: This directory will be expanded, and an update version will be provided via electronic mail the morning of Monday, February 6, 2006.

Organization	Name	Role	Phone	E-mail
Energy Sector				
[b2]				
[b2]	b6			
[b2]				
Electricity Sector Information Sharing Analysis Center (ESISAC)				b2 b6
Electricity Sector Information Sharing Analysis Center (ESISAC)	ESISAC Duty	Operations Center	b2	
Electricity Sector Information Sharing Analysis Center (ESISAC)				
Electricity Sector Information Sharing Analysis Center (ESISAC)	b6			
Electricity Sector Information Sharing Analysis Center (ESISAC)				
[b2 b2]				
[b2]				

Organization	Name	Role	Phone	E-mail
		Information Technology Lead Technical Analyst		
	b6	[b2] Operator 1		
		[b2] Operator 2		
		[b2] Coordinator 1		
		[b2], Coordinator 2	b2	b2 b6
		Information Technology		
b2	b6	Public Affairs / Media Contact		
		Security		
	Media Relations			
	Operations Shift Supervisor			
	[b2] Coordinator			
	b6			
	Operations Center			
	b6			

Organization	Name	Role	Phone	E-mail
		Operations		
		Information Technology		
		Operations		
	b6	Information Technology		
		Information Technology		
b2		Security		b2
		Operations	b2	b6
		Operations		
	[b2]	Operations Center A		
		Operations Center B		
	b6	System Operations-TO		
		System Operations-TO		
	Emergency Command Center			
	b6	[b2]		
		Security		

Organization	Name	Role	Phone	E-mail
[b2]		[b2] Operations		b2
[b2]	b6	Cyber Security Program Manager	b2	b6
Federal Departments and Agencies				
CIA- [b2]		NCRCG		
CIA- [b2]		NCRCG		
[b2]		NCRCG		
		NCRCG		
		NCRCG		
Department of Commerce	b6	NCRCG		
Department of Commerce / [b2]		[b2] Program Manager		b2 b6
Department of Commerce / [b2]			b2	
Department of Commerce / [b2]	m	Sr Staff Officer		
Department of Defense	DoD Other	Subject Matter Expert		
Department of Energy		NCRCG		
Department of Energy	b6	NCRCG		
Department of Energy	DOE Other	Subject Matter Expert		
Department of Energy / [b2]	[b2] Hotline	[b2] Hotline		

Organization	Name	Role	Phone	E-mail
Department of Energy [b2]	[redacted]		[redacted]	[redacted]
Department of Energy [b2]	b6			
Department of Energy [b2]	[redacted]			
Department of Energy [b2]	Network Security Team			
Department of Energy [b2]	[b6]			
Department of Energy [b2]	Watch Officer			
Department of Energy Office of Energy Reliability	[redacted]			b2 b6
Department of Health and Human Services		NCRCG		
Department of Health and Human Services		NCRCG	b2	
Department of Homeland Security / Infrastructure Partnerships Division (IPD)	b6			
Department of Homeland Security / Infrastructure Partnerships Division (IPD)		CWIN		
Department of Homeland Security / Infrastructure Partnerships Division (IPD)		Hurricanes, NRCC, GIS POC		
Department of Homeland Security / International Civil Aviation Organization (ICAO)	[redacted]	Energy Sector Specialist	[redacted]	[redacted]

Organization	Name	Role	Phone	E-mail
Department of Homeland Security / International Civil Aviation Organization (ICAO)		Aviation		
Department of Homeland Security / International Civil Aviation Organization (ICAO)	b6	Financial		
Department of Homeland Security / International Civil Aviation Organization (ICAO)		IT, Telecom, NCRCG	b2	
Department of Homeland Security / International Civil Aviation Organization (ICAO)		Transportation Sector Specialist		b2 b6
Department of Homeland Security / National Communications System (NCS)	Manager NCC	MGR NCC		
Department of Homeland Security / National Communications System (NCS)	NCC Industry	NCC Industry		
Department of Homeland Security / National Communications System (NCS)	NCC Watch	NCC Watch		
Department of Homeland Security / National Infrastructure Coordinating Center (NICC)	b6	Watch Supervisor		

Organization	Name	Role	Phone	E-mail
Department of Homeland Security / National Infrastructure Coordinating Center (NICC)		NICC Watch		
Department of Homeland Security / Office of Intelligence & Analysis		Portfolio Manager - Cyber Threat		
Department of Homeland Security / Office of Intelligence & Analysis		Public Affairs		
Department of Homeland Security / Office of Intelligence & Analysis		Cyber Analyst		
Department of Homeland Security / Protected Critical Infrastructure Information (PCIIP)	b6		b2	b2 b6
Department of Homeland Security/ICE		NCRCG		
Department of Homeland Security/ICE		NCRCG		
Department of Homeland Security/NCS		NCRCG		
Department of Homeland Security/NCS		NCRCG		
Department of Homeland Security/NCSD		NCRCG		
Department of Homeland Security/NCSD		NCRCG		
Department of Homeland Security/NCSD		NCRCG		

Organization	Name	Role	Phone	E-mail
Department of Homeland Security/NCSD/BAH		NCRCG		
Department of Homeland Security/NCSD/BAH		NCRCG		
Department of Homeland Security/NCSD/BAH		NCRCG		
Department of Homeland Security/NCSD/BAH		NCRCG		
Department of Homeland Security/NCSD/O&A		NCRCG		
Department of Homeland Security/NCSD/US-CERT		NCRCG		
Department of Homeland Security/NSCD		NCRCG		
Department of Homeland Security/PA		NCRCG		
Department of Homeland Security/USCERT		NCRCG		
Department of Homeland Security-IP		NCRCG		
Department of Justice		NCRCG		
Department of Justice		Public Affairs		
Department of Justice/CCIPS		NCRCG		
Department of Justice/CCIPS		NCRCG		
Department of Justice/CCIPS		NCRCG		
Department of State		Public Affairs		

b6 b2 b2 b6

Organization	Name	Role	Phone	E-mail
Department of State		NCRCG		
Department of State		NCRCG		
Department of State		NCRCG		
Department of the Treasury	b6	NCRCG		
Department of the Treasury		NCRCG		
Department of the Treasury		NCRCG		
Department of Transportation	[b2]			b2 b6
Department of Transportation	DOT Other	Subject Matter Expert	b2	
Department of Transportation		NCRCG		
Department of Transportation	b6	NCRCG		
Department of Transportation		NCRCG		
Department of Transportation		NCRCG		
Department of Transportation	[b2]			
Department of Transportation	[b6]	NCRCG		
Department of Transportation	[b2]	Help Desk and Developer		
[b2]				

Organization	Name	Role	Phone	E-mail
Department of Transportation [b2]	[b2]	IT Security Analyst		
DOD/ OSD (NII)-IA	y	NCRCG		
DOD/JCS [b2]		NCRCG		
DOD/JTF-GNO		NCRCG		
DOD/JTF-GNO b2	b6	NCRCG		
DOD/JTF-GNO		NCRCG		
DOD/JTF-GNO		NCRCG		
DOD/OSD/NII		NCRCG		b2 b6
DOD/OSD/NII		NCRCG	b2	
Federal Aviation Administration	[b2]			
Federal Aviation Administration	FAA Other	Subject Matter Expert		
Federal Aviation Administration	[b2]			
Federal Aviation Administration	[b6]	NCRCG		
Federal Aviation Administration [b2]	[b2]			
Federal Aviation Administration	[b6]	NCRCG		

Organization	Name	Role	Phone	E-mail
Federal Bureau of Investigation	[redacted]	Public Affairs	[redacted]	[redacted]
Federal Bureau of Investigation		NCRCG		
Federal Bureau of Investigation (FBI)		NCRCG		
Federal Bureau of Investigation (FBI)		Field Offices		
Federal Bureau of Investigation (FBI)	b6	Player		
Federal Deposit Insurance Corporation (FDIC)		Security Director		b2 b6
Federal Deposit Insurance Corporation (FDIC)		Planning & Analysis		
Federal Deposit Insurance Corporation (FDIC)		Management Review		
[b2]			b2	
Federal Reserve Bank of NY				
Federal Reserve Bank of NY	[redacted]			
Federal Reserve Bank of NY	NY FRB Other	Subject Matter Expert		
Federal Reserve Bank of NY	[redacted]			
Federal Reserve Bank of NY	b6			
Homeland Security Council [b4 b2]	[redacted]	NCRCG	[redacted]	[redacted]

Organization	Name	Role	Phone	E-mail
[b2]	[b6] SIAO Watch Desk	Acting Unit Chief		
	[b6]	NCRCG		
American Red Cross	ARC Other	Subject Matter Expert		
American Red Cross		Office of the Chief Information Security Officer		
American Red Cross		Office of the Chief Information Security Officer		
American Red Cross	b6	Manager, FIS Network Engineering		b2 b6
American Red Cross		NetOps Manager		
American Red Cross		System Admin	b2	
American Red Cross		System Admin		
JTF-GNO	Command Duty Officer			
JTF-GNO	[b2]			
[b2]	[b6]	NCRCG		
[b2]	NCS Other	Subject Matter Expert		
National Security Agency		NCRCG		
National Security Agency/NTOC		NCRCG		
National Security Council	b6	NCRCG		
NCRCG	d	NCRCG	41	
NCRCG		NCRCG		
[b2] Comm ISAC	NCC Watch			

Organization	Name	Role	Phone	E-mail
NORTHCOM	[b2]			
NORTHCOM	[b2]			
NSA NTOC		NCRCG		
NSA/NTOC/NCRCG				
NSC [b2]		NCRCG		
NTIA	b6	Chief, Emergency Planning & Policy (COOP Director)		
NTIA		NCRCG		
OMB [b2]		NCRCG		b2 b6
Transportation Security Administration		Public Affairs		
Transportation Security Administration	Transportation Security Intelligence Service (TSIS)		b2	
Transportation Security Administration	Transportation Security Operations Center (TSOC)			
Transportation Security Administration	TSA Other	Subject Matter Expert		
United States Secret Service		Public Affairs		
United States Secret Service	b6	NCRCG		
United States Secret Service		NCRCG		
United States Secret Service				

Organization	Name	Role	Phone	E-mail
United States Secret Service	b6	NCRCG		b2
US-CERT		NCRCG		b6
US-CERT	Operations Center		b2	
US-CERT	US-CERT Other	Subject Matter Expert		
[b2]	[b6]	NCRCG		
International				
Australia	Operations Center			
Australia		All other roles		
Canada		All other roles		
New Zealand	Operations Center			
New Zealand		All other roles	b2	b2
United Kingdom		All other roles		b6
United Kingdom [b2]	Analyst			
United Kingdom [b2]	Analyst b2			
[b2]				
United Kingdom [b2]	[b6]			
Information Technology & Communications				
[b2]	[b2]			
Citadel Security Software/IT ISAC	[b6]			b2
Communications Industry			b2	b6 com
[b2]				b4
[b4 b2]	[b6]	Public Affairs		

Organization	Name	Role	Phone	E-mail
Information Technology ISAC	b6			
Information Technology ISAC				
Information Technology ISAC	IT-ISAC Other	Subject Matter Expert		
[b4][b2]	b6	[b2] Operations Center		
	[b2]	Subject Matter Expert		
		[b2] Operations Center		b2 b6 b4
	b6	[b2]	b2	
b2		Public Affairs [b2]		
		Public Affairs		
	[b2]	Subject Matter Expert		
	b6	Public Affairs [b2] TAC		
	[b2]	Subject Matter Expert		
	b6			

Organization	Name	Role	Phone	E-mail
[redacted]	[redacted]	Subject Matter Expert	[redacted]	[redacted]
	[redacted]	Subject Matter Expert		
b2	b6		b2	b2 b6 b4
[redacted]	[redacted]	Subject Matter Expert		
b2 b4	b6		[redacted]	[redacted]
Other Private Sector				
[redacted]	[redacted]		[redacted]	[redacted]
FS-ISAC	[redacted]		b2	b2 b6 b4
FS-ISAC	FS-ISAC			
[redacted]	[redacted]		[redacted]	[redacted]
[redacted]	[redacted]			
State & Local				
Michigan	[redacted]	Public Affairs	[redacted]	[redacted]
Michigan	Operations Center		b2	

Organization	Name	Role	Phone	E-mail
Michigan	[b6]	Public Affairs	[redacted]	[redacted]
Montana	Operations Center			
Montana	[b6]	Public Affairs	b2	b2 b6
MS-ISAC	Operations Center			
New York	Operations Center			
[b2]	[b2]		[redacted]	[redacted]
Transportation				
[b2]	[b2]		[redacted]	[redacted]
[b4 b2]	[b2]	[b4 b2]	b2	b2 b6 b4
[b4 b2]				
[b2]				
[b2]			[redacted]	[redacted]

Cyber Storm Participant Directory

By Participant

Note: This directory will be expanded, and an update version will be provided via electronic mail the morning of Monday, February 6, 2006.

Organization	Name	Role	Phone	E-mail
Australia		All other roles		
Canada		All other roles		
[b2]				
Communications ISAC				
[b4 b2]				
[b2]				
[b2]			b2	b2 b6 b4
[b2 b4]				
[b2]				
New Zealand		All other roles		
b2		[b2] Coordinator 1		
		[b2] Coordinator 2		
		Information Technology		
		Operations		
		Information Technology		

Organization	Name	Role	Phone	E-mail
[b2]				
United Kingdom		All other roles		
[b2]				
[b2]	[b2]			
[b2]		System Operations-TO		
Information Technology ISAC	b6			
[b4b2]				
Department of Homeland Security / Infrastructure Partnerships Division (IPD)			b2	b2 b6 b4
United Kingdom [b2]	Analyst			
United Kingdom [b2]	Analyst			
[b2]				
American Red Cross	ARC Other	Subject Matter Expert		
Department of Justice/CCIPS	[b6]	NCRCG		
[b2]	[b2]			
National Security Council		NCRCG		
Citadel Security Software/IT ISAC				
American Red Cross	b6	Office of the Chief Information Security Officer		
DOD/JTF-GNO [b2]		NCRCG		

Organization	Name	Role	Phone	E-mail
American Red Cross		Office of the Chief Information Security Officer		
NTIA		Chief, Emergency Planning & Policy (COOP Director)		
Department of Energy [b2]				
Federal Reserve Bank of NY				
Department of Homeland Security/ICE		NCRCG		
Federal Deposit Insurance Corporation (FDIC)		Security Director		b2 b6
Federal Reserve Bank of NY [b2]	b6		b2	
Department of Homeland Security / International Civil Aviation Organization (ICAO)		Energy Sector Specialist		
[b2]	el	NCRCG		
[b2]		PSIRT		
[b2]	[b2]			
Federal Bureau of Investigation (FBI)		NCRCG		
United States Secret Service	b6	Public Affairs		

Organization	Name	Role	Phone	E-mail
Department of Energy / [b2]	[b2] Hotline	[b2] Hotline		
Information Technology ISAC [b4 b2]	b6			
NTIA		NCRCG		
Transportation Security Administration		Public Affairs		
JTF-GNO	Command Duty Officer			
Electricity Sector Information Sharing Analysis Center (ESISAC)	[b6]			b2 b6 b4
Department of Transportation	[b2]			
Federal Bureau of Investigation (FBI)	[b6]	Field Offices		
Federal Aviation Administration	[b2]		b2	
United States Secret Service	[b6]	NCRCG		
[b2]	[b6]	NCRCG		
[b2]	[b2]			
Department of Commerce / [b2]	[b6]	Acting DPAS Program Manager		
[b4 b2]	[b2]	[b4 b2]		
[b2]	[b6]	System Operations-TO		

Organization	Name	Role	Phone	E-mail
Department of Homeland Security/NCSD/US-CERT	[b6]	NCRCG		
Department of Defense	DoD Other	Subject Matter Expert		
Department of Energy	DOE Other	Subject Matter Expert		
[b2]	[b6]	Information Technology Lead Technical Analyst		
CIA [b2]	[b6]	NCRCG		
Department of Transportation	DOT Other	Subject Matter Expert		
[b2]	[b6]	Public Affairs / Media Contact		b2 b6
Department of Justice/CCIPS	[b6]	NCRCG		
[b2]	Emergency Command Center		b2	
Department of Homeland Security / International Civil Aviation Organization (ICAO)	[b6]	Aviation		
Department of Energy [b2]	[b6]			
Electricity Sector Information Sharing Analysis Center (ESISAC)	ESISAC Duty	Operations Center		
[b2]	[b6]			
Federal Aviation Administration	FAA Other	Subject Matter Expert		
[b2]	[b6]	IT-Corporate		

Organization	Name	Role	Phone	E-mail
National Security Agency/NTOC		NCRCG		
Department of Energy Headquarters	b6			
Department of Homeland Security/NCSD/O&A		NCRCG		
[b2]		[b2]		
FS-ISAC	FS-ISAC			
[b2]	[b2 b4]			
[b2]				
Department of Agriculture		NCRCG		
Federal Aviation Administration [b2]	b6	NCRCG		b2
Michigan		Public Affairs		b6
[b2]	[b2]		b2	b4
[b2]		Public Affairs		
CIA [b2]		NCRCG		
[b2]		IT-Business		
Federal Deposit Insurance Corporation (FDIC)	b6	Management Review		
[b2]		[b2]		
[b2]		Operations		
Department of Energy Office of Energy Reliability				
[b2]				

Organization	Name	Role	Phone	E-mail
Department of Health and Human Services		NCRCG		
DOD/OSD/NII		NCRCG		
NSA/NTOC [b2]				
NSA NTOC		NCRCG		
Department of State		Public Affairs		
Department of Homeland Security / Office of Intelligence & Analysis		Portfolio Manager - Cyber Threat		
[b2]		Security		
US-CERT	b6	NCRCG		b2 jov
[b2]				b6
Department of Homeland Security / Protected Critical Infrastructure Information (PCIIP)			b2	
NSC [b2]		NCRCG		
[b2]				
United States Secret Service		NCRCG		
Department of Commerce		NCRCG		
Information Technology ISAC	IT-ISAC Other	Subject Matter Expert		
Department of Transportation		NCRCG		
DOD/OSD/NII	b6	NCRCG		

Organization	Name	Role	Phone	E-mail
Department of Commerce / [b2]				
OMB [b2]		NCRCG		
Electricity Sector Information Sharing Analysis Center (ESISAC)				
Department of Energy		NCRCG		
Department of Homeland Security/NCSD/BAH		NCRCG		
DOD/JTF-GNO [b2]		NCRCG		
Electricity Sector Information Sharing Analysis Center (ESISAC) [b2]	b6	Public Affairs	b2	b2 b6
NCRCG [b2]		NCRCG Information Technology		
Department of Health and Human Services		NCRCG		
Department of Homeland Security/NCSD		NCRCG		
NCRCG [b2]		NCRCG [b2] Operations Center		

Organization	Name	Role	Phone	E-mail
United States Secret Service				
American Red Cross		Manager [b2]		
Department of Justice		NCRCG		
[b2]	b6	Information Technology		
[b2]				
Department of Homeland Security / International Civil Aviation Organization (ICAO)		Financial		b2 b6
Department of Homeland Security / National Communications System (NCS)	Manager NCC	MGR NCC	b2	
DOD/ OSD (NII)-IA		NCRCG		
Department of State		NCRCG		
[b4 b2]		Public Affairs		
Department of Homeland Security/NCSD	b6	NCRCG		
DOD/JTF-GNO		NCRCG		
Department of Transportation		NCRCG		
American Red Cross		NetOps Manager		
[b2]		Security		
Department of Homeland Security/NCSD [b2]		NCRCG		

Organization	Name	Role	Phone	E-mail
Department of Homeland Security-IP		NCRCG		
[b2]	b6			
Department of Commerce /		Sr Staff Officer		
[b2]				
[b2]	[b2]	Subject Matter Expert		
[b4 b2]	[b4 b2]			
[b2]	b6			
[b2]		Acting Unit Chief		
[b2]	[b2]	Subject Matter Expert	b2	b2 b6
Federal Bureau of Investigation		Public Affairs		
American Red Cross		System Admin		
[b2]	b6			
[b2]				
Department of Transportation		NCRCG		
		Subject Matter Expert		
[b2]	[b2]	Subject Matter Expert		
		Subject Matter Expert		
		Subject Matter Expert		

Organization	Name	Role	Phone	E-mail
Department of Transportation [b2]	[b2]	Help Desk and Developer		
Department of Homeland Security / National Communications System (NCS)	NCC Industry	NCC Industry		
Department of Homeland Security / National Communications System (NCS)	NCC Watch	NCC Watch		
[b2] Comm ISAC	[b2] Watch			
[b2]	NCS Other	Subject Matter Expert		
JTF-GNO	[b2]			
Department of Energy Headquarters	Network Security Team		b2	
National Security Agency		NCRCG		b2 b6
Electricity Sector Information Sharing Analysis Center (ESISAC) [b2]	b6	Public Affairs		
Department of the Treasury		NCRCG		
Federal Reserve Bank of NY	NY FRB Other	Subject Matter Expert		
Department of Homeland Security/NCSD/BAH	b6	NCRCG		
Department of Homeland Security/NCS		NCRCG		

Organization	Name	Role	Phone	E-mail
Federal Aviation Administration	[b2]			
Department of Homeland Security/ICE	[b6]	NCRCG		
Australia	Operations Center			
Michigan	Operations Center			
Montana	Operations Center			
MS-ISAC	Operations Center			
New York	Operations Center			
New Zealand	Operations Center			
[b2]	Operations Center			b2 b6
US-CERT	Operations Center		b2	
[b2]	Operations Shift Supervisor			
[b2]		[b2] Operations Center		
Department of Justice/CCIPS		NCRCG		
[b2]		[b2]		
United Kingdom [b2]	b6			
[b2]		NCRCG		
[b2]		TAC		
Department of Energy Headquarters				

Organization	Name	Role	Phone	E-mail
Department of the Treasury [b2]	b6	NCRCG		
Department of Homeland Security / National Infrastructure Coordinating Center (NICC)		Watch Supervisor		gov
Department of Transportation [b2]	[b2]	IT Security Analyst		b2
Department of Homeland Security / Infrastructure Partnerships Division (IPD) [b2]		CWIN	b2	b6
Federal Reserve Bank of NY				
Department of Homeland Security/NCSD [b2]	b6	NCRCG		
Department of Homeland Security/NCSD		NCRCG		
Department of Homeland Security / Infrastructure Partnerships Division (IPD) [b2]	[b2] Coordinator	Hurricanes, NRCC, GIS POC Operations		om
Department of Homeland Security / National Infrastructure Coordinating Center (NICC)	[b6]	NICC Watch		ov

Organization	Name	Role	Phone	E-mail
Department of State	[redacted]	NCRCG	[redacted]	
Federal Aviation Administration		NCRCG		
American Red Cross		System Admin		
Federal Reserve Bank of NY				
Department of Agriculture	b6	NCRCG		
Department of the Treasury		NCRCG		
Department of State		NCRCG		
[b2]				
Homeland Security Council		NCRCG		b2
Department of Homeland Security/PA	[redacted]	NCRCG		b6
[b2]	[b2] Watch Desk		b2	
[b4 b2]	[redacted]			
United States Secret Service		NCRCG		
Department of Homeland Security/NSCD		NCRCG		
DOD/JTF-GNO [b2]		NCRCG		
Department of Homeland Security / Office of Intelligence & Analysis	b6	Public Affairs		
[b2]		Security	[redacted]	
Federal Bureau of Investigation (FBI)	[redacted]	Player		[redacted]

Organization	Name	Role	Phone	E-mail
[b2]	[redacted]	NCRCG	[redacted]	[redacted]
Department of Justice		Public Affairs		
DOD/JCS [b2]	b6	NCRCG		
[b2]		[b2] Operations		
NORTHCOM	[b2]			
NORTHCOM	[b2]			
Federal Bureau of Investigation	[redacted] b6	NCRCG		
Department of Transportation		NCRCG	b2	b2 b6
[b2]	[b2]	Operations Center A Operations Center B		
Department of Transportation	Transportation Cyber Incident Response Center (TCIRC)			
Transportation Security Administration	Transportation Security Intelligence Service (TSIS)			
Transportation Security Administration	Transportation Security Operations Center (TSOC)			
Transportation Security Administration	TSA Other	Subject Matter Expert		
US-CERT	US-CERT Other	Subject Matter Expert		
Department of Transportation	[b6]	NCRCG	[redacted]	[redacted]

IIL

Organization	Name	Role	Phone	E-mail
[b2]	b2	[b2] Operator 1		
[b2]		[b2] Operator 2		
Federal Aviation Administration	[b2]			
Department of Energy [b2]	Watch Officer			
Department of Homeland Security / International Civil Aviation Organization (ICAO)		IT, Telecom, NCRCG		
[b2]				b2 b6
Department of Homeland Security / International Civil Aviation Organization (ICAO)		Transportation Sector Specialist	b2	
[b2]		Cyber Security Program Manager		
Michigan	b6	Public Affairs		
Department of Homeland Security/NCS		NCRCG		
[b2]		Operations		.com
Montana		Public Affairs		
[b2]				
FS-ISAC				
Department of Homeland Security/USCERT		NCRCG		

Organization	Name	Role	Phone	E-mail
Department of Homeland Security / Office of Intelligence & Analysis [b2]	b6	Cyber Analyst	b2	b2 b6
Department of Energy		NCRCG		
DOD/OSD/NII		NCRCG		