
Homeland Security

# CYBER STORM

## Exercise Report

***September 12, 2006***

**Department of Homeland Security**
**National Cyber Security Division**

This page intentionally left blank.

# Contents

# EXECUTIVE SUMMARY

The National Cyber Exercise (NCE) Cyber Storm was executed successfully on February 6–10, 2006. The United States (U.S.) Department of Homeland Security (DHS)/National Cyber Security Division (NCSD) was responsible for developing, implementing, and coordinating all aspects of Cyber Storm. The first Government-led, full-scale, cyber security exercise of its kind, Cyber Storm was a coordinated effort between international, Federal and State governments, and private sector organizations to exercise their response, coordination, and recovery mechanisms in reaction to simulated cyber events.

Cyber Storm provided participants with a controlled environment in which to exercise a coordinated cyber incident response, including information sharing mechanisms, procedures for establishing situational awareness, public and private organizational decision making, and public communications during a cyber-related Incident of National Significance.

Over 100 public and private agencies, associations, and corporations participated in the exercise from over 60 locations and 5 countries. They collaborated in crisis response at operational, policy and public affairs levels in this federally funded and congressionally mandated emergency response exercise. The exercise included participation of more than 30 private sector corporations and associations in its planning, execution, and after action analysis.

The exercise scenario simulated a large-scale cyber campaign affecting or disrupting multiple critical infrastructure elements primarily within the Energy, Information Technology, Transportation, and Telecommunications Sectors. The exercise was conducted primarily on a separate exercise network without impacting real world information systems. This report provides details of the scenario, timeline, and lessons learned from exercise play.

The findings from the exercise showed many areas where intra-sector, cross-sector and public/private partnerships worked effectively to communicate and resolve issues but also highlighted areas where communications and planning could be improved. Future focus on correlation of multiple incidents; and communication, coordination, and collaboration across the cyber incident response community were emphasized by both public and private stakeholders.

### *Significant Findings*

Eight major findings were revealed as a result of exercise execution. These findings impact all participating sectors and agencies.

- **Finding 1: Interagency Coordination.** While the Interagency Incident Management Group (IIMG)[1] and National Cyber Response Coordination Group (NCRCG) activated and interacted constructively during the exercise, further refinement is needed for operations and coordination procedures. Broader understanding, both within government and in the private sector, of the thresholds and ramifications of activation of these bodies will also improve interagency coordination. Specifically the cyber community needs to better understand the readiness and security postures to be considered based on such activations, as well as the level of Federal engagement they imply.

[1] *Note: As outlined in the Notice of Change to the National Response Plan, dated May 25, 2006, the IIMG underwent a reorganization and has been renamed the Interagency Advisory Council (IAC). In an effort to maintain consistency within Cyber Storm documentation, reference to the organization will continue to be listed as IIMG since this was the organizational construct during the exercise, the functions still exist and related findings remain valid.*

- **Finding 2: Contingency Planning, Risk Assessment, and Roles and Responsibilities.** Formal contingency planning, risk assessment, and definition of roles and responsibilities across the entire cyber incident response community must continue to be solidified. Responses were timely and well coordinated where existing process procedures were clear and fully understood by players.
- **Finding 3: Correlation of Multiple Incidents between Public and Private Sectors.** Correlation of multiple incidents across multiple infrastructures and between the public and private sectors remains a major challenge. The cyber incident response community was generally effective in addressing single threats/attacks, and to some extent multiple threats/attack. However, most incidents were treated as individual and discrete events. Players were challenged when attempting to develop an integrated situational awareness picture and cohesive impact assessment across sectors and attack vectors.
- **Finding 4: Training and Exercise Program.** An established training and exercise program will strengthen awareness of organizational cyber incident response, roles, policies, and procedures.
- **Finding 5: Coordination Between Entities of Cyber Incidents**. Response coordination became more challenging as the number of cyber events increased, highlighting the importance of cooperation and communication across the community.
- **Finding 6: Common Framework for Response and Information Access.** A synchronized, continuous flow of information available to cyber incident stakeholders created a common framework for response, impact development, and discussions. Early and ongoing information access strengthened the information-sharing relationship between domestic and international cyber response communities.
- **Finding 7: Strategic Communications and Public Relations Plan**. Public messaging must be an integral part of a collaborated contingency plan and incident response to provide critical information to the response community and empower the public to take appropriate individual protective or response actions consistent with the situation.
- **Finding 8: Improvement of Processes, Tools and Technology.** Improved processes, tools, and training—focused on the analysis and prioritization of physical, economic, and national security impacts of cyber attack scenarios—would enhance the quality, speed, and coordination of response. This is particularly true in the case of integrated or cascading attacks or consequences.

***Next Steps***

The DHS/NCSD is moving rapidly to turn the lessons learned from Cyber Storm into solutions. These include, but are not limited to, procedures, policy and practice development, and organizational changes. Other exercise participants are also taking measures, such as developing institutional concept of operations to address findings related to their organization and sector.

The cyber community must continue to improve its ability to effectively respond to and recover from even the most sophisticated of cyber attacks. In doing so, the community must consider formalizing many of these practices into standard of operations (SOPs) and contingency plans, clarifying the roles and responsibilities of players and organizations, and providing further training and exercises. The interdependencies, gaps in response structure, and positive cross-sector collaboration among infrastructure sectors—Federal and State, international and domestic, public and private— are all critical parts of Cyber Storm lessons learned and will have enduring impact throughout the cyber community.

# INTRODUCTION

The U.S. Department of Homeland Security (DHS)/National Cyber Security Division (NCSD) successfully executed the National Cyber Exercise (NCE), Cyber Storm, February 6 –10, 2006. The exercise was the first government-led, full-scale cyber security exercise of its kind. NCSD, a division within DHS's Preparedness Directorate, provides the Federal Government with a centralized cyber security coordination and preparedness function as called for in the National Strategy for Homeland Security, *the National Strategy to Secure Cyberspace*, and Homeland Security Presidential Directive 7. NCSD is a focal point for the Federal Government's interaction with state and local government, the private sector, and the international community concerning cyberspace vulnerability reduction efforts.

In accordance with authorities and responsibilities in the DHS National Response Plan (NRP)[2] Cyber Annex, the exercise was conducted to examine preparedness, response, coordination, and recovery mechanisms to a simulated cyber event within international, Federal, and State Governments in conjunction with the private sector. During the exercise, NCSD and participating organizations (see Appendix A) observed exercise activities and compared anticipated player actions with their actual responses in order to identify strengths and suggested areas for improvement within the cyber incident response community.

Over 100 public, private, and international agencies, organizations, and companies were involved in the planning and implementation of Cyber Storm. Players and observer/controllers[3] included participants from the public sector (Federal and State agencies), the private sector (information technology [IT], telecommunications, energy, transportation, and financial services firms selected in consultation with their respective Industry Information Sharing and Analysis Centers [ISACs], and Sector Specific Agencies [SSA]), and select international government partners.

## Purpose and Objectives

Cyber Storm was designed to exercise communication, incident response policies, and operational procedures in response to various cyber incidents, and to identify future planning and process improvements. The exercise challenged players to identify policies and procedures required for sharing information with groups internal and external to their organizations, such as across Federal and State departments, private organizations, and across international borders. This required players to determine what information should be shared with which organization and at what time. The exercise also highlighted the collaboration capabilities among international and government communities and their respective capacity to maximize communications and enhance response and recovery efforts.

One fundamental objective of the exercise was for key interagency organizations within the Federal response infrastructure to exercise their roles and responsibilities under the NRP in

---

[2] *NRP refers to the Department of Homeland Security's plan to coordinate domestic response efforts to terrorist activities, natural disasters, or other large-scale emergencies.*

[3] *Observer – Individuals who observe and make note of player actions; Controller – Individuals who manage an exercise and influence player actions by injecting preplanned events to stimulate play and to keep the exercise from going off track.*

response to multiple incidents. These organizations include the National Cyber Response Coordination Group (NCRCG) and the Interagency Incident Management Group (IIMG)[4], both comprised of senior representatives from Federal departments/agencies. The successful activation of both the NCRCG and IIMG was a result of significant alert warnings by the U.S. Computer Emergency Readiness Team (US-CERT) and the Homeland Security Operations Center (HSOC). Further, information was collected and disseminated to players within the respective Information Sharing and Analysis Centers (ISACs) for the transportation, energy, IT, and telecommunications sectors for cyber response efforts.

The objectives of the exercise as articulated in the Cyber Storm concept of operations were to stimulate participants to:

- Exercise interagency coordination (e.g., standard operating procedures, communications and decision support mechanisms) through the activation of the NCRCG and the IIMG
- Exercise inter-governmental (international) and intra-governmental (Federal-State) coordination and incident response
- Identify policies/issues that hinder or support cyber security requirements
- Identify public/private interface communications and thresholds of coordination to improve cyber incident response and recovery, as well as identify critical information sharing paths and mechanisms
- Identify, improve, and promote public and private sector interaction in processes and procedures for communicating appropriate information to key stakeholders and the public
- Identify cyber physical interdependence of infrastructure of real world economic and political impact
- Raise awareness of the economic and national security impacts associated with a significant cyber incident
- Highlight available tools and technology with analytical cyber incident response and recovery capability

## Scope

The Cyber Storm scenario[5] simulated a large-scale cyber campaign affecting and disrupting multiple critical infrastructure elements, primarily within the energy, IT, and transportation sectors, and secondarily within telecommunications. Limiting the scenario to the three primary sectors helped improve the capability of each player to respond while allowing observer/controllers to provide more adequate coverage for each of the key cyber elements requiring analysis and evaluation.

---

[4] *Note: As outlined in the Notice of Change to the National Response Plan, dated May 25, 2006, the IIMG underwent a reorganization and has been renamed the Interagency Advisory Council (IAC). In an effort to maintain consistency within Cyber Storm documentation, reference to the organization will continue to be listed as IIMG since this was the organizational construct during the exercise, the functions still exist and related findings remain valid.*

[5] *Scenario – A sequential, narrative account of a hypothetical incident or accident. The scenario provides the catalyst for the exercise and is intended to introduce situations that will stimulate player response(s).*

The adversary(ies) staged primary cyber attacks and, in certain circumstances, included complementary physical demonstrations and disturbances targeting the energy, transportation, and IT/telecommunications sectors. These attacks were intended to disrupt certain elements of critical infrastructure, potentially leading to cascading effects within other facets of the U.S. and other participating countries' national economic, societal, and governmental structures. Cyber attacks were 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 infrastructure attacks, and, subsequently, undermine public confidence in the government(s).

Consequence management of physical infrastructure disruption as a result of the cyber attacks was generally outside the scope of the exercise. The exercise construct did, however, provide players with information on physical impacts that encouraged the consideration of interdependencies in their cyber response procedures, including triage and resource prioritization.

## Key Achievements

The Cyber Storm exercise was an important milestone both in national and international cyber incident response, as well as in the public and private partnership's interest in protecting both physical and cyber-related critical infrastructures. The exercise achieved the stated training objectives for participants and stakeholders. The following list highlights key achievements of the exercise:

- Executed the largest, most complex multinational, cross-sector, cyber exercise to date
- Organized and simultaneously exercised the cyber response organizations of over 100 public and private agencies, associations, and corporations in over 60 locations and five countries
- Achieved multinational collaboration in crisis response at operational, policy, and public affairs levels
- Extensive direct participation by over 30 private sector corporations and associations in the planning, execution, and after action analysis of a federally funded and congressionally mandated emergency response and recovery exercise
- Achieved unprecedented cooperation and information sharing across Federal agencies including intelligence, law enforcement, military, and civilian interests; across boundaries among the private sector and government and between international partners
- Tested, for the first time, the full range of cyber-related response policy, doctrine, and communications methodologies that would be required in a real world crisis
- Tested policies and procedures associated with a cyber-related Incident of National Significance, as outlined within the National Response Plan's Cyber Incident Annex
- Through its planning and execution, established numerous public and private relationships that will be invaluable in future preparation for and response to cross-sector cyber incidents
- Identified recovery issues that warrant additional review through collaboration between the public and private sectors.

## SUMMARY OF MAJOR FINDINGS

Cyber Storm yielded eight major findings with significant impact across all sectors and agencies and for all players. Exercise players and observers/controllers provided input and feedback, creating the aforementioned findings. Input was captured through direct observations during the exercise, as well as through player responses to post-exercise conferences.

### *Finding 1: Interagency Coordination*

*While the IIMG and NCRCG activated and interacted constructively during the exercise, further refinement is needed for NCRCG operations as well as IIMG-NCRCG coordination procedures. Broader understanding, and clarity both within government and in the private sector, of the thresholds and ramifications of activation of these bodies will also improve interagency coordination before, during, and after crisis situations. It is also important that the cyber community recognize and understand the appropriate postures of readiness and security that should be considered based on such activations, as well as the anticipated level of Federal engagement during major incidents.*

Observations:

One of the primary objectives of the Federal/Interagency sector was to exercise interagency coordination through the stand-up (activation) of the NCRCG and the IIMG during a Cyber Incident of National Significance. Observations and discussions within the NCRCG and the IIMG during exercise play indicated:

- The NCRCG and IIMG coordinated closely during the exercise to develop a refined situational awareness picture, assess impacts on the Nation's critical infrastructure, and define the threats to national security and economic interests. As a result, the Homeland Security Advisory System threat level was elevated based on these and other factors. Even in light of this relative success, additional work is needed to determine how to most effectively elevate the alert levels in response to cyber attacks or threats.
- There was exemplary information sharing between some parts of the government, in particular, sector-specific agencies and private sector infrastructure owners/operators. However, greater public-private sector collaboration could be achieved if the private sector was afforded robust connectivity to, or interaction with, the NCRCG during major incidents such as the scenario presented by Cyber Storm. Greater information sharing would leverage capacity both inside and outside of government, and provide a more cohesive decision-making process critical to national and homeland security operations.
- Bi-directional flow of information is critical to cyber response activity. During Cyber Storm, the US-CERT served as a clearinghouse for response information for DHS and the NCRCG between internal and external organizations. This key operational role, which was critical to DHS's and the NCRCG's ability to gain situational awareness, required a significant surge capability during the high point of the attacks.
- At the strategic level, the NCRCG did not have sufficient technical experts on staff to fully leverage the large volume of incident information that was being provided. As a result, development of an accurate situational picture was challenging, albeit in part due to the difficulty of the scenario. Consequently, US-CERT was called upon to fill this role

on an ad hoc basis. While they performed well in support of the NCRCG, it had a detrimental impact on their ability to surge in their role as the operational information clearinghouse.

- It was noted that one of the important roles of the NCRCG and the IIMG during an event similar to the Cyber Storm exercise is to establish a clear public communications channel in the face of a significant disaster or sequence of events, regardless of origin. Communications procedures are needed to deliver key technical messages at a layman's level to organizations' public affairs groups in a timely manner and establish a confident and accurate media presence. More damage could have occurred as a result of erroneous and panicked public responses to incorrect media coverage than by actual attacks by the adversary. The current NCRCG composition and staffing was significantly challenged by the adversary's robust media campaign that accompanied the cyber attacks, and may warrant re-examination for possible adjustments.
- While not specifically exercised during Cyber Storm, the international players observed a need to pre-identify their counterpart response organizations to the IIMG and NCRCG amongst closely allied countries. An established information-sharing process between the NCRCG and its allied nations would also facilitate communication and help ensure a more effective response. This would also provide a means of communication and collaboration across the spectrum of technical, operational, strategic and political issues, thus allowing for more integrated decision making on critical cyber security response and consequence evaluation.

***Finding 2: Contingency Planning, Risk Assessment, and Roles and Responsibilities***

*Formal contingency planning, risk assessment, and definition of roles and responsibilities across the entire cyber incident response community must continue to be solidified. Responses were timely and well coordinated where existing process procedures were clear and fully understood by players.*

Observations:

- Observers noted that players had difficulty ascertaining what organizations and whom within those organizations to contact when there was no previously established relationship or pre-determined plans for response coordination and risk assessments/mitigation. There was a general recognition of the difficulties organizations faced when attempting to establish trust with unfamiliar organizations during time of crisis.
- Contingency planning for backup or resilient communications methods is a critical need. While only tested for a few players during the exercise, many players noted a high reliance of cyber incident response activities on communication systems that can be, themselves, vulnerable to attack or failure.

***Finding 3: Correlation of Multiple Incidents between Public and Private Sectors***

*Correlation of multiple incidents across multiple infrastructures and between the public and private sectors remains a major challenge. The cyber incident response community was generally effective in addressing single threats/attacks, and to some extent multiple*

*threats/attack. However, most incidents were treated as individual and discrete events. In the coordinated cyber attack as presented by the exercise, players were challenged when attempting to develop an integrated situational awareness picture and cohesive impact assessment across sectors and attack vectors.*

Observations:

- Cyber Storm highlighted the need to establish a method of rapid assessment and prioritization or "triage" capability when dealing with cyber incidents. Establishing a prioritization scheme should be addressed quickly. While there is no such thing as perfect information, we also need to prioritize information sources and determine their applicability. For example, during the exercise, US-CERT found that the sheer volume of information constrained their ability to simultaneously provide situational awareness coordination and conduct second order technical analysis.
- US-CERT roles, responsibilities, and Standard Operating Procedures (SOP) required greater clarification as to which public and private agencies they should connect to and for what reasons, what type of services they should perform, and what their role is as point of contact for cyber security incidents with the private sector and among the civilian Departments and Agencies of the Federal Government. US-CERT was inundated throughout the exercise with emails and information.

***Finding 4: Exercise Program***

*Recurring exercises will strengthen awareness of organizational cyber incident response, roles, policies, and procedures.*

Observations:

- Conducting ongoing training activities, discussions, and exercises is needed to build relationships among organizations and strengthen coordinated responses to cyber incidents.
- Developing situational awareness in a timely manner that anticipates consequences and disruptions in a rapidly changing cyber environment proved challenging for participants. Valid, trustworthy, and timely information is critical to the selection of response options during cyber attacks, and would benefit greatly from regular exercises.
- Several of the participants recommended training through the execution of smaller routine exercises. These exercises would train knowledgeable, "tech-smart" personnel and could be distributed through various agencies to provide the intellectual capital required in detecting cyber attacks, as well as cross-functional knowledge to increase situational awareness.

***Finding 5: Coordination between Entities of Cyber Incidents***

*Coordinating the response activities became more challenging as the number of cyber events increased, indicating the importance of community cooperation and communication during simultaneous cyber incidents.*

Observations:

- Cyber Storm exercised both the capability and the capacity components of organizations' cyber response activities. Exercise participants noted the overwhelming effects that multiple, simultaneous, and coordinated incidents had on their response activities. It proved important to accurately fuse information to identify the appropriate response to simultaneous attacks. Prioritization of response activities was also crucial during coordinated attack activity, particularly for organizations with multiple effects or responsibilities, prioritization is critical.

- Clarifying roles and responsibilities across government, and clearly articulating expectations between public and private sectors will enable the advancement of processes and communications architecture to support the development and maintenance of situational awareness across sectors. When the roles and responsibilities are defined and understood then the means to coordinate preventive measures and responses to remediate disruptions can be better established, keeping in mind that both lateral coordination and hierarchical response will occur simultaneously.

***Finding 6: Common Framework for Response and Information Access***

*A synchronized, continuous flow of information available to cyber incident stakeholders created a common framework for response, impact development, and discussions. Early and ongoing information access strengthened the relationship between domestic and international cyber response communities*.

Observations:

- Much like the real world, Cyber Storm presented situations where at times there was an absence of information and at others, an overabundance of data. The majority of players reported difficulty in identifying accurate and up-to-date sources of information. Multiple alerts on a single issue created confusion among players, making it difficult to establish a single coordinated response. Players noted that the concept of a single point for information would enable a common framework for all to work from and likely increase effective response.

- US-CERT provided significant actionable information in the form of alerts and technical bulletins. However, the need to further explore US-CERT capabilities to post information in a timely, secure, and accurate manner was also noted. Participants believed US-CERT is the correct agency to disseminate time sensitive and critical information to the appropriate organizations.

***Finding 7: Strategic Communications and Public Relations Plan***

*Public messaging must be an integral part of a collaborated contingency plan and incident response to provide critical information to the incident response community and empower the public to take appropriate individual protective or response actions consistent with their particular situations.*

Observations:

- To the private sector *public affairs* was interpreted as *strategic communications*. Observers noted that cross-sector (public-private) alignment of communications and public relations plans must be in place in order to have a coordinated approach during a crisis situation.
- It is important for public affairs to be a part of the planning and response process, as it plays a vital role in shaping public and consumer response and confidence, as well as providing information to the general public and media. For example, as the Transportation Sector observed, publicly released information on a private sector entity could undermine consumer confidence and have potentially large-scale negative impacts on their business viability.
- Cyber Storm highlighted the importance of coordinating and integrating incident communications and public affairs outreach. Players observed that communication to the public through the issuance of press releases alone was not sufficient in all cases. Tangible demonstration of response activity is equally vital in providing the public with the reassurance needed to maintain general public confidence.
- Federal responses must include agile public affairs teams to ensure that press releases and accurate situation updates are provided to partner organizations as well as media outlets. Coordination among these teams will ensure that inaccurate coverage is countered in a timely manner and that all Federal officials are provided a consistent message in addressing a situation. Success in this area increases public trust and will minimize the adverse impact of individuals and businesses reacting to incorrect information.

***Finding 8: Improvement of Processes, Tools and Technology***

*Improved processes, tools, and training focused on the analysis and prioritization of physical, economic, and national security impacts of cyber attack scenarios, will enhance the quality, speed, and coordination of response. This is particularly true in the case of integrated or cascading attacks or consequences.*

Observations:

- There was a great deal of research and discovery in the area of Supervisory Control and Data Acquisition (SCADA) patching processes during the exercise planning process. This process identified and demonstrated the various difficulties that would result in recovery if a vulnerability existed.

Exchanging and sharing classified information among organizations proved to be a challenge. Processes must be developed to address and share critical information at lower classification levels throughout the response community. Clearly defined communication channels and processes need to be developed to downgrade/sanitize and share information from classified sources with organizations involved in cyber response activities.

## EXERCISE PLAY

The exercise simulated a sophisticated cyber attack campaign through a series of scenarios directed against critical infrastructures. The intent of these scenarios was to highlight the interconnectedness of cyber systems with the physical infrastructure and to exercise coordination and communication between the public and private sectors. Each of the scenarios was developed with the assistance of industry experts and was executed in a closed and secure environment.

The exercise was a simulated event with no real world effects on, tampering with, or damage to any critical infrastructure. While the scenarios were based on hypothetical but possible situations, they were not intended as a forecast of future terrorist-related events. The collective Cyber Storm scenarios had three major adversarial objectives:

- To disrupt specifically targeted critical infrastructures through cyber attacks
- To hinder the governments' ability to respond to the cyber attacks
- To undermine public confidence in the governments' ability to provide/protect services

The simulated adversaries did not represent a specific or existing terrorist group, activist group, or nation state. The simulated attackers were a loose coalition of well financed "hacktivists" with a political agenda, who directed anti-globalization and anarchist activism around the world using their computer skills. Implementing a consorted and sophisticated cyber campaign, the adversaries aimed to make political statements and protest actions by government and industry by perpetrating attacks across multiple infrastructures and misleading news media.

Key elements of the hacker attack plan were to strike at trusted cyber systems that were used to control both physical infrastructures and digital commerce and services. The attackers focused on maximizing economic harm and fomenting general distrust of big business and government by disrupting services and misleading news media and other information outlets. Effective response to the scenario was designed to require rapid communications and deconfliction of critical information between players in all sectors and organizations, as well as strategic integration of information to gain accurate situational awareness.

It is important to emphasize that the exercise scenario was neither a forecast of any particular threats or vulnerabilities currently existing nor an expression of any specific concerns. Rather, the scenario was designed to elicit certain player action(s) in response to the hypothetical situation in order to achieve the exercise objectives.

### Sample Scenario

The scenario vignette below is only one of many that exercised cyber preparedness, coordination and response at State and Federal levels. In this case, there were a series of suspicious events that led to an incident that compelled a State Chief Information Security Officer (CISO) to approach the State governor and request standup (activation) of the State's Emergency Operations Center.

The circumstances the CISO was concerned about included the following:

- Hackers broke into the HIPAA (Health Insurance Portability and Accountability Act) database, which could potentially compromise the public's medical records

- State officials learned through communications between the State, the Multi-State State Information Sharing and Analysis Center (MS-ISAC), and the US-CERT about reports from the Intelligence Community of nonspecific cyber threats
- Upon consulting with the MS-ISAC, it was revealed that six other states were having similar problems
- Reports that certain State service support systems (everything from welfare to license issuing) were down or behaving erratically due to what appeared to be a massive computer virus attack

After evaluating the alleged incidents, the Governor determined that the threats were coordinated and serious enough to stand up the State Emergency Operations Center and reported the situation to the HSOC. Several Federal law enforcement, intelligence, homeland security, defense, and sector-specific departments/agencies were able to act in coordination with their international counterparts to reduce the impact of additional attacks, identify and neutralize critical threats, and reconstitute infrastructure elements and public confidence.

Although the State maintained control and successfully halted the attacks, the CISO received indication from the attackers that this type of situation would reoccur if their extortion demands were not met. The State in question took the threat seriously, coordinating efforts with the Federal Bureau of Investigation (FBI) to apprehend the adversary and continuing their cyber response procedures.

This information flow was one of many that allowed players to connect information from over 700 e-mail and telephone injects[6] from control, as well as thousands of communications between players, into a picture of a concerted campaign by well-financed and determined attackers.

## STAKEHOLDER AND MEDIA OUTREACH

For purpose of the exercise the DHS Office of Public Affairs (OPA) established and led a Public Affairs Working Group (PAWG) to coordinate all Cyber Storm public affairs initiatives. The PAWG consisted of public affairs representatives from Cyber Storm stakeholders and players. In coordination with the PAWG, DHS OPA led Cyber Storm media outreach efforts and produced all public affairs materials.

The OPA also initiated a core set of Cyber Storm communications tools, including a Cyber Storm fact sheet (see Appendix B) and press release (see Appendix C) announcing the conclusion of the exercise. In an effort to maintain coordination in media outreach and communication to the public, DHS OPA shared outreach plans and communications tools to exercise stakeholders through the PAWG. Coordinating public affairs exercise play, the OPA also sponsored a warm-up table top exercise prior to Cyber Storm that identified the need for NCRCG technical advisors to the Public Affairs staffs/Joint Information Center (JIC) in order to translate complex issues into terms understood by the general public.

---

6 *Term "injects" refers to pre-scripted messages that place an exercise event into exercise. Injects are the means by which the Master Scenario Events List (MSEL) incidents are disseminated into exercise play.*

## VIP Visit Program

Our nation's critical cyber infrastructures are safeguarded by a vast, diversified universe of hardware, software and people. Synergizing these assets requires broad support from stakeholders within and beyond the IT and homeland security communities. The VIP Visit Program was designed to demonstrate the value of Cyber Storm and cyber security to key stakeholders and opinion leaders, and to educate them on the efforts being made by DHS, NCSD, and others.

### *Outreach*

Cyber Storm exercise control activities took place at the United States Secret Service (USSS) Headquarters in Washington, DC. Program designers initiated the invitee outreach process by identifying key exercise stakeholders inside and outside the cyber security community. Cyber Storm participant organizations also played a role in identifying and vetting priority invitees. Invitations were extended to elected officials, international partner representatives, government executives, military commanders, and private industry corporate officers.

A total of 117 VIP visitors attended the Cyber Storm briefings. Among this group were Members of Congress and staff; corporate officers from 10 private sector player organizations; NCSD key partners representing 16 trade and issue advocacy organizations; Federal and State officials from 18 participant government agencies; and international partners from Australia, Canada, New Zealand, and the United Kingdom.

The VIP Visit Program provided attendees an opportunity to (1) learn about DHS and NCSD cyber preparedness efforts; (2) further understand the goals and processes of the exercise; and (3) observe the Exercise Control (ExCon) Center. VIPs attended scheduled briefings delivered by NCSD senior leadership and completed tours of the Cyber Storm Control Center at the United States Secret Service Headquarters over a period of three days (February 7 to 9), each visit running approximately 1 hour and 30 minutes.

The VIP program helped illustrate how NCSD and its stakeholders work to protect the Nation's critical infrastructure and prepare governments and organizations to effectively respond to a cyber-related Incidents of National Significance.

## Media Outreach

Cyber Storm not only provided an opportunity to exercise communication and coordination among Federal, State, international, and private sector entities, but also served as a ground to educate the public on the need for and the importance of cyber security. To this end, DHS conducted a media outreach campaign to educate the press and the public on the steps that the Department of Homeland Security is taking to coordinate enhancement of our nation's cyber preparedness.

On the final day of Cyber Storm, Friday, February 10, 2006, a press conference was held at DHS Headquarters in Washington, D.C. DHS Undersecretary of Preparedness George Foresman delivered the opening remarks about the importance of exercises and the interconnectedness of physical and cyber security. Mr. Andy Purdy, Acting Director of NCSD, then discussed the exercise's mission and goals and provided examples of scenarios. Executives from participating public and private sector organizations were also present and available to answer questions from

the press regarding their involvement with the exercise. A full transcript of this press conference can be found on the DHS web site at: http://www.dhs.gov/dhspublic/display?content=5431.

The media coverage resulting from DHS outreach efforts is an indication of the increasing interest in cyber security and the significance of conducting an exercise of this scale. The exercise especially highlighted the international appeal in that media coverage appeared in over 12 countries worldwide.

The media is a key ally in informing and educating the public during national emergencies of a physical or cyber nature. Cyber Storm has helped raise awareness of the importance of cyber security and the measures that our nation, its organizational components, and its international counterparts have begun to implement to protect its citizenry.

## CONCLUSION

Cyber Storm provided government, private sector, and international participants with a neutral and controlled environment in which to exercise their response procedures to a significant and coordinated cyber attack. The exercise examined information sharing mechanisms, procedures for establishing situational awareness, public-private sector decision making, and communication of appropriate information to the public during a Cyber Incident of National Significance.

DHS, NCSD, and their partners are moving rapidly to turn the lessons learned from Cyber Storm into solutions. These include, but are not limited to procedures, policy and practice development, and recommendations for organizational changes. Other exercise participants are also taking measures to address findings related to their organization and/or sector.

Cyber Storm presented the cyber incident response community with a type of attacker that they had not yet extensively dealt with in the real world. The attacker used multiple cyber attack vectors, which overlapped and reinforced one another, then exacerbated public and market responses by encouraging and injecting believable but misleading information in the media. In order to effectively respond, the community needed to communicate at the highest levels with appropriate tools requiring correlation, coordination and collaboration. By and large, the participating organizations and their practices met the challenges presented and, where necessary, improvised agreements and relationships to handle unexpected issues. It became apparent that a broader and deeper understanding of the National Response Plan is needed by all members of the community.

The cyber community must continue to improve its ability to effectively respond to and recover from the most sophisticated of cyber attacks. In doing so, formalization of many of these practices into standard operating procedures and contingency plans, clarification of roles and responsibilities of players and organizations, and further training and exercises must be considered. The interdependencies, gaps in response structure, and positive cross-sector collaboration between infrastructure sectors, Federal and State, international and domestic are all critical parts of Cyber Storm lessons learned and will have enduring impact throughout the player communities.

# APPENDIX A – PARTICIPATING ORGANIZATIONS

- Department of Commerce
  - National Telecommunications & Information Administration
  - Bureau of Industry and Security
  - Office of the Chief Information Officer
- Department of Defense
  - Joint Staff
  - National Military Command Center
  - U.S. Northern Command
  - U.S. Strategic Command
  - Joint Functional Component Command – Network Warfare
  - Joint Task Force – Global Network Operations
  - Office of the Assistant Secretary of Defense for Networks and Information Integration
  - Information Assurance Directorate, Office of the Assistant Secretary of Defense, Networks and Information Integration
- 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
- Federal Deposit Insurance Corporation
- Federal Reserve Bank of New York
- Department of Justice
  - Computer Crime and Intellectual Property Section
  - Federal Bureau of Investigation
- Department of Health and Human Services
- Director for National Intelligence
  - Central Intelligence Agency
  - Intelligence Community Incident Response Center
- Interagency
  - National Cyber Response Coordination Group
  - Interagency Incident Management Group
- Office of Management & Budget
- National Security Council
- Homeland Security Council
- Department of Homeland Security
  - National Cyber Security Division/US Computer Emergency Readiness Team
  - National Communications System
  - Transportation Security Administration/Transportation Security Operations Center
  - United States Secret Service
  - Homeland Security Operations Center
  - Homeland Security Information Network
  - Immigration and Customs Enforcement (Customs and Border Protection)
  - Infrastructure Partnerships Division (NICC, CWIN, PCII, HSIN, ICAO)
  - Intelligence & Analysis
  - Science & Technology (DETER Testbed)
  - Operations Directorate/Incident Management Division (IMD)
  - 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
- American Red Cross
- Multi-State ISAC
- State Government of Michigan
- State Government of Montana
- State Government of New York
- Financial Services ISAC
- Financial Services Private Sector
  - 1 Major Banking & Finance Company
- Information Technology ISAC
- Information Technology Private Sector
  - 11 Major IT Corporations
- Communications ISAC
  - Telecommunications simulation cell
- Electricity Sector ISAC
- Energy Private Sector
  - North American Electric Reliability Council
  - 7 Major Electric Power Companies
- Transportation Private Sector
  - NAV CANADA
  - 2 Major Air Carriers
- International Lead Participants
  - Canada – Public Safety and Emergency Preparedness Canada
  - UK – National Infrastructure Security Co-Ordination Centre
  - Australia – Attorney General's Department
  - New Zealand – Centre for Critical Infrastructure Protection

## APPENDIX B – CYBER STORM FACT SHEET

*Press Office*
**U.S. Department of 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.

## APPENDIX C - CYBER STORM PRESS RELEASE

*Press Office*

**U.S. Department of Homeland Security**

# Press Release

February 10, 2006

Contact: Press Office 202-282-8010

### U.S. DEPARTMENT OF HOMELAND SECURITY CONDUCTS CYBER SECURITY EXERCISE TO ENHANCE NATION'S CYBER PREPAREDNESS

***International, Federal, State, and Private Sector Coordination***

***Affecting Key Critical Infrastructure Sectors Examined***

*Washington, D.C.* -- The U.S. Department of Homeland Security (DHS) today announced the completion of Cyber Storm, the largest government-led cyber security exercise to examine response, coordination, and recovery mechanisms to a simulated cyber-event within international, Federal, state, and local governments in conjunction with the private sector.

"Cyber security is critical to protecting our Nation's infrastructure because information systems connect so many aspects of our economy and society," said Mr. George W. Foresman, Under Secretary for Preparedness at DHS. "Preparedness against a cyber attack requires partnership and coordination between all levels of government and the private sector. Cyber Storm provides an excellent opportunity to enhance our Nation's cyber preparedness and better manage risk."

Cyber Storm emphasizes the Administration's commitment to cyber security and preparedness. The exercise simulated a sophisticated cyber attack through a series of scenarios directed against critical infrastructures. For example, one of the scenarios simulated a cyber incident where a utility company's computer system is breached, causing numerous disruptions to the power grid. The intent of this scenario is to highlight the interconnectedness of cyber security with the physical infrastructure and to exercise coordination and communication between the public and private sectors. Each of the scenarios was developed with the assistance of industry experts and was executed in a closed and secure environment.

Cyber Storm exercised national cyber incident response within the context of a large-scale cyber incident affecting the energy, IT, telecommunications, and transportation sectors. Capabilities examined included:

- Interagency coordination through the National Cyber Response Coordination Group;
- Identification of policy issues that affect response and recovery;
- Identification of critical information sharing paths and mechanisms among public and private sectors; and
- Improvement and promotion of public and private sector interaction.

The exercise was a simulated event, and there were NO real world effects on, tampering with, or damage of any critical infrastructure. While the exercise scenario was based on a hypothetical situation, it was not intended as a forecast of future terrorist related events.

Cyber Storm participants included members of the public sector (Federal, and state agencies), the private sector (information technology, telecommunications, energy, transportation, and financial services firms selected by Industry Information Sharing and Analysis Centers and sector specific agencies), and select international government partners.

As part of Secretary Michael Chertoff's reorganization of DHS, the new Preparedness Directorate will enhance coordination and deployment of preparedness assets in order to best address potential threats – both present and future – that face our nation. The Preparedness Directorate includes the Office of Infrastructure Protection, the National Cyber Security Division, the National Communications System, the Office of Grants and Training, the U.S. Fire Administration, the Office of National Capitol Region Coordination, and the Office of the Chief Medical Officer.

###

## APPENDIX D - ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| DHS | Department of Homeland Security |
| DoD | Department of Defense |
| DRG | Domestic Readiness Group |
| ExCon | Exercise Control |
| FBI | Federal Bureau of Investigation |
| HIPAA | Health Insurance Portability and Accountability Act |
| HSOC | Homeland Security Operations Center |
| IC | Intelligence Community |
| IIMG | Interagency Incident Management Group |
| IMPT | Incident Management Planning Group |
| IT | Information Technology |
| ISAC | Information Sharing and Analysis Center |
| MS-ISAC | Multi-State Information Sharing and Analysis Center |
| NCE | National Cyber Exercise: Cyber Storm |
| NCRCG | National Cyber Response Coordination Group |
| NCSD | National Cyber Security Division |
| OPA | Office of Public Affairs |
| PAWG | Public Affairs Working Group |
| SCADA | Supervisory Control and Data Acquisition |
| SSA | Sector Specific Agencies |
| SOP | Standard Operating Procedures |
| US-CERT | U.S. Computer Emergency Readiness Team |