THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

The NSTAC's Input to the National Plan

An Assessment of Industry's Role in National Level Information Sharing, Analysis, and Dissemination Capabilities for Addressing Cyber Crises

November 2001

NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

November 6, 2001

The President
The White House
1600 Pennsylvania Avenue, NW
Washington, DC 20500

Dear Mr. President:

At the June 6, 2001, meeting of your National Security Telecommunications Advisory Committee (NSTAC), Mr. Richard Clarke, recently appointed as Special Advisor to the President for Cyberspace Security, asked the NSTAC to participate in revising the *National Plan for Critical Infrastructure Assurance* (National Plan).

Enclosed are the Committee's analyses and views on National Security Emergency Preparedness (NS/EP) telecommunications aspects for the National Plan. This input focuses on the need for a recognized, authoritative, national-level capability to disseminate warnings and facilitate response and mitigation efforts for cyber crises across the nation's infrastructures. Key elements of such a capability spanning public and private sectors should include information collection and sharing, information analysis, dissemination of alerts and warnings, and post-event analysis and dissemination. Information sharing and analysis is critical for ensuring that critical infrastructures will support national emergencies.

In light of the tragic events of September 11, 2001, and the establishment of the new Homeland Security Office, we understand that the National Plan will evolve to a national strategy for addressing critical infrastructure protection. To that end, we will continue to work closely with the Department of Commerce's Critical Infrastructure Assurance Office and the National Telecommunications and Information Administration's Information and Communications Sector to ensure that NS/EP telecommunications are addressed in the new strategy.

The NSTAC remains committed to providing advice to you and your Administration on critical cyber issues facing our Nation's security and emergency preparedness posture.

Sincerely,

D P Burnham

Daniel P. Burnham
NSTAC Chair

1 Enclosure:
1 NSTAC's Assessment of Industry's Role in
  National Level Information Sharing, Analysis,
  and Dissemination Capabilities for Addressing
  Cyber Crises

Copy to:
Vice President
Secretary of Defense (ASDC3I)
National Security Advisor
Special Advisor to the President for Cyberspace Security
Manager, National Communications System
Director, Critical Infrastructure Assurance Office
NSTAC Principals

TABLE OF CONTENTS

1.0 INTRODUCTION

At NSTAC XXIV, the National Coordinator for Security, Infrastructure Protection, and Counter-terrorism requested NSTAC's assistance in developing the telecommunications part of the National Plan. In addition, a new national initiative for information sharing and dissemination, the Cyber Warning Information Network (CWIN), was briefed at NSTAC XXIV as part of the discussion on information sharing capabilities. NSTAC's Industry Executive Subcommittee established the National Plan to Defend Critical Infrastructures Task Force (NPTF) to draft a response to the National Coordinator's request. Subsequently, NPTF leadership met with National Security Council (NSC) and Critical Infrastructure Assurance Office staff to discuss approaches for providing input to the National Plan. One tasking focused on providing input on capabilities for national information sharing, analysis, and dissemination to counter cyber threats. The NPTF held discussions with members of the Government's CWIN Working Group to gain an understanding of the CWIN initiative. The NSTAC's input to the National Plan (see Section 5.0), which is based on the NPTF's work, includes an industry-based assessment of a national information sharing, analysis, and dissemination capability for addressing "cyber crises." The assessment considers CWIN as a part of that larger national capability.

2.0 DESIGN PRINCIPLES FOR A NATIONAL INFORMATION SHARING, ANALYSIS, AND DISSEMINATION CAPABILITY

2.1 General Considerations

On a daily basis the Nation's critical infrastructures face some type of cyber threat. Whether that threat is intentional or unintentional, the actions of insiders, script kiddies, or hackers can affect the networks of infrastructure owners, operators, and users. The private sector owns and operates the Nation's critical infrastructures and is, for the most part, well equipped to deal with "routine" cyber events such as viruses, probes, and scans. Although largely informal, information sharing processes and mechanisms exist to facilitate response and mitigation efforts for these types of "routine" cyber events.

Coordinated, large-scale cyber events that result in or have the potential to result in a widespread outage[1] or disrupt multiple infrastructures are a national security concern. These events can be referred to as cyber crises. Cyber crises may target one or more of the following three levels: (1) end users, (2) traffic capacity, and (3) network controls. An event involving one level may affect the other levels. In addition, cyber crises affecting one infrastructure may result in problems in another infrastructure because of the interdependence of the Nation's critical infrastructures. Cyber crises may also transcend national and geographic boundaries. A national capability to

[1] A widespread outage is defined as a sustained interruption of telecommunications service that will have strategic significance to Government, industry, and the general public. Such an outage would likely affect the telecommunications service in at least one region of the country, including at least one major metropolitan area. It would involve multiple carriers, affecting both long distance and local service, and significantly degrade the ability of other essential infrastructures to function. Such an outage would have an impact on the availability and integrity of telecommunications service for at least a significant portion of a business day. *(NSTAC's Widespread Outage Subgroup)*

disseminate national warnings and facilitate response and mitigation efforts for these types of events across infrastructures does not exist.

A national capability should consider the following basic design principles:

- Be primarily concerned with cyber crises, not routine, cyber events
- Include key entities from all of the critical infrastructures
- Leverage public-private partnerships involving Government, non-Government organizations, and corporations
- Include international partners
- Provide an authoritative, national alerting and coordination mechanism across infrastructures.

2.2 Elements of a National Capability

In addition to the general considerations outlined above, key elements of a national capability spanning public and private sectors should include information collection and sharing, information analysis, dissemination of alerts and warnings, and post-event analysis and dissemination.

Information Collection and Sharing

Information collection and sharing consists of owners, operators, and users of infrastructures detecting attacks or anomalies in their networks and then sharing that information with others. Because the set of conditions surrounding each cyber crisis is unique, sources of information will likely be unique as well. Information and data can be obtained from numerous sources, including the Government, the private sector, academia, media, nonprofit organizations, for-profit vendors of security products and services, and individuals. Informal and formal processes and mechanisms exist to facilitate the collection and sharing of information; however, they must be tailored to meet the specific requirements of each event. Because sources of information cannot be identified in advance, a dedicated sharing network will most likely be unsuitable. Consequently, information sharing is distributed, ad hoc, and involves multiple subnetworks of relationships. In the context of Presidential Decision Directive (PDD) 63 and national critical infrastructure protection (CIP) policy, Information Sharing and Analysis Centers (ISAC) facilitate the collection and sharing of information from multiple subnetworks within a particular infrastructure. A recognized national-level capability to aggregate information from across the infrastructures will be required to meet CIP objectives.

Information Sharing and Analysis Centers

Presidential Decision Directive (PDD) 63: *Critical Infrastructure Protection* encouraged the establishment of an Information Sharing and Analysis Center (ISAC) as a framework for sharing information between Government and industry about vulnerabilities, threats, intrusions, and anomalies within and across infrastructures. Since PDD-63's release, multiple ISACs have been or are being established within the financial services, telecommunications, information technology, transportation, and energy sectors.

Information Analysis

Information analysis consists of interpretation and correlation of data to identify problems, solutions, and trends. Analysis turns information from multiple, disparate sources into knowledge. Analytical processes and methods are often ad hoc; they vary depending on the event. Information is analyzed through a collaborative process. Multiple entities and individuals are involved. Because of the changing nature of cyber events, it is not possible to predetermine the set of subject matter experts that will be needed to perform analysis. Building relationships with these individuals when analyzing routine events is critical to ensuring access to them during cyber crises. Analysis occurs at multiple points, beginning with affected organizations within the enterprise, then enterprisewide, and then in an ISAC. Subsequently, collaboration occurs among the enterprises within an ISAC. A national capability to provide analysis of information obtained from multiple ISACs and other sources will be required.

Dissemination of Alerts and Warnings

Dissemination of alerts and warnings consists of distributing analyzed and sanitized information in the form of alerts and warnings to infrastructure owners, operators, and users. Definitions for the terms "alert" and "warning" vary from infrastructure to infrastructure. The distribution of alerts and warnings must be controlled carefully because recipients, who vary depending on the event, want information that is timely, actionable, and issued with authority. However, the need to issue warnings quickly can limit the "authority" with which they are issued because of limits inherent in the data available at the time the warning is issued. Established processes within and across infrastructures are needed for disseminating warnings and coordinating action to ensure that infrastructure owners, operators, and users respond appropriately. Within an infrastructure, ISAC participants may agree to authorize an ISAC for a particular sector to issue an alert or warning to ISAC participants. A recognized, authoritative national-level source for issuing national cross-infrastructure alerts and warnings on behalf of the entire Nation's welfare will be required to meet CIP objectives and inform subnetworks within and across infrastructures of cyber crises.

Post-Event Analysis and Dissemination

Post-event analysis and dissemination consists of preparing and distributing "after-action reports" that provide an analysis of the event, its consequences, and lessons learned. Post-event analysis provides closure to an event by defining actions taken and outlining agreed on protection measures for mitigating or preventing further activity. Although the dissemination of after-action reports should be encouraged, reports should minimally discuss specific details of the event so as to dissuade further exploits. For participants, the ISAC framework facilitates the development and dissemination of post-event analysis. A national capability to provide post-event analysis and dissemination will be required to coordinate cross-infrastructure sharing of lessons learned.

Private enterprises in each of the infrastructures have focused their resources and CIP efforts on ISACs specific to their infrastructure. ISACs provide the private sector with a framework for interfacing with each other, and in some cases, with Government. In addition, ISACs facilitate information collection and sharing, information analysis, dissemination of alerts and warnings, and post-event analysis and dissemination in the manner agreed on by participants of the ISAC. For this reason, Government should make the ISACs the focal point for interfacing with the private sector in a national capability. Capabilities that are developed in an ad hoc manner or that bypass ISACs may result in confusion and compromise the authority required by a national capability.

A national capability must be convenient if it is to be used. Routine use may help ensure convenience and sustain readiness. In addition to developing an architecture that supports the four elements described above, processes and procedures for the capability's use should be available. A national capability will position the Nation to react to cyber crises and provide a means for returning the Nation to its "pre-crisis" state.

3.0 PROGRESS TOWARD BUILDING A NATIONAL INFORMATION SHARING, ANALYSIS, AND DISSEMINATION CAPABILITY

The Nation has made progress toward achieving its CIP goals through information sharing initiatives. Government is sponsoring the development of CWIN, an initiative designed initially to provide Government with a capability for disseminating interagency warnings and potentially for facilitating interagency information sharing and coordination. Several of the infrastructures have voluntarily established ISACs to facilitate and promote information sharing, analysis, and dissemination among industry, and in some cases, with Government. For example, the National Coordinating Center for Telecommunications-Information Sharing and Analysis Center (NCC-ISAC) is a model for joint Government-industry information sharing.

3.1 Cyber Warning Information Network

The NSC recognized the need for an efficient communications mechanism for U.S. watch centers to relay critical, time-sensitive threat and vulnerability information. The NSC proposed the CWIN as a means to facilitate, at the national level, the immediate sharing of critical cyber warning information within Government and, eventually, with industry partners. CWIN also potentially provides a recognized, authoritative medium for information sharing and coordination.

CWIN is designed to provide simultaneous communication among network participants using a reliable and secure voice communications path. It is anticipated that CWIN will

- Provide for multiple levels of participation
- Accommodate the exchange of data and images
- Support security and handling requirements for the exchange of classified and unclassified information
- Accommodate unique information handling caveats as determined by the originating organization
- Be able to expand to accommodate other Government and private sector watch centers
- Be dedicated to the sharing of vital cyber warning information

- Have a significant degree of independence from the public network (PN)
- Include documented operating policies and procedures
- Provide near-real-time communication capabilities with a high survivability index.[2]

The Government's CWIN Working Group is employing a phased approach to develop, implement, and operate the CWIN. Phase I consists of developing and implementing operational procedures over existing network capabilities at seven Government watch centers in five physical locations.[3] The NCS was tasked to determine what capabilities exist at the sites and how to best use them to operate the CWIN. Phase I will use secure modes of communication and develop trust among the seven watch centers. Phase II will deploy a dedicated network to support CWIN operations at the seven watch centers.[4] Phase III will expand the CWIN to include non-Government members; however, specific requirements for accomplishing this effort have not been addressed.[5]

CWIN is viewed primarily as a warning network; however, as the phases are implemented it may evolve into an information sharing network permitting the exchange of both technical and policy information. Administrative documents such as a concept of operations are being developed to codify its use as it evolves. As conceptualized, CWIN provides Government with an architecture to support communications and dissemination of warnings in the event routinely used communications media are unavailable.

Recognizing the commitment the private sector has voluntarily made to ISACs, the CWIN point of interface between Government and industry should be at the ISACs. Relationships among organizations in each ISAC and the processes and mechanisms used to share information should be left to the discretion of the ISAC participants. ISAC participants should also determine how they should develop relationships with other ISACs. However, material support and funding from Government should be considered to help establish relationships between ISACs and with Government.

3.2 National Coordinating Center for Telecommunications-Information Sharing and Analysis Center

Designated as an ISAC in January 2000, the NCC-ISAC jointly represents industry and Government elements of the telecommunications infrastructure. This joint relationship enables Government and industry to work together to collect, analyze, and share information among the telecommunications sector. Specifically, the NCC-ISAC performs the following activities—

- Facilitates voluntary collaboration and information sharing among its participants

[2] CWIN White Paper.

[3] May 30, 2001, National Security Council Memorandum on Implementation of CWIN.

[4] Ibid.

[5] Ibid.

- Gathers information on vulnerabilities, threats, intrusions, and anomalies from the Government, the telecommunications industry, and other sources
- Analyzes the data with the goal of averting or mitigating impact on the telecommunications infrastructure
- Establishes baseline statistics and patterns
- Maintains a library of historical data
- Sanitizes and disseminates results in accordance with sharing agreements established among the participants.[6]

NCC-ISAC participants share information with each other through agreed on procedures and processes. Before sharing information, participants conduct analysis in their respective organizations to determine if information is "significant and valuable." NCS personnel work with participants to analyze and correlate shared information with other sources. Participants also tap into expertise within their organizations and "personal networks" to analyze an event. Sanitized information is distributed per information sharing agreements to NCC-ISAC participants, Government departments and agencies, and other organizations. After receiving information from the NCC-ISAC, participants turn to contacts within their organizations to further distribute the information to appropriate personnel who can take action.

The NCC-ISAC is a function of the NCC, the operational arm of the NCS. As a result, the NCC-ISAC is able to take advantage of NCC and NCS communications resources. The NCC and NCS maintain several emergency communications resources for use when other means of communication are unavailable.

Alerting and Coordination Network

One resource, the Alerting and Coordination Network (ACN), provides participants with a private, switched, alternative network for use in coordinating a resolution in the event of a widespread outage or severe congestion in the PN.[7] Participating network service providers, gateway operators, equipment and software providers, selected Government agencies, and others are able to communicate with one another regarding the nature of the outage and the appropriate actions to take in response.

ACN Architecture

Currently, the ACN utilizes two geographically separated private branch exchange switches. The ACN has the ability to bridge disparate networks. Calls originating on the ACN can be passed to the PN, sent over high frequency radio, or uplinked to satellite. The ACN can also receive calls through these same media. Participants may have access lines to the ACN provisioned as either off premise (line side) exchange circuits, or as tie line (trunk side) connections. Line side exchange connections are limited in that only one location can access/be accessed in the network, whereas tie line connections allow multiple locations to have access/be accessed through the ACN, though only one per tie line at any one time.

[6] NCC-ISAC Concept of Operations, Version 1.0, May 1, 2000.

[7] The ACN evolved out of the divestiture of AT&T and the Modified Final Judgment's requirement that there be an alerting mechanism for the Bell Operating Companies.

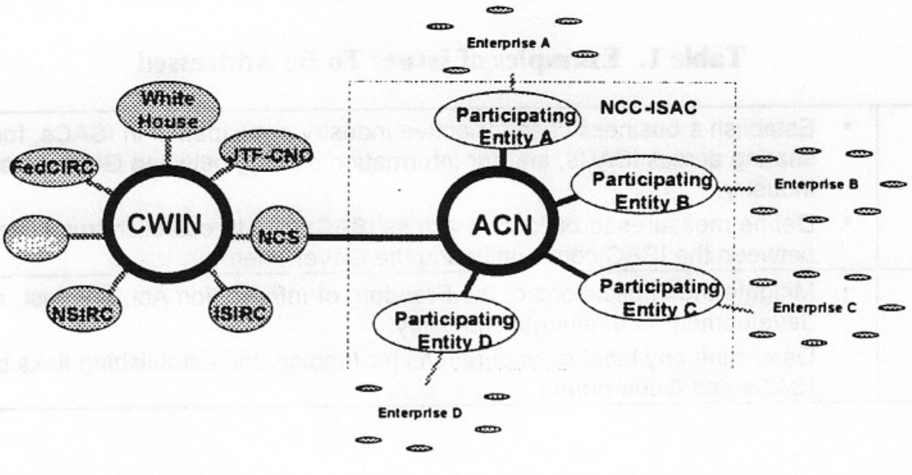
The ACN is designed as a backup capability that when used with other communications media available at the NCC (e.g., high frequency radio) provides a robust coordination capability. The ACN's intra-switch station-to-station dialing ensures it will not be affected by a failure in the Signaling System 7 network or associated databases, and the private-line architecture of the ACN eliminates problems such as delays in getting dial tone, trunk congestion, or call blocking. Because the ACN still rides the nationwide backbone, network equipment failures in the backbone can have limited impact on ACN communications.

In addition to NCC and NCS emergency communications resources, NCC-ISAC participants have internal corporate resources that can be deployed during a cyber crisis. Some participants have "ACN-like" networks deployed within their enterprises to ensure connectivity in the event of an emergency.

Within the proposed CWIN architecture, the NCS is one of the seven Government watch centers to be connected during Phase I. Through the NCC-ISAC, which is collocated with the NCS, Government can interface with the telecommunications infrastructure. This relationship positions the telecommunications industry to be among the first to partner with Government in the context of CWIN. This partnership is a step toward building a national capability for information sharing, analysis, and dissemination.

Figure 1 illustrates how the telecommunications sector and the Government may use emergency communications resources during cyber crises. During a cyber crisis when other communication media may not be available or appropriate, information disseminated by Government within the CWIN architecture can be made available to the telecommunications industry through the NCS. The operational arm of the NCS, the NCC, can use the ACN to provide alert and coordination information to NCC-ISAC participants who have connectivity to the ACN. In addition, enterprises can use internal emergency networks to ensure that information is communicated to individuals within the organization who can take action.

Figure 1. Notional Diagram of Telecommunications Sector Emergency Communications Capability for Information Sharing, Analysis & Dissemination



4.0 FUTURE CONSIDERATIONS FOR BUILDING A NATIONAL INFORMATION SHARING, ANALYSIS, AND DISSEMINATION CAPABILITY

Based on the present understanding of the CWIN architecture, the NSTAC applauds the efforts of the Government to address the need for a national information sharing, analysis, and dissemination capability. Recognizing the role that industry must play in a national capability, the NSTAC encourages Government and industry to consider the following when building a national capability.

The ISACs should be Government's primary means of interface with industry for CIP. ISACs provide information collection and exchange, analysis, and dissemination capabilities for industry and, in the case of the NCC-ISAC, Government and industry. In addition, the ISAC framework allows participants to determine the processes, procedures, and means for communication that is most appropriate to meet their needs. An emergency communications mechanism should be considered for linking the ISACs to each other and to Government.

Infrastructures should be encouraged to consider alternative means for communicating during emergencies as appropriate to the sector. The NCC's ACN, which links the telecommunications industry and provides reliable and survivable communications, is an example of an emergency communications mechanism that has worked for the telecommunications sector. Other infrastructures may realize that this approach meets their needs or they may wish to develop mechanisms tailored to their specific needs. In addition, enterprises should consider building private, internal corporate networks to support information dissemination, warning, and coordination during emergencies.

The NSTAC encourages other sectors to consider developing emergency communications mechanisms and encourages Government to work in partnership with industry to explore appropriate means for linking capabilities between Government and industry. However, building a national capability for information sharing, analysis, and dissemination is a complex undertaking. Before a national capability can become fully operational, a number of issues will need to be examined more closely and resolved. Table 1 provides examples of the types of issues that both industry and Government will need to address individually and in collaboration.

Table 1. Examples of Issues To Be Addressed

Policy	• Establish a business case for active industry participation in ISACs, for information sharing across ISACs, and for information sharing between Government and industry. • Define measures to build trust across ISACs and to establish trusted relationships between the ISAC community and the Government.
Legal	• Mitigate the implications of the Freedom of Information Act, antitrust, and liability for development of a national capability. • Determine any legal considerations for funding and establishing links between the ISACs and Government.

Table 1. Examples of Issues To Be Addressed cont.

Operational	• Integrate analysis at the national level. • Establish procedures to ensure the protection and proper handling of information to be shared (e.g., proprietary information, law enforcement sensitive information, and classified information).
Technical	• Define the technical requirements for linking ISACs together; ISACs to CWIN. • Define the scalability of such networks and the functionalities appropriate for the range of participants.
Financial	• Estimate orders of magnitude cost estimates for linking ISACs together; ISACs to CWIN. • Investigate funding options.

5.0 NSTAC'S INPUT TO THE NATIONAL PLAN

The following text is provided for inclusion in the National Plan. The text addresses an industry-based assessment of national level information sharing, analysis, and dissemination capabilities for addressing cyber attacks.

An Industry-Based Assessment of National Level Information Sharing, Analysis, and Dissemination Capabilities for Addressing Cyber Crises

On a daily basis, the Nation's critical infrastructures face some type of cyber threat. Whether that threat is intentional or unintentional, the actions of insiders, script kiddies, or hackers can affect the networks of infrastructure owners, operators, and users. The private sector owns and operates the Nation's critical infrastructures and is, for the most part, well equipped to deal with "routine" cyber events such as viruses, probes, and scans. Although largely informal, information sharing processes and mechanisms exist to facilitate response and mitigation efforts for these types of routine cyber events.

Coordinated, large-scale cyber events that result in or have the potential to result in a widespread outage[8] or disrupt multiple infrastructures are a national security concern. These events can be referred to as "cyber crises." Cyber crises may target one or more of the following three levels: (1) end users, (2) traffic capacity, and (3) network controls. An event involving one level may affect the other levels. In addition, cyber crises affecting one infrastructure may result in problems in another infrastructure because of the interdependence of the Nation's critical infrastructures. Cyber crises may also transcend national and geographic boundaries.

A national capability to disseminate national warnings and facilitate response and mitigation efforts for these types of events across infrastructures does not exist.

[8] A widespread outage is defined as a sustained interruption of telecommunications service that will have strategic significance to Government, industry, and the general public. Such an outage would likely affect the telecommunications service in at least one region of the country, including at least one major metropolitan area. It would involve multiple carriers, affecting both long distance and local service, and significantly degrade the ability of other essential infrastructures to function. Such an outage would have an impact on the availability and integrity of telecommunications service for at least a significant portion of a business day. *(NSTAC's Widespread Outage Subgroup)*

Key elements of a national capability spanning public and private sectors should include information collection and sharing, information analysis, dissemination of alerts and warnings, and post-event analysis and dissemination.

Information Collection and Sharing

Information collection and sharing consists of owners, operators, and users of infrastructures detecting attacks or anomalies in their networks and then sharing that information with others. Because the set of conditions surrounding each cyber crisis is unique, sources of information will likely be unique as well. Information and data can be obtained from numerous sources, including the Government, the private sector, academia, media, nonprofit organizations, for-profit vendors of security products and services, and individuals. Informal and formal processes and mechanisms exist to facilitate the collection and sharing of information; however, they must be tailored to meet the specific requirements of each event. Because sources of information cannot be identified in advance, a dedicated sharing network will most likely be unsuitable. Information sharing is distributed, ad hoc, and involves multiple subnetworks of relationships. In the context of Presidential Decision Directive (PDD) 63 and national critical infrastructure protection (CIP) policy, Information Sharing and Analysis Centers (ISACs) facilitate the collection and sharing of information from multiple subnetworks within a particular infrastructure. A recognized national-level capability to aggregate information from across the infrastructures will be required to meet CIP objectives.

Information Analysis

Information analysis consists of interpretation and correlation of data to identify problems, solutions, and trends. Analysis turns information from multiple, disparate sources into knowledge. Analytical processes and methods are often ad hoc; they vary depending on the event. Information is analyzed through a collaborative process. Multiple entities and individuals are involved. Because of the changing nature of cyber events, it is not possible to predetermine the set of subject matter experts that will be needed to perform analysis. Building relationships with these individuals when analyzing routine events is critical to ensuring access to them during cyber crises. Analysis occurs at multiple points, beginning with affected organizations within the enterprise, then enterprisewide, and then in an ISAC. Subsequently, collaboration occurs among the enterprises within an ISAC. A national capability, which could be distributed or centralized, will be required to provide analysis of information obtained from multiple ISACs and other sources.

Dissemination of Alerts and Warnings

Dissemination of alerts and warnings consists of distributing analyzed and sanitized information in the form of alerts and warnings to infrastructure owners, operators, and users. Definitions for the terms "alert" and "warning" vary from infrastructure to infrastructure. The distribution of alerts and warnings must be controlled carefully because recipients, who vary depending on the event, want information that is timely, actionable, and issued with authority. Established processes within and across infrastructures are needed for disseminating warnings and coordinating action to ensure that infrastructure owners, operators, and users respond appropriately. Within an infrastructure, ISAC participants may agree to authorize the ISAC to issue an alert or warning to ISAC participants. A recognized, authoritative national-level source for issuing national cross-infrastructure alerts and warnings on behalf of the entire Nation's welfare will be required to meet CIP objectives and inform subnetworks within and across infrastructures of cyber crises.

Post-Event Analysis and Dissemination

Post-event analysis and dissemination consists of preparing and distributing "after-action reports" that provide an analysis of the event, its consequences, and lessons learned. Post-event analysis provides closure to an event by defining actions taken and outlining agreed on protection measures for mitigating or preventing further activity. Although the dissemination of "after-action reports" should be encouraged, reports should minimally discuss specific details of the event so as to dissuade further exploits. For participants, the ISAC framework facilitates the development and dissemination of post-event analysis. A national capability to provide post-event analysis and dissemination will be required to coordinate cross-infrastructure sharing of lessons learned.

In summary, a national capability should consider the following basic design principles:

- Be primarily concerned with cyber crises, not routine cyber events,
- Include key entities from all of the critical infrastructures,
- Leverage public-private partnerships involving Government, non-Government organizations, and corporations,
- Include international partners,
- Aggregate information from across the infrastructures,
- Provide analysis of information obtained from multiple ISACs and other sources,
- Provide an authoritative source for coordinating national alerts and warnings within and across infrastructures, and
- Provide post-event analysis and dissemination to coordinate cross-infrastructure sharing of lessons learned.

Conceptualizing the architecture for a national capability for addressing cyber crises is a complex undertaking; however, recognizing that the private sector owns, operates, and uses the Nation's infrastructures, ISACs should be considered as Government's primary means of interface with industry for CIP. Private enterprises in each of the infrastructures have focused their resources and CIP efforts on ISACs specific to their infrastructure. ISACs provide the private sector with a framework for interfacing with each other, and in some cases (e.g., the telecommunications ISAC), with Government. In addition, ISACs facilitate information collection and sharing, information analysis, dissemination of alerts and warnings, and post-event analysis and dissemination in the manner agreed on by participants of the ISAC. The ISAC framework allows participants to determine the processes, procedures, and means for communication that is most appropriate to meet their needs. Efforts in this area should be leveraged when building a national capability. Capabilities that are developed in an ad hoc manner or that bypass ISACs may result in confusion and compromise the authority required by a national capability.

The architecture for a national capability should also support communications when other communications media are not available. Processes and procedures for use of the architecture should be available and employed on a regular basis to ensure convenience and sustain readiness. In addition, development of communications mechanisms to link the ISACs to each other and to Government should be considered.

Government is sponsoring development of the Cyber Warning Information Network (CWIN), an initiative designed initially to provide Government with a reliable capability for disseminating warnings and potentially facilitating information sharing and coordination. Recognizing the commitment the private sector has voluntarily made to ISACs, the CWIN point of interface between Government and industry should be at the ISACs.

Infrastructures should also be encouraged to consider alternative means for communicating during emergencies as appropriate to the sector. For example, the telecommunications industry developed an alerting and coordination mechanism, which connects key elements of the sector and provides reliable and survivable communications in the event other communications media are unavailable or requirements warrant its use. Individual enterprises also have internal private networks that support coordination during emergencies when other communications media are unavailable. Enterprises across the infrastructures should consider building private corporate networks for information dissemination, warning, and coordination, as appropriate to meet their needs.

Building a national capability for information sharing, analysis, and dissemination is a complex undertaking. Before a national capability can become fully operational, numerous policy, legal, financial, operational, and technical issues must be addressed by Government and industry individually and in collaboration. Government and industry should continue to work in partnership to explore appropriate means for linking information sharing, analysis, and dissemination capabilities between Government and industry.