**THE PRESIDENT'S**
**NATIONAL SECURITY TELECOMMUNICATIONS**
**ADVISORY COMMITTEE**


# *OPERATIONS SUPPORT GROUP REPORT*

## SEPTEMBER 1998

# OPERATIONS SUPPORT GROUP REPORT
# TABLE OF CONTENTS

## EXECUTIVE SUMMARY

The President's National Security Telecommunications Advisory Committee's (NSTAC) Operations Support Group (OSG) was formed in April 1997 to evaluate the overall progress and direction of national security and emergency preparedness (NS/EP) operational activities. Among its specific taskings, the OSG was instructed to refine NSTAC's national coordinating mechanism (NCM) concept and develop standardized intrusion incident information reporting criteria for the National Coordinating Center for Telecommunications (NCC). Two OSG subgroups, the NCC Vision-Operations Subgroup and the NCM Subgroup, respectively, addressed these actions. This report presents the charge, activities, analysis, conclusions, and recommendations of the OSG and its two subgroups.

An NCM process would provide senior Federal Government decisionmakers with real-time information from related components of critical national infrastructures to enhance NS/EP. In May 1998, the President released Presidential Decision Directive (PDD) 63,[1] a critical infrastructure protection directive establishing the National Infrastructure Protection Center (NIPC) and calling for industry to voluntarily participate in the Government's efforts to ensure the security of the Nation's infrastructures. In a series of meetings with Government officials from the President's Commission on Critical Infrastructure Protection Transition Team and the NIPC, members of the Industry Executive Subcommittee (IES) and the NCM Subgroup shared their NCM concept, describing how a virtual information sharing process based on the NCM concept and the NCC could be established. PDD-62[2] was also issued in May 1998 establishing a structure for overseeing a wide range of Government agency policies and programs to defeat terrorism.

The IES approved the NCC Vision-Operations Subgroup's *NCC Intrusion Incident Reporting Criteria and Format Guidelines* in May 1998 for use in the NCC's 120-day-long electronic intrusion incident information processing pilot. The NCC officially began the pilot program in June 1998 for processing reports from industry and Government service providers and network operators regarding public network electronic intrusions.

The NCC Vision-Operations Subgroup accepted additional tasking to support the NCC's efforts to coordinate a response to potential network outages caused by the Year 2000 (Y2K) problem.

The following recommendations are based on the OSG's determinations.

### Recommendations to the President

The President should direct the lead departments and agencies as designated in PDD-63 to:

- establish an industry-Government coordinating body to advise in the selection of a sector coordinator and provide continuing advice to effectively represent each critical infrastructure, and

[1] Protecting America's Critical Infrastructures: Presidential Decision Directive 63
[2] Combating Terrorism: Presidential Decision Directive 62

- consider adapting the NCC model as appropriate for the various critical infrastructures to provide warning and information centers for reporting and exchange of information with the NIPC through the NCM process.

**Recommendation to the NSTAC**

The NSTAC should task the IES to continue to refine the NCM concept in coordination with the designated Government departments and agencies developing critical infrastructure protection plans, processes, and procedures.

**Recommendations to the IES**

The IES should task the OSG to:

- review and make recommendations on the makeup of the NCC to accomplish its expanded mission, focusing on facilities, staffing, funding, and support tools and resources,

- continue to monitor PDD-39[3] and PDD-62 related activities for impacts on NS/EP telecommunications,

- continue to monitor and identify Global Information Infrastructure NS/EP issues, and

- assist the NCC in its Y2K preparation and provide coordination efforts if existing NCC processes and procedures prove inadequate in responding to potential Y2K outages.

[3] Counterterrorism Policy: Presidential Decision Directive 39

## 1.0 INTRODUCTION/BACKGROUND

The President's National Security Telecommunications Advisory Committee's (NSTAC) Industry Executive Subcommittee (IES) created the Operations Support Group (OSG) to evaluate the overall progress and direction of national security and emergency preparedness (NS/EP) operational activities. OSG members represent the telecommunications, information technology, and systems integration industries and provide unique perspectives on the challenges of NS/EP operations and planning.

In October 1996, the IES created the National Coordinating Center for Telecommunications (NCC) Vision Task Force to determine whether the mission, organization, and capabilities of the NCC should be changed, considering the ongoing changes in technology, industry composition, threats, and requirements. The OSG assumed oversight of the task force in April 1997, renaming it the NCC Vision Subgroup and later the NCC Vision-Operations Subgroup. The National Coordinating Mechanism (NCM) Subgroup was originally formed before NSTAC XX to examine the need for and feasibility of a cross-infrastructure NCM.

## 2.0 CHARGE

The IES charge to the OSG for the NSTAC XXI cycle included the following:

- refine the concept of an NCM
  - explore and identify linkages within Government and between critical infrastructures.
  - solicit Government participation to develop the NCM process
    - National Communications System (NCS) member departments and agencies
    - White House/President's Commission on Critical Infrastructure Protection (PCCIP) Transition Team.

- develop standardized intrusion incident information reporting criteria for the NCC
  - work with the Office of the Manager, NCS (OMNCS) and the Manager, NCC, to implement the intrusion incident processing pilot
  - utilize *Draft NCC Intrusion Incident Reporting Criteria and Format Guidelines* to develop final guidelines.

Other ongoing charges to the OSG included:

- assess emergency communications capabilities in the context of U.S. counterterrorism policy concerning nuclear, biological, and chemical (NBC) materials
  - monitor OMNCS and industry participation in the telecommunications disaster planning aspect of the Federal Emergency Management Agency (FEMA) NBC study

- assess Global Information Infrastructure developments to identify NS/EP issues
  - identify the status of the World Trade Agreement

– assess Global Mobile Personal Communications by Satellite Memorandum of Understanding developments.

## 3.0 ACTIVITIES

### 3.1 The NCM Concept

#### *3.1.1 Analysis*

In October 1997, the PCCIP issued its final report and recommendations on an infrastructure protection framework encompassing the Nation's critical infrastructures. Meanwhile, as a result of NSTAC XX recommendations, the NCM Subgroup began to share its NCM concept with Government officials in a series of meetings.

Two Presidential Decision Directives (PDD) were issued in May 1998. PDD-62 was issued to achieve the President's goal of defeating terrorism, managing the consequences should such an attack occur, and protecting computer-based systems. The President also released PDD-63, a critical infrastructure protection directive establishing the National Infrastructure Protection Center (NIPC) and calling for industry to voluntarily participate in the Government's effort to ensure the security of the Nation's infrastructures. These infrastructures include telecommunications, banking and finance, energy, transportation, and essential Government services. As part of the directive, an industry-funded information sharing and analysis center was also proposed. This center would be used to funnel threat information and analysis between industry and the NIPC.

In a series of meetings with Government officials from the PCCIP Transition Team and the NIPC, members of the IES and the NCM Subgroup shared their NCM concept,[4] describing how a virtual information sharing process based on the NCM concept and the NCC could be established. The subgroup also discussed industry's potential role in the new infrastructure protection environment, including its views on a multi-infrastructure, information-sharing construct.

These meetings led to direct NCC□NIPC coordination. Instead of establishing a new, independent NCM plan, the subgroup tracked Government initiatives and provided input for the Government's infrastructure protection plans. NCC representatives provided NCC Standing Operating Procedure (SOP) 016, Public Network Electronic Intrusion Indications, Assessment, and Warning Activities, for review by NIPC representatives. The SOP enabled the NIPC to consider potential media for exchange of information, appropriate points of contact, and various scenario-based training and exercise needs. As a result of this cooperation, an NCC□NIPC memorandum of understanding is being developed to detail the flow of information between the two entities.

[4] For a more detailed description of the NCM concept, see the *Operations Support Group Report to NSTAC XX*, December 1997, specifically that report's Annex titled *Information Assurance: A Joint Report of the IA Policy Subgroup of the Information Infrastructure Group and the NCM Subgroup of the Operations Support Group.*

### *3.1.2 Conclusions*

Because the Government is continuing to establish an information reporting structure, the NCM concept cannot be finalized at this time. However, experience within NSTAC indicates that more than one individual may be required to adequately represent each critical infrastructure sector.

The NCC provides a model, which is currently being examined to provide cyber indications, alerting, and warning, through which several telecommunications companies have found it worthwhile to provide, at their own expense, personnel to work with the Government in facilities provided by the Government. It can provide a model for cooperation and the gathering, analyzing, sanitizing, and disseminating of information that can be scaled appropriately to fit the other critical infrastructures.

### *3.1.3 Recommendations*

The OSG proposes the following recommendations**.**

#### *3.1.3.1 Recommendations to the President*

The President should direct the lead departments and agencies as designated in PDD-63 to:

- establish an industry Government coordinating activity to advise in the selection of a sector coordinator and provide continuing advice in order to effectively represent each critical infrastructure, and

- consider adapting the NCC model as appropriate for the various critical infrastructures to provide warning and information centers for reporting and exchange of information with the NIPC through the NCM process.

#### *3.1.3.2 Recommendation to the NSTAC*

The NSTAC should task the IES to continue to refine the NCM concept in coordination with the designated Government departments and agencies developing critical infrastructure protection plans, processes, and procedures.

## 3.2 NCC Vision-Operations Subgroup Intrusion Incident Information Reporting Criteria

### *3.2.1 Analysis*

When the NCC Vision Task Force formed in October 1996, the Manager, NCS, requested that the NSTAC assist the NCS in developing a concept of operations (CONOPS) and implementing an electronic intrusion indications and reporting capability in the NCC. The Manager also asked that the NCC's information assurance capabilities include the ability to evaluate intrusion incidents and take mitigative actions. The IES then formally instructed the task force to examine the NCC's membership; the NCC's role in relation to critical control networks of other infrastructures; and NCC indications, detection, and warning functions and relationships to

national information assurance activities, such as the PCCIP. The task force held its first meeting on November 15, 1996.

When the IES reorganized in April 1997, the OSG was assigned oversight of the NCC Vision Task Force. The OSG renamed the task force the NCC Vision Subgroup, and later the NCC Vision-Operations Subgroup.

Based on the Intrusion Incident Information CONOPS, developed by the NCC Vision Subgroup for NCC intrusion incident information processing, and a tabletop exercise validating the CONOPS, the NSTAC concluded that the NCC Charter was broad enough to allow the addition of an Indications, Assessment, and Warning (IAW) mission. The Manager, NCS, then tasked the NCC with implementing a pilot program as a result of the OSG's recommendation to NSTAC XX in December 1997. The NCC modified its SOP to accommodate the electronic intrusion incident information processing capability.

In May 1998, the NCC Vision-Operations Subgroup completed the *NCC Intrusion Incident Reporting Criteria and Format Guidelines* with the assistance of various Government department and agency representatives. The subgroup emphasized that the reporting criteria focused on receipt of timely reports and assessments by industry and Government and accounted for intrusions that could directly or indirectly affect network integrity and performance involving the telecommunications infrastructure. The subgroup determined that intrusion reports should be voluntarily submitted to the NCC and should include the following components: the type of system attacked, data feedback, an analysis of the intrusion incident, implications of the intrusion incident, damage assessment, and needed response actions.

Following IES approval of the reporting criteria, the OSG assisted the Manager, NCC, in initiating the voluntary NCC electronic intrusion incident information processing pilot. The subgroup stressed the need for industry and Government participation in the pilot and its final evaluation.

For the duration of the pilot, the NCC Vision-Operations Subgroup decided to close the *NCC Intrusion Incident Reporting Criteria and Format Guidelines* to further changes, emphasizing that changes would be considered after the pilot's conclusion. The NCC started the intrusion pilot on June 15, 1998, for a 120-day trial period. Center operations are being conducted in accordance with the CONOPS developed by the NCC Vision-Operations Subgroup and NCC SOP 016. At the end of the 120-day trial, center activities will be reviewed and the IAW process evaluated.

### *3.2.2 Conclusion*

The ongoing work of the electronic intrusion incident information pilot program, the NCC Year 2000 (Y2K) coordination study (see Section 3.5), and other ongoing efforts may reveal a requirement for expanded NCC capabilities.

### *3.2.3 Recommendation*

The OSG proposes the following recommendation.

*3.2.3.1 Recommendation to the IES*

The IES should task the OSG to review and make recommendations on the makeup of the NCC to accomplish its expanded mission, focusing on facilities, staffing, funding, support tools, and resources.

## 3.3 Emergency Communications Capabilities in the Context of U.S. Counterterrorism Policy Concerning NBC Materials

### *3.3.1 Analysis*

PDD-39, published on June 21, 1995, emphasizes interagency coordination to prevent and manage the consequences of terrorism in all its forms, including matters related to NBC terrorism, or threats to the Nation's infrastructure. PDD-62, issued in May 1998, established a National Coordinator for Security, Infrastructure Protection, and Counterterrorism to oversee programs and policies of Government agencies to defeat terrorism. When PDD-62 is made available to industry, OSG will review the PDD and monitor related activities.

The OSG continued to monitor Government and NCC PDD-39-related activities during the NSTAC XXI cycle. In response to PDD-39, FEMA was tasked with analyzing the adequacy of the Federal Government to respond to the consequences of terrorist incidents involving NBC material within the United States. The NCS, as a member of the Catastrophic Disaster Response Group, assisted in developing that assessment. As a follow-on effort, the OSG assisted the NCS in determining the telecommunications industry's capabilities for maintaining critical facilities following an NBC attack. Specifically, the OSG monitored the results of an NCS survey of NCC member companies and provided qualified discussion group members to verify the relevant findings.

The survey revealed that several of the companies polled were aware of the NBC problem and had addressed it. The remaining companies had not included NBC terrorist events in their contingency planning.

### *3.3.2 Conclusion*

Efforts to ensure awareness of NBC terrorism implications for NS/EP telecommunications are ongoing. The survey provided preliminary data. The OSG will continue to monitor developments in this area.

### *3.3.3 Recommendation*

The OSG proposes the following recommendation.

*3.3.3.1 Recommendation to the IES*

The IES should task the OSG to continue to monitor PDD-39 and PDD-62 related activities for impacts on NS/EP telecommunications.

## 3.4 Global Information Infrastructure Developments

### *3.4.1 Analysis*

When the NSTAC's National Information Infrastructure Task Force concluded in March 1997, the IES decided that the OSG should monitor the U.S. information infrastructure's global interfaces because of the potential for increased vulnerabilities adversely affecting the national interest. The OSG continued to monitor Global Information Infrastructure (GII) developments in the NSTAC XXI cycle to consider the NS/EP implications of the International Telecommunication Union's (ITU) Global Mobile Personal Communications by Satellite (GMPCS) Memorandum of Understanding (MOU).

The GMPCS MOU dates back to the ITU's 1996 World Technology Policy Forum. The MOU was developed as one of the forum's nonbinding opinions, addressing the establishment of unrestricted circulation of GMPCS user terminals. GMPCS arrangements included mutual recognition agreements between nations regarding approval of equipment, terminal marking and identification methods, and authorized national authorities' access to traffic data. Some aspects of these arrangements have been contentious issues within the international telecommunications community.

### *3.4.2 Conclusion*

Although there are security issues requiring resolution by the ITU, the agreement is expected to facilitate increased transport of approved GMPCS, thereby facilitating NS/EP telecommunications.

### *3.4.3 Recommendation*

The OSG proposes the following recommendation.

*3.4.3.1 Recommendation to the IES*

The IES should task the OSG to continue to monitor and identify GII issues.

## 3.5 NCC Coordination Requirements for Year 2000 Response

### *3.5.1 Analysis*

In light of the NCS's enhancement of the National Telecommunications Coordinating Network (NTCN) and the NSTAC Network Group's study of Y2K preparedness, the NCC Vision-Operations Subgroup accepted additional tasking to evaluate NCC resources and help determine its coordination requirements for potential outages caused by any Y2K problems. Recognizing

that the previous NTCN concept had not included a response to the Y2K problem, the NCC Vision-Operations Subgroup agreed to review and evaluate critical Government and industry operations centers that might require connectivity to the NCC via nonpublic network based multicommunication media. While working on this issue, the subgroup agreed to support NCC efforts to review procedures for response to public network outages caused by Y2K. The NCC Vision-Operations Subgroup agreed that if the NCC identified any shortfalls in its existing procedures, the subgroup would provide assistance as needed.

The subgroup also noted that NCC member companies should report any information from Y2K outages to the NCC. Through the NCC, Federal departments and agencies would be made aware of telecommunications remediation efforts while allowing the NCC member companies to focus solely on restoring the public network. The subgroup also agreed that the NCC should encourage Government entities with NS/EP responsibilities to consider the Telecommunications Service Priority (TSP) System to ensure that critical circuits have priority restoration in the event of Y2K outages.

### *3.5.2 Conclusion*

The subgroup concluded that existing NCC processes and procedures used to respond to public network outages should be adequate to respond to potential Y2K outages.

### *3.5.3 Recommendation*

The OSG proposes the following recommendation.

#### *3.5.3.1 Recommendation to the IES*

The IES should task the OSG to assist the NCC in its Y2K preparation and provide coordination efforts if existing NCC processes and procedures prove inadequate in responding to potential Y2K outages.

## 4.0 SUMMARY OF RECOMMENDATIONS

In summary, the OSG proposes the following recommendations.

### 4.1 Recommendations to the President

The President should direct the lead departments and agencies as designated in PDD-63 to:

- establish an industry□Government coordinating activity to advise in the selection of a sector coordinator and provide continuing advice to effectively represent each critical infrastructure, and

- consider adapting the NCC model as appropriate for the various critical infrastructures to provide warning and information centers for reporting and exchange of information with the NIPC through the NCM process.

### 4.2 Recommendation to the NSTAC

The NSTAC should task the IES to continue to refine the NCM concept in coordination with the designated Government departments and agencies developing critical infrastructure protection plans, processes, and procedures.

### 4.3 Recommendations to the IES

The IES should task the OSG to:

- review and make recommendations on the revised makeup of the NCC to accomplish its expanded mission, focusing on facilities, staffing, funding, and support tools and resources,
- continue to monitor PDD-39 and PDD-62 related activities for impacts on NS/EP telecommunications,
- continue to monitor and identify GII NS/EP issues, and
- assist the NCC in its Y2K preparation and provide coordination efforts if existing NCC processes and procedures prove inadequate in responding to potential Y2K outages.

# ANNEX A

# OPERATIONS SUPPORT GROUP MEMBERS

## OPERATIONS SUPPORT GROUP MEMBERS

| | |
|---|---|
| COMSAT | Mr. Ernie Wallace, Chair |
| EDS | Mr. Bob Donahue, Vice-Chair |
| U S WEST | Mr. Jon Lofstedt, Vice-Chair |
| | |
| AT&T | Mr. Dave Bush |
| CSC | Mr. Guy Copeland |
| GTE | Ms. Ernie Gormsen |
| ITT | Mr. Joe Gancie |
| MCI | Mr. Michael McPadden |
| NTA | Mr. Bob Burns |
| Nortel | Dr. Jack Edwards |
| SAIC | Mr. Bernie Ziegler |
| Teledesic | Mr. Gordon Booker |
| Unisys | Dr. Dan Wiener |
| USTA | Dr. Vern Junkmann |

## GOVERNMENT PARTICIPANTS

| | |
|---|---|
| DOS | Mr. Stephen Springer |
| TREAS | Mr. Don Hagerling |
| DOJ | Mr. Wayne Williams |
| DOC | Mr. Jorome Gibbon |
| DOT | Mr. Rich Weigand |
| USDA | Mr. Brenda Boger |
| GSA | Mr. Tom Sellers |
| NTIA | Mr. Bill Belote |
| OMNCS-NCC | Mr. Bernie Farrell |

# ANNEX B

# NATIONAL COORDINATING CENTER FOR TELECOMMUNICATIONS INTRUSION INCIDENT REPORTING CRITERIA AND FORMAT GUIDELINES

# NCC INTRUSION INCIDENT REPORTING CRITERIA AND FORMAT GUIDELINES

## GENERAL

NCC intrusion information collection focuses on the receipt of near real-time reports and assessments by Government and industry of intrusions that may directly or indirectly affect network integrity and performance involving the telecommunications sector of the critical national infrastructures.

Report the incident as soon as possible even though the available information is incomplete.

Report to the NCC (if your organization is one with a resident representative at the NCC, report through the resident representative; otherwise, report directly to the NCC).

Report using appropriate means to guarantee the delivery of information.

## REPORTING CRITERIA

Report an intrusion incident whenever you:

- Detect an intrusion occurrence, e.g.,
    - report denial/disruption of service incidents such as the physical disabling of equipment, the flooding of a communications network by waves of message traffic, etc.,
    - report breaches in communications or data security that affect the confidentiality, integrity, or availability to an authorized user of information, data, or a program or system,
    - report unauthorized electronic access to include denial/disruption of service as well as breaches in communications or data security.
- Receive any indication (information that suggests a threat) of a potential intrusion on a Government or public information system or network.
- Need verification of the scope of your problem.

## REPORTING STAGES

Provide an initial intrusion incident report upon determining that an intrusion or potential intrusion was detected or occurred.

Provide subsequent interim report(s) as appropriate upon determining more relevant facts concerning the incident.

Provide a final report upon incident closure or resolution.

## REPORTING FORMAT

An initial report should include the first category of information (Type of System Attacked or Intruded), and any other categories for which information is known. Any interim report(s) should include additional information placed in the appropriate category as it is determined. The final report should include all six categories of information as follows:

**1- TYPE OF SYSTEM ATTACKED OR INTRUDED:** Describe the type of network/system, etc. involved in the intrusion generally (e.g., LAN/WAN) and more specifically (e.g., security classification of the network or system such as Secret), the function/mission system running on the attacked network/system, the IP address as applicable, etc.

**2- DATA FEEDBACK:** If necessary, indicate information needed to help determine the scope of the incident.

**3- ANALYSIS OF INTRUSION INCIDENT:** Describe as well as possible the nature of the intrusion [i.e., what happened and how it happened (e.g., specify how the intruder gained access to the network or system, the particular vulnerability exploited, how it was exploited)]; specify when the intrusion occurred; specify any known source of the intrusion; specify any known intent, purpose, or motivation for the intrusion such as to corrupt or destroy data, manipulate data, achieve unauthorized access to data, block authorized access to data, etc.; and provide any other pertinent information.

NOTE: Report the incident as soon as possible even though the available analysis information is incomplete; provide interim reports as well as the final report later.

**4- IMPLICATIONS OF INTRUSION INCIDENT:** Describe any known potential implications of the intrusion for other network/system providers and users.

**5- ASSESSMENT OF DAMAGE:** Provide a succinct assessment of the actual damage/impact that resulted from the intrusion (e.g., corrupted or compromised data, etc.).

**6- RESPONSE ACTIONS:** Describe relevant actions taken or planned to correct the exposed vulnerabilities, repair any damage, etc., emphasizing any recommendations to preclude a similar intrusion in the future.

## INCIDENT REPORT PROCESSING AND DISTRIBUTION

When an initial report is received by the NCC, the Manager, NCC and the NCC Representative receiving the report will determine its sensitivity. The NCC Representative will sanitize the report as necessary to protect the reporting organizations and their clients. NCC personnel will then enter the report contents into the NCC Intrusion Incident Database. NCC personnel will process all reports to:

- Correlate information with any other similar incidents to see if a pattern can be determined.

- Determine to whom the report should be distributed.

- Organize and format releasable information for ease of access and use.

As soon as meaningful information on an incident is available (this may be only after interim reports are received), NCC personnel will distribute it to authorized users based on established user profiles. This approach will allow users to receive only incident information that they find useful.

As the NCC receives interim reports and final reports on the incidents, NCC personnel will update the incident database file, correlate the information again, and issue additional reports. NCC personnel will acknowledge, in writing (e.g., fax, e-mail, etc.), receipt of all reports received.

NCC personnel will forward appropriate reports to the Network Security Information Exchanges (NSIEs). As a general rule, the NCC will forward to the NSIEs reports requiring special technical expertise or lengthy analysis, a consolidated incident initial/interim/final report, and any other previously agreed upon report.