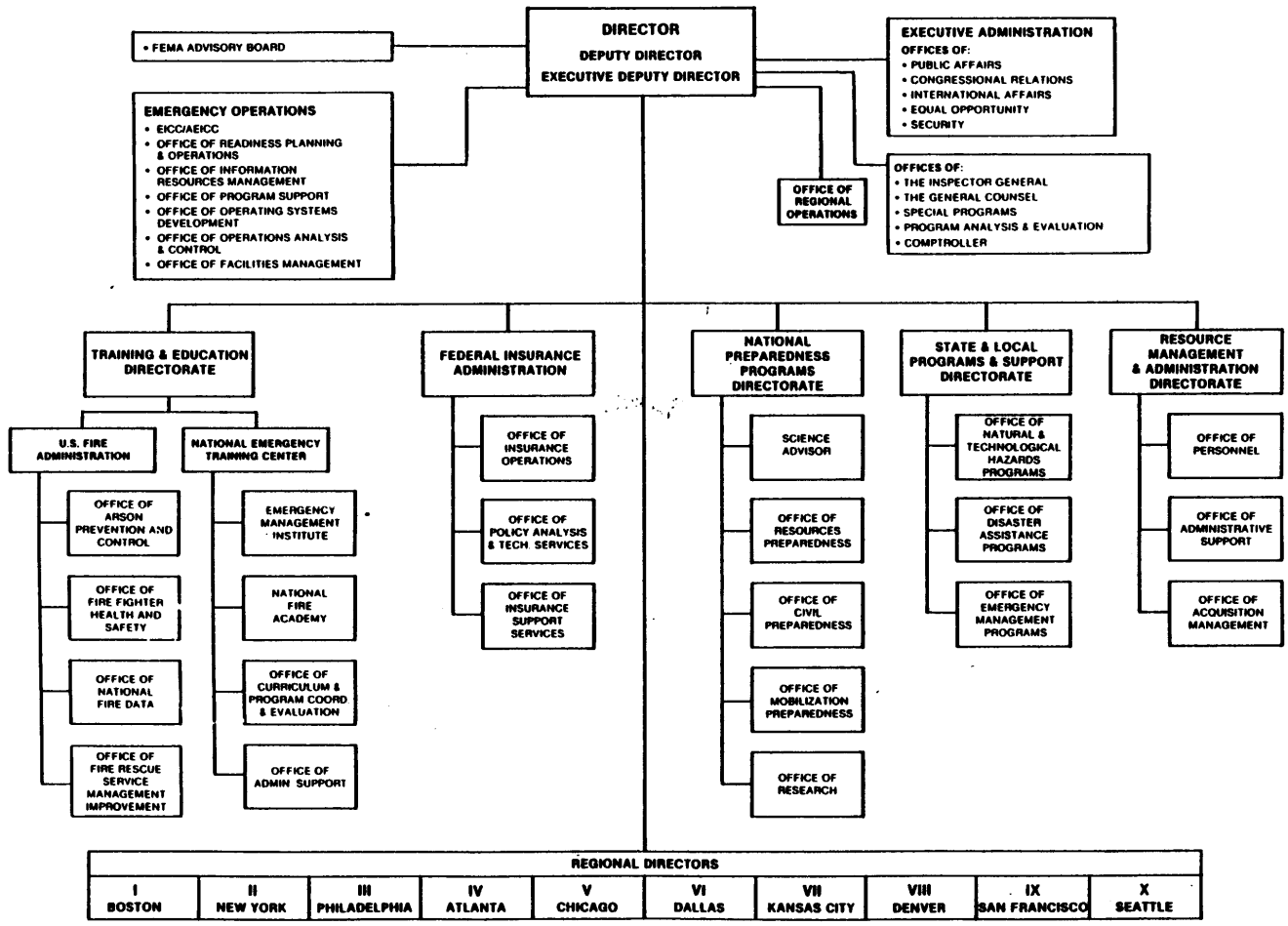
STAT

Next 2 Page(s) In Document Denied

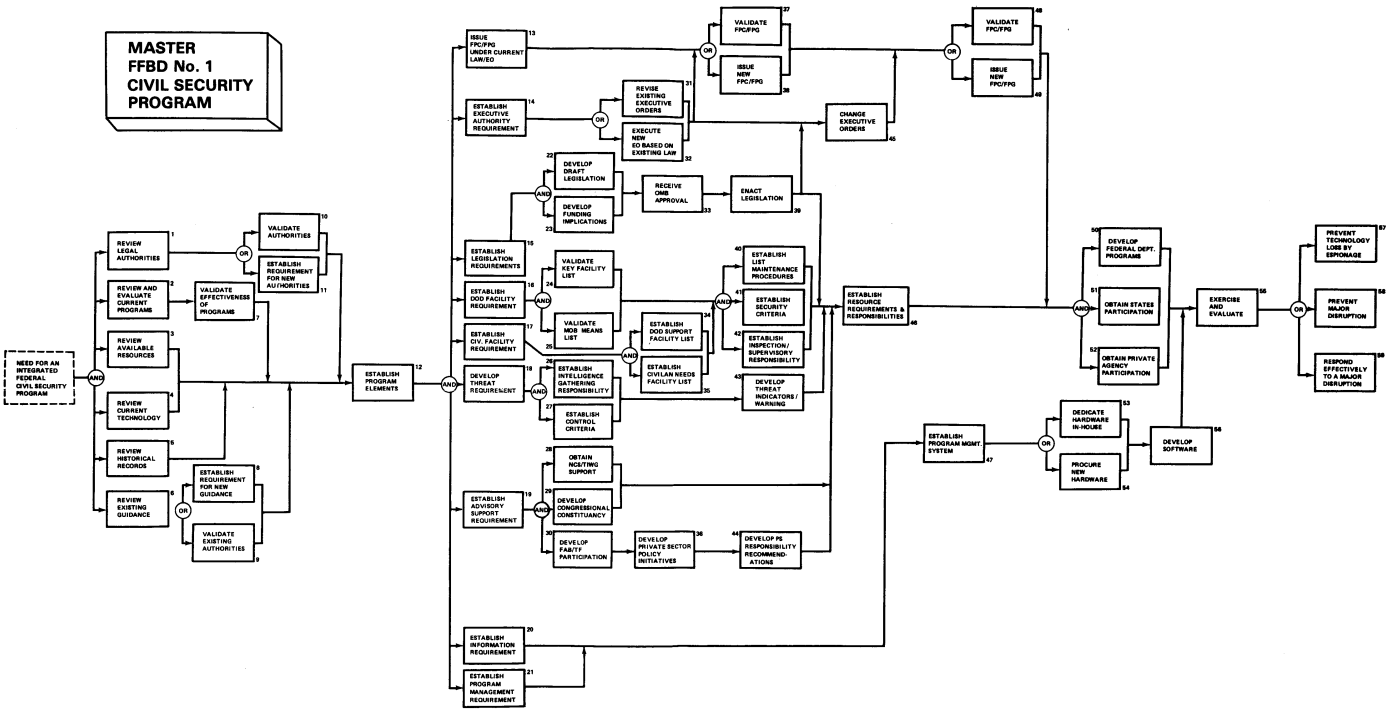
new

ORGANIZATION

FEDERAL EMERGENCY MANAGEMENT AGENCY



Approved: DIRECTOR
7 January 83



FEMA Civil Security Functions and Information Requirements

March 1983

FEMA Civil Security Functions and Information Requirements

March 1983

This document was prepared by the MITRE Corporation for the Federal Emergency Management Agency, Civil Security Division under contract EMW-C-1035.

Declassified in Part - Sanitized Copy Approved for Release 2011/12/09 : CIA-RDP89B01330R000600870001-6

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIST OF TABLES

LIST OF TABLES
(Concluded)

EXECUTIVE SUMMARY

The Federal Emergency Management Agency (FEMA) is the focal point within the federal government for dealing with a wide spectrum of emergencies affecting the United States in peace and war. It has a central role in both domestic and national security emergencies ranging from natural and technological disasters through nuclear attack. One of its mission areas falling midway on the emergency spectrum is civil security. The organizational element of FEMA principally involved is the Civil Security Division of the Office of Mobilization Preparedness under the National Preparedness Programs Directorate. A growing awareness of the functional dimensions and operational complexity of the mission made it increasingly apparent that existing information handling arrangements were inadequate, and that significant improvements were necessary if all of the diverse responsibilities of civil security were to be fulfilled. Accordingly, as part of a larger task to assist FEMA in developing an overall National Emergency Management System (NEMS), The MITRE Corporation was requested to give priority attention to a component sub-system of NEMS that would provide data and information management support expressly for civil security. The present report documents the results of this initial effort.

Purpose and Approach

The basic task objective is to identify and define the information requirements of the FEMA civil security mission. In order to reach that objective, specific answers are sought for the following questions:

- What are FEMA's responsibilities with respect to civil security?
- What functions are performed to discharge those responsibilities?
- What information is required to support each of the functions?
- What are the associated parameters and constraints of the needed information?

The analytically derived findings that answer these questions in detail are contained in the body of the report. Salient highlights are summarized below.

FEMA Civil Security Responsibilities

The scope of FEMA's civil security mission is broad. It covers a variety of measures to reduce the risks and potential consequences of disruption caused by deliberate acts of terrorism, civil disorder, sabotage, and subversion. This includes responsibilities for mitigation, preparedness, response, and recovery - and the coordination of related activities among other federal agencies, the States and local governments, and numerous private sector organizations. The mission is cast in a comprehensive time frame: pre-event, trans-event, and post-event. And it is concerned with the entire span of vital national resource systems, such as, electric power, telecommunications, transportation, food and water, governance, and public health.

FEMA Civil Security Functions

FEMA's civil security functions can be divided into three broad time phases: (1) pre-event preparedness; (2) trans-event response; and (3) post-event recovery. A total of 26 essential functions has been identified throughout all three periods. By far the largest number, amounting to 13, is found in the pre-event preparedness phase. These are on-going functions performed on a continuing basis under normal conditions. They include all those activities of a prudential nature undertaken in anticipation of any civil security incident prior to its occurrence. They are projected toward the future, with the aim of enhancing prevention, mitigation, preparations for, response to, and recovery from such incidents should they materialize. These pre-event functions mainly address: threats and risks; policy, plans, and programs; coordination and liaison; legislative and interagency matters; and training and exercises.

Trans-event response functions focus on the actual emergency at hand, and are therefore largely extempore, unique to a particular event, and of relatively short duration. Depending on scenario circumstances, most are temporary, and some might be concurrent, truncated, or omitted entirely. Direct participation by civil security staff personnel may be brief, confined only to the early stage until the FEMA response management principals can take over. Among the eight functions identified for this time phase, the major ones are: warning notification; providing various forms of decision support, including monitoring and assessment; decision implementation and interim operational coordination; plus initiating execution planning, mobilization, and readiness for recovery.

The fewest number of civil security functions occur in the post-event recovery phase. They are oriented to ancillary

support of those FEMA elements having primary responsibility for recovery management. Of the five functions identified, the most notable are: staff expertise and advice on residual threats and risks; special liaison regarding civil security; and drawing lessons learned from the emergency experience.

Information Requirements to Support Civil Security Functions

The foregoing civil security functions were then subjected to further analysis to determine the kind and extent of information required in order to perform them. The results of this analysis reveal that a total of approximately 145 major categories of information is needed for all of the functions: some 83 types are essential for the pre-event preparedness functions; 40 types during the trans-event phase; and 21 in the post-event recovery phase. Most of these information requirements, moreover, are cast in generic terms, each category embracing a considerable breadth and depth of substantive content. Much of that information, by its nature, has to be obtained piecemeal or in increments from many different sources, and then must be aggregated syncretically before it can be utilized. Clearly, the volume and variety of information demands posed by the civil security functions imply a correspondingly sizeable and complex systems capability to acquire, process, and exchange the large quantities of data involved.

Information Parameters and Constraints

Finally, the functional information needs were examined at the next level of detail and characterized in operational terms. Each requirement item was analyzed according to the following attributes: source, security classification, frequency, accessibility, and application. It was found in the majority of instances that multiple sources must furnish the information; sometimes ten or more contributing agencies are involved. Security classification, even within a given information category, tends to run the gamut from unclassified through top secret, and often beyond into the compartmented levels. Frequency of need for information, and of its updating, ranges from hourly or daily to quarterly and annually, with many of the entries indeterminate because of scenario dependency.

In general, those requirements pertaining to pre-event functions permit a more structured flow of information. There is usually less urgency and longer intervals between updates. During an actual civil security incident, however, the information processes are likely to change dramatically. In such a

trans-event phase, the need and currency are dictated by situational imperatives that are innerently unpredictable -- varying with the nature, scale, and pace of the emergency as it unfolds. For certain types of information, the desired frequency, on both counts, then approaches real time. In the post-event recovery phase, the time-sensitivity of some informaton, though diminished, nevertheless remains relatively acute. Here again, frequency depends on the circumstances surrounding the recovery situation itself.

FEMA's access to the different types of information may be routine, limited, or on an ad hoc basis, that is, only case by case upon request. Overwhelmingly, throughout all three phases, accessibility of most categories should be routine, while roughly a fifth would be limited in one way or another, and about 10 per cent ad hoc. The last parameter was the application of the required information when received, defined in terms of whether it is used by and within FEMA or becomes part of an output product. Some of the information types fall into both classes. For all functions and information requirements, the ratio between internal and output applications is found to be on the order of three to one. These output products, however, are disproportionately critical, for they embody and articulate FEMA's civil security management role in practice.

1. INTRODUCTION

At the time of its establishment, in 1979, the Federal Emergency Management Agency (FEMA) was assigned responsibility for an "all hazards" approach to disaster mitigation, preparedness, response, and recovery in the United States. In carrying out this mandate, the Agency tries to provide the vital ingredients for comprehensive emergency management--spanning the full spectrum from local disasters to nuclear war and extending through all levels of government and the private sector.

One of the vital ingredients in comprehensive emergency management is the development of information systems designed to satisfy both the mission requirements of FEMA as a whole and those of its separate components. The basic goal that FEMA has set for itself is the establishment of a National Emergency Management System (NEMS) and its correlative integrated information systems architecture. In its efforts to achieve this goal, the FEMA management has requested the assistance of The MITRE Corporation, an organization that has specialized in the development and utilization of advanced information systems. As a part of this larger task, MITRE was asked to concentrate initial attention on one of FEMA's component missions--the preparation for and response to major civil security threats and incidents. The present report records the results of this initial study.

1.1 Purpose and Objectives

The basic purpose of this study is to review the FEMA civil security mission requirements and to identify the data and information needed to fulfill these requirements. More specifically, the study is aimed at the following four questions:

- What are FEMA's responsibilities with respect to civil security?
- What functions are performed to discharge those responsibilities?
- What information is required to support these civil security functions?
- What are the associated parameters and constraints of the information?

The answers to these questions are documented in this report. Its contents present the substantive findings and recommendations resulting from the study effort, and the product constitutes the "Requirements Book" called for in the sponsor's statement of work.

1.2. Scope

The Scope of the FEMA Civil Security Mission is quite broad, covering efforts to reduce the consequences of major acts of terrorism, civil disorder, sabotage, and subversion. It includes actions aimed at mitigation, preparedness, response, and recovery--and the coordination of these actions among Federal, State, and local governments and numerous organizations in the private sector of society. It deals with these actions in a comprehensive time frame: pre-event, trans-event, and post-event. And it is concerned with protection of the entire range of national resource systems--including all the lifeline systems (electric power, telecommunications, and transportation, as well as water, petroleum, natural gas, and waste disposal pipelines) and food, raw materials, industrial production, finance, public health, governance, and people (civil society). These various dimensions are taken into account in the subsequent analysis of the information functions, needs, and resources essential for the fulfillment of the FEMA civil security mission.

1.3 Approach

The key members of the MITRE staff assigned to this project have had extensive previous contacts with FEMA and its predecessor agencies and have drawn on this background of experience in formulating and conducting the present analysis. This previous experience provided basic knowledge of the structure and functions of FEMA. This basic knowledge was augmented and refined in a series of interviews with staff members of the Civil Security Division and other relevant FEMA components. These initial fact gathering interviews, in turn, were supplemented by reinterviews wherein the "straw man" briefing technique was utilized to test the applicability, relevance, and usefulness of the central ideas developed for this study. This involved the presentation of the conceptual framework and central ideas to key FEMA staff members and--based on several interactive iterations--the progressive refinement and elaboration of this conceptual framework and body of ideas. These data were further supplemented by an extensive and detailed review of numerous documents pertaining to FEMA as a whole and to the responsibilities and mission of the Civil Security Division.

1.4 Report Organization

The subsequent chapters of this report are devoted to a detailed presentation of the analyses dealing with the FEMA civil security mission requirements and the corresponding data and information management needs. Chapter 2 begins the analysis with a review of the FEMA civil security mission and with the notation that this analysis has broad applicability for other FEMA mission areas. Chapter 3 presents an analysis of

FEMA civil security functions in relation to pre-event preparedness, trans-event response, and post-event recovery phases. Chapter 4 details the types of information needed to support FEMA civil security functions during each of these three time phases. Finally, Chapter 5 deals with various attributes of the needed information in terms of source, security classification, frequency of need and update, accessiblity, and application.

Beginning in Chapter 3, the reader will note that an internal coding scheme has been incorporated into the text, figures, and tables. The contents of this report were reproduced, at the request of the sponsor, on a Wang word processor Diskette as an added product of the research effort. The code is based on an alpha-numeric key designed to facilitate machine access and retrieval of the substantive findings according to any preselected combination of system features and their related information properties. A detailed explanation of the key is presented below.

The first element of the code is a letter designating the respective time phase, as follows: "P", for Post-event Preparedness; "T", for Trans-event Response; and "R", for Post-event Recovery. The next element is an ordinal number corresponding to one of the discrete civil security functions performed within a given phase; thus P.5 refers to the fifth pre-event function. The third character is a letter indicating the particular information requirement associated with a specific function; thus T.4.B represents the second information requirement for the fourth trans-event function. The final element is a number in parentheses denoting one of the five parameters relating to a particular functional information

requirement. An example drawn from the report that illustrates the full code would be R.2.C.(4), which translates into: R, the "Post-event Recovery Phase"; 2, the function cited is "Assess Continuing or Follow-on Threat:, C, the information requirement specified for that function is "Projected Risk Analysis Estimates"; and (4) the parameter of the required information pertains to "Accessibility".

2. FEMA CIVIL SECURITY MISSION

2.1 Background

Prior to the formation of the Federal Emergency Management Agency, there was no mechanism for coordinating all civil security emergency planning, management, mitigation, and assistance fuctions of the Federal Establishment. On August 25, 1977, President Carter authorized a reorganization study of Federal emergency preparedness and response programs. A special task force of the President's Reorganization Project was established to review the then-current status of those programs and to recommend appro- priate organizational remedies.

One on the principal foci of attention in this task force was the wave of hijackings, kidnappings, bombings, and assassinations around the globe that seemed to signal an increase in the frequency and violence of terrorism and other civil disorders. The final summary report of the President's Task Force on Federal Emergency Preparedness and Response recommended a comprehensive reorganization by consolidating existing agencies and additional responsibilities into a single, independent Executive Agency accountable to the President and to Congress for all Federal mitigation, preparedness, and response activities. Among the specific recommendations was one dealing with the Federal response to the consequences of terrorist incidents:

> Experts on terrorism charge that Federal organization for dealing with terrorist incidents is insufficiently comprehensive. Specifically, they express concern over the lack of a focal point for coordination of the Federal response to meet such potential consequences of terrorist action as significant resource disruptions and physical damage.

> The Project finds that such a focal point is lacking, and recommends that responsibility to coordinate vulnerability analysis and preparedness measures to mitigate the consequences of terrorism should be assigned to the new agency. (Task Force on Federal Emergency Preparedness and Response, President's Reorganization Project, Summary Report. Washington, D.C.: Executive Office of the President, June 19, 1978.)

The consolidation of existing emergency preparedness and response agencies into a single new agency called the Federal Emergency Management Agency was accomplished by Reorganization Plan No. 3, submitted to the Congress by President Carter on June 19, 1978. In his transmittal message, the President also noted that responsibility for the Federal response to the consequences of terrorist incidents--a new function not then assigned to any specific agency--would subsequently be assigned to the new Agency. That assignment was made in Executive Order 12148, which charged FEMA with responsibility for "the coordination of preparedness and planning to reduce the consequences of major terrorist incidents". That same Executive Order gave FEMA much broader authority for handling emergencies than existed in its predecessor agencies. The "all hazards" mission of FEMA is clearly stated in the following sections of that Executive Order:

> 2-101. The Director of FEMA shall establish Federal policies for, and coordinate, all civil defense and civil emergency planning, management, mitigation, and assistance functions of Executive agencies.
>
> 2-102. The Director shall periodically review and evaluate the civil defense and civil emergency functions of the Executive agencies. In order to improve the efficiency and effectiveness of those functions, the Director shall recommend to the President alternative methods of providing Federal planning, management, mitigation, and assistance.

> 2-203. For purposes of this Order, "civil emergency" means any accidental, natural, man-caused, or wartime emergency or threat thereof, which causes or may cause substantial injury or harm to the population or substantial damage to or loss of property. (Executive Order 12148, July 20, 1979.)

Additional authority on the subject of civil security was given to FEMA in two other Executive Orders. Executive Order 10421 provides for the physical security of facilities important to the national defense to include "security against sabotage, espionage, and other hostile activity and other destructive acts and omissions" not attributable to military defense or combat or to the dispersal and post-attack rehabilitation of facilities. The Director of FEMA is given broad authority to prescribe policies and programs governing activities of Federal agencies; developing and promulgating standards; assigning facilities to Federal agencies; approving or revising security ratings established by the Department of Commerce; reviewing physical security programs of Federal agencies; and keeping the President informed about the physical security of the facilities and furnishing him with appropriate recommendations.

Executive Order 11490 consolidates the assignment of emergency preparedness functions to various Federal departments and agencies. The Director of FEMA is assigned responsibility for determining national preparedness goals and policies for the performance of emergency preparedness functions by Federal departments and agencies and in coordinating their performance with the total national preparedness program. FEMA also is directed to provide guidance to Federal departments and

agencies and to evaluate their emergency planning and preparedness activities.*

2.2 FEMA Civil Security Division Roles and Responsibilities

Following the establishment of FEMA, these various authorities and responsibilities were delegated to the Civil Security Division, located in the National Preparedness Programs Directorate's Office of Mobilization Preparedness. The basic mission of the Civil Security Division is to coordinate the Federal Government's preparations for and response to civil security threats and incidents. This includes responsibilities for transforming national objectives and federal policy into planning guidance for the Federal Government's activities aimed at avoiding or mitigating the consequences of acts of terrorism, civil disorder, sabotage, and subversion. This involves requesting and receiving threat estimates; evaluating their impact on civil security programs; coordinating the production of vulnerability and consequence estimates for the various threats; reviewing and coordinating the civil security planning development of the executive agencies; and performing periodic appraisals of the government's civil security readiness posture.

The major generic functions of the Civil Security Division--officially recognized by FEMA--include the following:

- o Conceptualizes and develops policy options for the Director of FEMA on the activities required to avoid

*For other, more basic, authority on the civil security mission, see Pompan and Murray, A Practice Guide to the Legal Authorities for Reducing Widescale Consequences of Incidents Caused by Deliberate Manmade Acts, Washington, D.C. 1983.

or mitigate consequences resulting from acts of terrorism, civil disorder, sabotage, and subversion.

- Prepares and promulgates Federal planning guidance to implement the approved policy.

- Reviews existing authorities for civil security programs and recommends changes or new authorities, as appropriate.

- Develops civil security programs and reviews Federal, State, and local government and private sector plans to avoid or mitigate the consequences of civil security incidents.

- Coordinates the development of vulnerability and consequence estimates for each of the national resource systems (energy, transportation, food, etc.). Ensures that appropriate threat information is received and acted upon by other responsibile agencies.

- Funds research relating to the mission and functions of the Civil Security Division. Develops procedures to ensure the exchange of civil security information between scientific and technical groups and Federal, State, and local agencies.

- Recommends procedures for reviewing, evaluating, and improving the Federal Government's civil security preparedness. Prepares reports on the efficiency and effectiveness of the Federal civil security program for inclusion in the Director's annual report to the President.

- Develops the "lessons learned" from incidents and exercises, and coordinates recommendations for necessary changes in policies and programs.

- In coordination with the Information Resources Management Office, develops a management information system that will effectively support civil security objectives.

- Represents the Federal Emergency Management Agency in meetings where civil security issues are discussed.

- Participates with other FEMA components and other Federal agencies in the design and conduct of exercises to test emergency procedures and plans for dealing with civil security incidents.

- Develops coordination procedures between Federal, State, and local governments and the private sector for the exchange of civil security information.

2.3 Civil Security Information Management as a Microcosm

These and other specific functions of the Civil Security Division are subjected to detailed analysis in the following chapter. Before turning to that analysis, however, it should be noted that the civil security functions of FEMA comprise only one segment of the total FEMA information management system. The analysis that follows focuses attention exclusively on the civil security domain but should be viewed in a wider context of the information support mechanism needed for the conduct of all FEMA emergency management activities. Figure 2.1 depicts the overall National Emergency Management System (NEMS) and the civil security mission within that system. The civil security domain comprises only one segment of the larger NEMS. Despite certain unique features, it can serve as a microcosm of similar information management requirements characterizing other FEMA mission areas. As a microcosm of the larger system, civil security shares the following characteristics with most of the other mission areas:

- The actors involved in emergency mitigation, preparedness, response, and recovery plans, programs, and operations are numerous and diverse. As shown in Figure 2.1, they include the President and the White House Staff, other Federal Agencies, the FEMA regions, the States and local jurisdictions, and many agencies in the private sector.

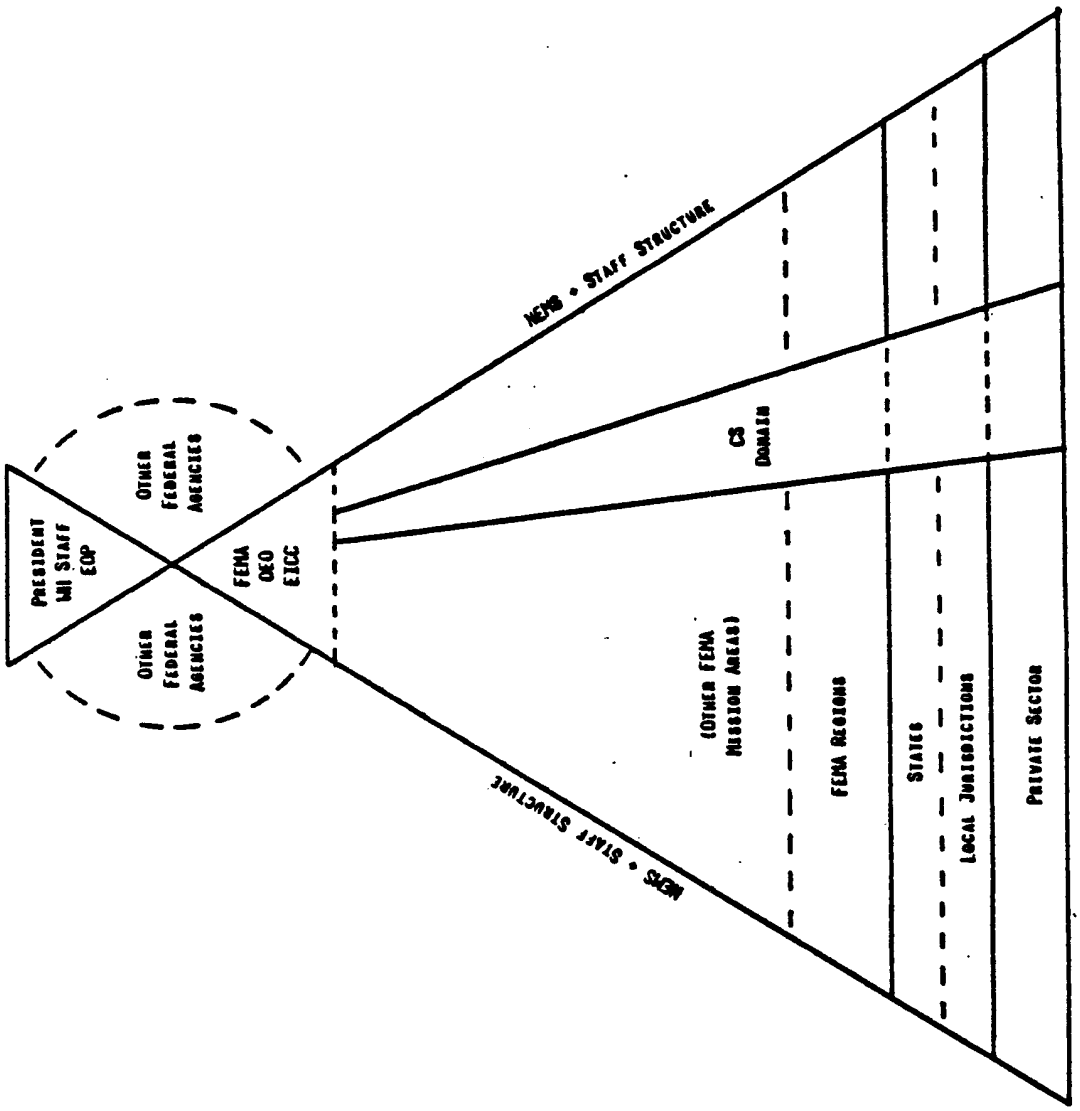


FIGURE 2.1

CIVIL SECURITY SEGMENT OF FEMA INFORMATION SUPPORT MECHANISM

- The audiences with whom FEMA must communicate in carrying out its missions are similarly numerous and diverse, both in terms of input and output information.

- The types of information required pertain to functions in all emergency time phases--pre-event mitigation and preparedness; trans-event response; and post-event recovery.

- All activities must be closely coordinated internally and externally--with both governmental and nongovernmental agencies.

- Persons responsible for carrying out mission responsibilities must be prepared to act in both a routine and in an emergency or crisis mode. The sudden shift from routine planning activities to emergency operations places a premium on organizational adaptiveness and flexibility.

- Risk assessments and vulnerability and consequence analyses are essential in structuring mission activities and in determining key informational requirements.

- The national resource systems of civil security concern (see Figure 2.2) are also of concern to all other mission areas. They cover the gamut of elements essential for societal survival and continuity and thus require continuing attention and protection.

- Education and training programs, the conduct of tests and exercises, and the continuing critical evaluation of actual emergency operations are essential for achieving the requisite coordination of effort among relevant agencies and for developing an enhanced state of readiness.

In the light of these similarities, the subsequent detailed analysis of the information needed for handling civil security functions can be viewed as a prototype for studying other FEMA mission areas and for developing the overall architecture of the FEMA National Emergency Management System.

PETROLEUM/NATURAL GAS

ELECTRIC POWER

TELECOMMUNICATIONS

TRANSPORTATION

WATER (POTABLE, INDUSTRIAL, AGRICULTURAL)

FOOD (GROWING, PROCESSING, DISTRIBUTION)

WASTE DISPOSAL

INDUSTRIAL PRODUCTION

RAW MATERIALS/STRATEGIC STOCKPILE

FINANCE

PUBLIC HEALTH

GOVERNANCE

SOCIETAL PROCESSES

FIGURE 2.2

NATIONAL RESOURCE SYSTEMS OF CIVIL SECURITY CONCERN

Declassified in Part - Sanitized Copy Approved for Release 2011/12/09 : CIA-RDP89B01330R000600870001-6

3. ANALYSIS OF FEMA CIVIL SECURITY FUNCTIONS

Inherent in the broad scope of the civil security mission is a wide variety of roles played by FEMA. Most of these roles are of complex dimensions, some with many ramifications. The following analysis, identifying the different kinds of component activities that must be carried out, reveals the range of discrete functions essential to accomplishing one or another aspect of the overall mission. Not every function, by any means, is actually executed by the Civil Security Division alone. Many are performed by or with substantial assistance from other FEMA staff elements, or by other Federal agencies or even the States and local jurisdictions. The role of the Civil Security Division is one of initiation, coordination, oversight, and general orchestration, to ensure that all of the functions are in fact fulfilled.

3.1 Functional Overview

A salient feature of the civil security mission is the sheer number of functions involved. Depicted schematically in Figure 3.1 is a macro-view showing the total functional universe of FEMA civil security. It is intended to be comprehensive and embraces the full spectrum of major functions to be performed throughout the successive stages of the entire management process relating to the civil security mission area.

The functions displayed are arranged in successive groups from left to right along the horizontal axis according to three time frames. Those appearing in the first, or pre-event preparedness phase, are generic functions performed on a continuing basis under conditions of normalcy. They are of a contingency nature and include all conceivable preparatory measures that

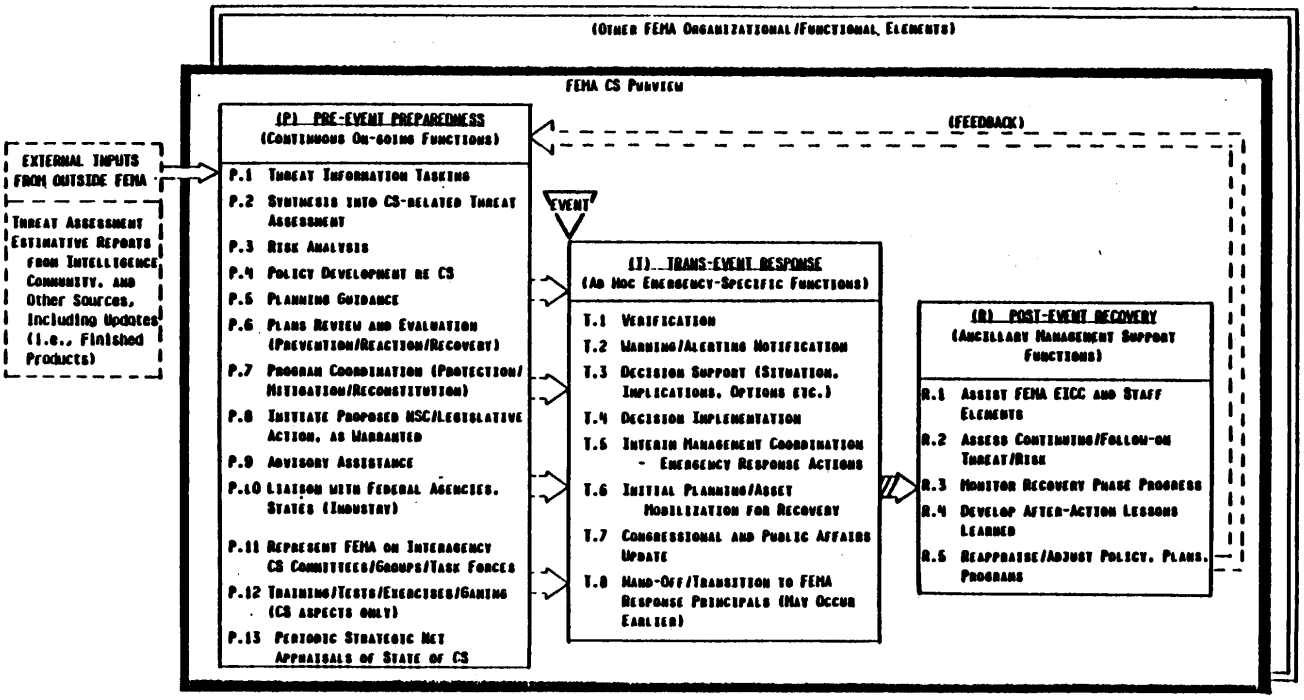


FIGURE 3.1

FUNCTIONAL CONCEPT FEMA CIVIL SECURITY MISSION
(Emergencies Resulting from Terrorism, Civil Disorder, Sabotage, Subversion)

might be taken in anticipation of any civil security incident prior to its occurrence. Those grouped in the second time frame, the trans-event response phase, are the ad hoc emergency-specific functions performed in real time when such an incident actually happens. Triggered by the event itself, they are acute, usually compressed in time, and, depending on scenario circumstances then prevailing, may be of relatively short duration before giving way and melding into the functions of the next phase. This last set, associated with the post-event time frame, marks an indefinite period. It represents those ancillary civil security functions attending the restoration and clean-up operations to recover from the consequences of an incident. The basic dynamics of this three-stage process can be viewed as a single grand cycle closing upon itself, one where the last function links again with the very first.

Within each time frame, the functions are also arrayed generally in descending order along the vertical axis. The sequence, however, reflects logical relationships as much as chronology. There is considerable overlap among them. Some of the functions are performed concurrently, while many others generate feedback affecting preceding ones. Together they form a coherent continuum that unfolds more or less incrementally as shown. This, however, may not always be the case. Under some conditions, the sequence of functions may be compressed, truncated, or inverted. Discussion of the individual functions themselves will be deferred to subsequent sections immediately following. There, each function is described in detail for all three time phases in turn.

As shown in Figure 3.1, there is an obvious time-skewed pattern to the functional distribution. Overwhelmingly the greatest number of functions take place during the first, or pre-event

preparedness phase. The number diminishes markedly in the second, or trans-event phase. By far the least are found in the final, or post-event phase. The explanation for the decrease is that once such an emergency has materialized there are few civil security-unique functions remaining. On a majority of occasions the response and recovery demands confronting FEMA are likely to be little different from those posed by similar disruptions irrespective of cause. The consequences of a critical bridge collapsing, for example, are fundamentally the same whether the result of terrorist demolition, natural disaster, or accident. Most management functions, therefore, would devolve upon appropriate elements of FEMA normally responsible for recovery activities in the aftermath of any emergency situation. Civil security considerations then become peripheral compared to the main task of recovery itself.

3.2 Pre-event Preparedness Functions (P)

The pre-event phase is a continuous on-going process that includes all of FEMA's management activities addressed to future civil security contingencies. The object is to enhance prevention, mitigation, preparation for, response to, and recovery from such incidents before they occur. Figure 3.2 identifies the specific types of functions involved. Each is described in further detail in the sections below.

3.2.1 Tasking the Providers of Threat Assessments (P.1)

The process begins with threat. FEMA is not in the intelligence business, but is a user of finished threat assessment products obtained elsewhere. It relies on external inputs from the intelligence community and other sources to acquire the needed assessments, as well as updates and amplification. For

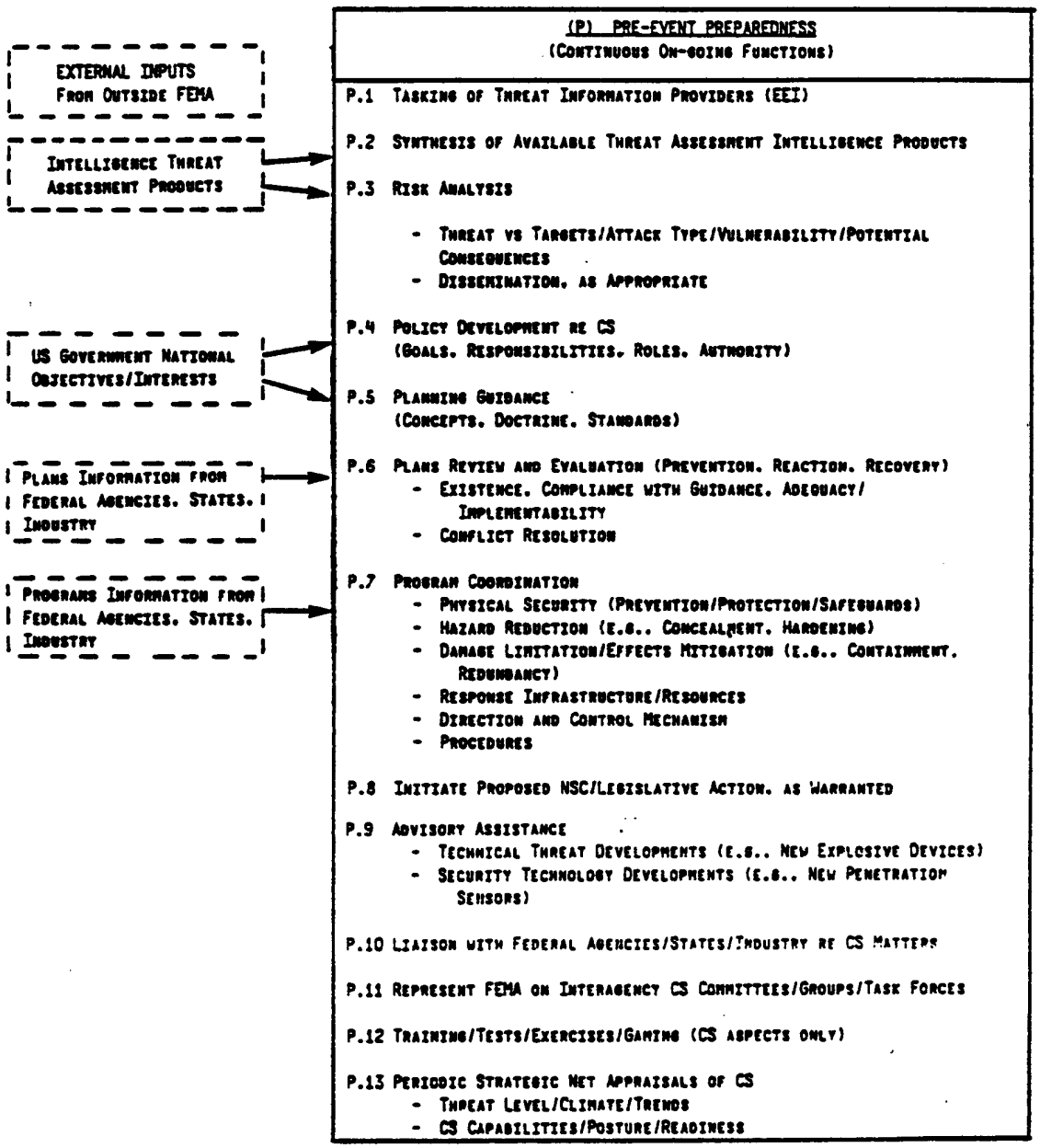


FIGURE 3.2

PRE-EVENT PREPAREDNESS FUNCTIONS

civil security purposes, the threat information derived from sources outside FEMA may be regarded as strategic intelligence. It serves as the premises on which most of the pre-event functions are predicated.

The first function (P.1), accordingly, is the tasking by FEMA of those organizations that are in a position to supply threat assessment information. This presumes that prearranged authority to do so exists. The tasking may be in the form of requests for formal estimative products analagous to a National Intelligence Estimate (NIE), but dealing with civil security threats, or to a Special National Intelligence Estimate (SNIE) focusing on a particular aspect of a given threat. In addition, FEMA might also levy standing requirements cast in a form similar to Essential Elements of Information (EEI) to guide those who acquire threat information. Provisions must also be made for periodic, spot, and by-exception reporting of significant new items bearing on the threats as they develop.

3.2.2 Synthesis of Available Threat Assessment Products (P.2)

The second function is one of aggregation, collation, and integration of the threat assessment information coming from multiple external sources. It has to be organized and interpreted into a master current assessment expressly tailored to the needs and interests of civil security. For a full appreciation of the threat, common patterns must be recognized, trends inferred, and forecasts extrapolated. These second order implications are the driving factors that determine how and where the threat intelligence should be exploited to enhance national civil security. They motivate and shape all aspects of preparedness.

3.2.3 Risk Analysis (P.3)

Based on the threat assessments, the next function is to analyze what they mean insofar as risks posed for national resource systems. All that is known about a given threat has to be matched against the resource systems that it might disrupt. Then, each such combination of threat vs. system must be examined in terms of:

- Types of targets likely to be struck
- Probable attack mode employed
- Vulnerability and susceptibility of those targets to such attack
- Potential consequences expected or possible if the postulated threat action succeeds.

Each of the above dimensions of risk analysis constitute major subfunctions in their own right. Many of them, however, would be performed in large part by others in coordination with the FEMA Civil Security Division.

3.2.4 Policy Development for Civil Security (P.4)

One of the most important functions is formulating national policy with respect to civil security matters. Since the civil security community is so large and pervasive, with many different participating agencies, echelons of jurisdiction, and private sector organizations involved, there is need for a coherent and comprehensive body of U.S. Government policy establishing common national aims and priorities. A concomitant of setting policy goals is allocating roles, missions, and authority governing who is assigned which tasks and objectives, along with defining the responsibilities and prerogatives attendant thereto. The function of FEMA in this regard is to

help initiate, develop, and coordinate such national civil security policy, and once adopted, to promulgate and implement it. The function applies equally to amendment or amplification to existing policy.

3.2.5 Planning Guidance (P-5)

This function is essentially the issuance of strategic direction and terms of reference for the development of civil security plans or annexes to plans. Central management at the national level is necessary to ensure that the resulting family of plans is compatible and the plans reinforce one another. The guidance stems largely from the preceding policy function.

Depending on the agency concerned, the plans to be drawn can pertain to any phase or aspect of civil security operations, from prevention and mitigation, through preparedness, to response and recovery. FEMA, besides levying the requirements for such planning, provides the concepts and premises on which it will be based, outlines the doctrinal principles its substance should reflect, and establishes criteria and standards to be met. Other instructions may also be given, such as identifying critical areas where planning coordination is needed between agencies.

3.2.6 Plans Review and Evaluation (P.6)

Effective preparedness requires quality assurance of civil security plans. A mosaic of separate yet interrelated plans must be produced by the various Federal departments and agencies, by the States and localities, and by private sector organizations. They would differ in content, purview, and application. An important FEMA function, therefore, is to see to it that, individually and collectively,these plans take into

account and adequately provide for every contingency need bearing upon civil security.

The first step is determining whether required plans exist, and if so, their status. They must then be reviewed for compliance with current policy and FEMA guidelines, and be evaluated from the viewpoints of completeness, currency, appropriateness, and feasibility. Missing plans must be developed, and any gaps, problems, or conflicts within or between plans must be reconciled. The function is essential to a sound planning structure, national in scope and accommodating all civil security requirements whatever the action level or scenario circumstance.

The large number of plans involved will undoubtedly require the delegation of a portion of this function. Such delegated review and evaluation, as well as the major planning products that result, would be subject to oversight by FEMA.

3.2.7 Program Coordination (P.7)

The program coordination function is multidimensional and complex. It may be regarded as a set of parallel but separately performed functions. There is virtually an unlimited number and variety of potential programs, or distinct program increments, to contend with, though not all are being actively pursued at present. They can range the gamut of preparatory measures directed toward reducing vulnerability, improving response capability, or lessening the disruptive consequences when an incident occurs. Characteristically, many participants are involved in implementing them. The national focal point for coordinating and managing all such programs is FEMA.

Physical Security is a broad program area containing several major components. It embraces prevention, protection, and safeguards against disruptive acts. The measures and means are designed to deter or preclude successful attack, or to counter and defeat it if attempted. Illustrative examples, either currently underway or projected, are:

- o Emplacement of barriers and perimeter fences
- o Surveillance devices and alarms
- o Patrols
- o Tactical teams to eliminate or neutralize threats

A complementary program area is hazard reduction, such as concealment or hardening of sensitive facilities and critical system elements. An example might be to put emergency operations centers underground, or to install failsafe equipment, such as automatic sprinklers wherever flammable or volatile substances are concentrated. Another closely related program pertains to damage limitation and mitigation of immediate effects stemming directly from an attack. This could be, for example, redundant or backup facilities, modular configuration and dispersed siting of components, or containment features to minimize collateral damage. The latter is extremely important for certain inherently inviting and exposed targets where any initial destructive impact is likely to be escalatory, triggering widespread chain reactions. A case in point is POL tank farms—or storage depots for explosives. These attractive, high-value targets of opportunity, particularly if located within or in proximity to congested urban and industrial centers, call for special program attention on civil security grounds alone. The program could, among other things, encourage construction codes

requiring revetments and levees around such installations, or zoning ordinances to isolate them geographically.

Other programs are oriented mainly to enhancing the civil security infrastructure and its capacity to respond. They provide for better organization and training, upgraded facilities, and acquisition of necessary resources, including personnel, equipment, and supplies. A more general program area of FEMA that has direct utility for civil security purposes is the development of direction and control mechanisms at every response level. This applies particularly to telecommunications and information management systems. An additional response program, though not formally defined as such, emphasizes emergency action procedures, which apply to civil security emergencies in common with other types. There is also currently underway a program covering all aspects of civil security relating to maritime ports. It represents in microcosm the entire civil security mission. Presumably other analagous applications programs will follow.

In sum, program coordination is a constellation of functions, each keyed to its respective program. It may be expected that over time the total agenda of civil security programs under FEMA purview will expand.

3.2.8 Initiate Proposed NSC or Legislative Action (P.8)

As the civil security environment evolves and policies and strategy change, there will be need for new authority, modification or clarification of existing charters, or other basic institutional adjustments regarding the civil security structure and process. At issue might be jurisdictional ambiguity

or statutory constraints impeding FEMA's civil security mission. Initiating, coordinating, and advocating such proposals, whether to be acted upon by the Executive Branch at the White House level or by Congress, is a function of the FEMA civil security staff. It is the Agency's organizational element having the relevant expertise, subject competence, and responsibility. Thus, in conjunction with the legal counsel, it would, formulate, develop, and coordinate any proposed executive orders, directives, or laws affecting its sphere. This includes preparing the supporting rationale and testimony to justify the proposed action before the National Security Council or Congressional committees. By extension, the function also includes similar staffing vis-a-vis regulatory boards and commissions.

3.2.9 Advisory Assistance (P.9)

Advising the civil security community is a general function. Advice might be requested or volunteered, and could cover a wide range of topics. One specific area would be technology. FEMA is in a unique position to serve as the central clearinghouse for maintaining and exchanging technical information regarding civil security. As part of its responsibilities in this mission area, it could advise all parties concerned on current and emerging technical developments with respect to threat capabilities, such as new explosive devices and toxic agents or sophisticated new skills and techniques employed in perpetrating terrorist acts or sabotage. On the other hand, it could also advise on developments in technology designed to thwart threats, such as new penetration sensors and surveillance devices or new methods of fire suppression and bomb disposal. In addition, advice might also be provided on new vulnerabilities being incurred in national resource systems

because of technological advances, such as the introduction of sensitive and critical control equipment.

None of the above excludes other, more basic kinds of advisory assistance. This could be in the form of recommended organizational and procedural solutions for dealing with local problems or special circumstances.

3.2.10 Liaison with Federal Agencies, States, and Private Sector Organizations (P.10)

The liaison function is essential for establishing and maintaining rapport with the civil security community at large. The purpose and scope are broad and flexible, rather than circumscribed. It is performed through informal dialogue directly between the FEMA civil security staff and counterpart elements of key agencies and, at times, selectively with state officials and with certain private sector organizations having a major role in the national resource systems. The mutual exchange of information allows FEMA to keep abreast of what is happening throughout the community and to recognize latent or emerging problems and opportunities that might not otherwise become apparent. Conversely, members are apprised of developments elsewhere that may have implications for them. Such open channels promote cooperation generally, and when occasion demands, can facilitate coordination to deal with specific matters of immediate concern.

3.2.11 Represent FEMA on Interagency Civil Security Committees (P.11)

At any given time there are a number of interagency committees, panels, and task forces set up to address civil security issues. One of the functions of the FEMA civil security staff

is to serve as the agent of FEMA, presenting its views, positions, and recommendations in the deliberations of these groups. This function includes performing all the staffing preparations and coordination, both internally within FEMA as well as externally with other agencies affected and other interested parties. It may involve extensive interactions with many levels of FEMA's civil security constituency, at the Federal, State, local and private sector levels Achieving consensus beforehand on controversial points could be critical to the favorable outcome of such interagency proceedings.

3.2.12 Training, Tests, Exercises, and Gaming Support (P.12)

This function refers to a standing requirement to provide special expertise in support of, or to participate in, any training, tests, exercises, and simulation gaming wherever civil security is involved. It could include assisting in the development, planning, or conduct of such activities, as well as managing their execution and evaluating the results. What the function consists of and how it is performed, therefore, vary considerably insofar as the kind and extent of demands placed on the FEMA civil security staff.

3.2.13 Periodic Strategic Net Appraisals of Civil Security (P.13)

From time to time, FEMA must produce strategic net appraisals of the state of the nation's civil security. Basically the function is overall assessment of conditions with respect to threat, vulnerabilities, and capabilities. Included would be an estimate of the threat climate in terms of its current level, salient characteristics, and perceived trends. A correlative estimate would address significant vulnerabilities presently existing in national resource systems, their susceptibility to attack, and the disruptive effects likely to

ensue. There would also be an accompanying estimate of civil security capabilities, posture, and readiness to cope with the threats, along with vulnerability reduction measures underway or planned. Finally, summary conclusions would be drawn as to the prospects for responding to such emergencies and recovering from their potential consequences. The function provides a vital service, not only in support of senior executives and decisionmakers, both in FEMA and the Administration, but also may have value for Congress and the public.

3.3 Trans-event Response Functions (T)

The trans-event response phase commences when a threat materializes and a civil security incident occurs. By definition, it focuses on the event at hand and, therefore, the functions are ad hoc, performed in real time, and are emergency-specific. Figure 3.3 presents schematically a description of the major functions carried out during this phase.

Normally the functional sequence would be triggered abruptly by the first awareness by FEMA that something has happened relating to civil security. However, as the dotted area appearing in the Figure 3.3 diagram indicates, there may sometimes be advance tactical warning that an event is imminent, thus providing lead time. The functions would then begin immediately upon receipt of such warning.

It should be noted that the duration and extent of civil security involvement is scenario-dependent. On most occasions it is expected to be relatively brief, lasting only until the regular FEMA apparatus for response management is marshalled and can take over. Hence, the civil security staff may not be directly involved in all of the functions listed.

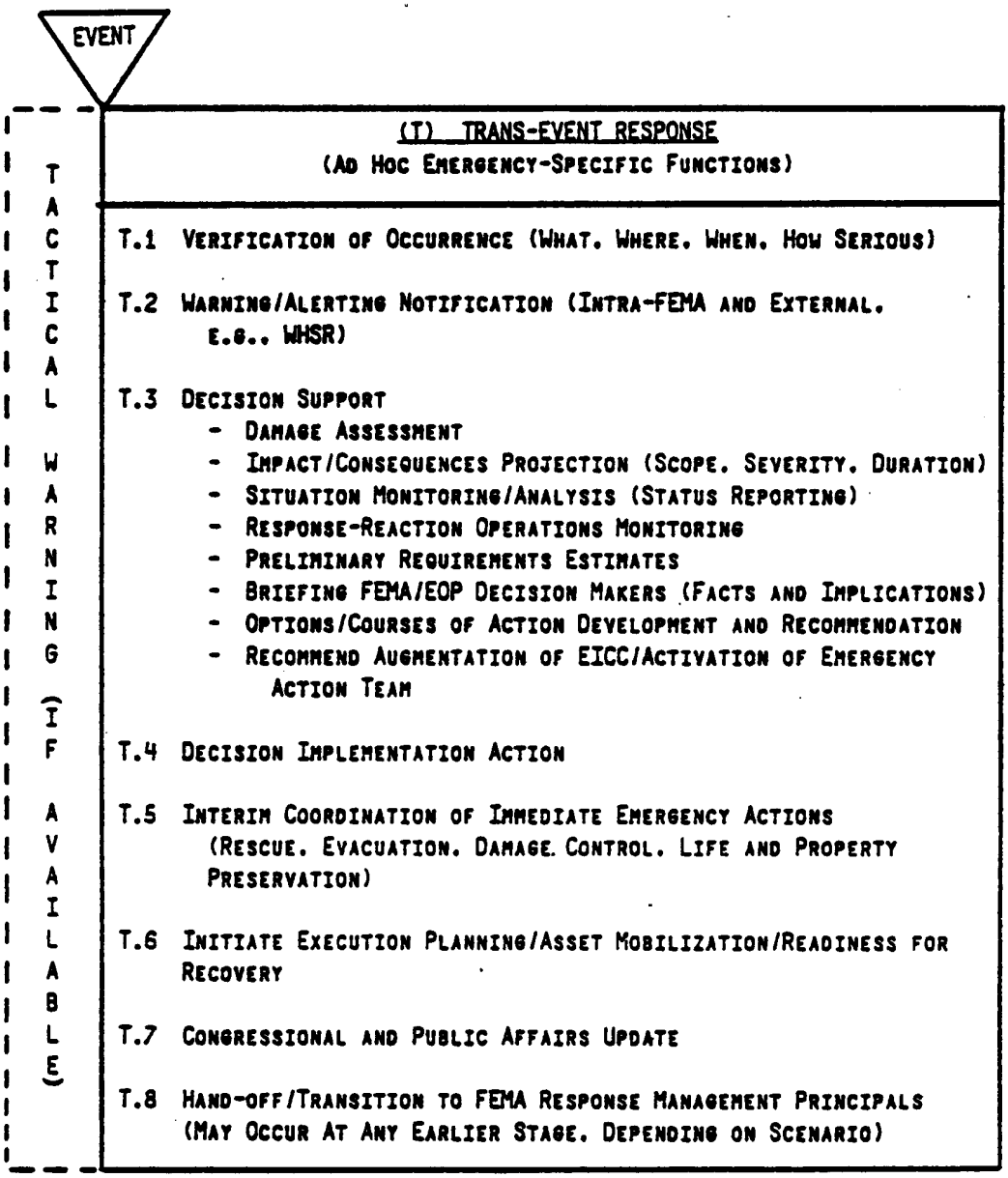


FIGURE 3.3

TRANS-EVENT RESPONSE FUNCTIONS

The individual functions are discussed in the sub-sections immediately following. Selected details explain and amplify each of them in turn.

3.3.1 Verification of Occurrence (T.1)

The essential first function is to verify that a reported civil security incident has indeed occurred. A vital component of that function is establishing basic facts: what happened, where, and how serious does the event appear to be? Initial characterization and sizing estimates are critical as to whether many of the subsequent steps should be taken. The report could be a false alarm, or the incident may be only of local significance. On the other hand, a seemingly trivial event may be seen from the national perspective as bearing the seeds of a major emergency.

3.3.2 Warning and Alerting Notification (T.2)

The next function is a crucial one. All of the agencies, officials, and watch centers having a direct need to know must be warned that an emergency exists. Among those to be immediately notified, for example, would be the FEMA Emergency Information Coordination Center (EICC) and the Director and senior executives of FEMA, the White House Situation Room (WHSR), the National Military Command Center, the FBI operations center, other relevant departments and agencies, and perhaps certain State governments. Also to be alerted as a second priority would be those agencies and organizations likely to be affected in one way or another by the event or its aftermath. This could include private sector elements, such as the transportation carrier industry or telecommunications companies.

3.3.3 Decision Support (T.3)

A vital function of the trans-event phase is the multifaceted one of providing decision support, which shapes the kind of operational response that is taken in connection with the incident. The function consists of its own sequence of functional steps. As outlined in Figure 3.3, the series of component sub-functions comprises the following:

- Initial assessment of the emergency event in terms of immediate casualties and damage incurred, based on the information available
- Estimated direct impact on national resource systems and projected consequences, including the probable scope of disruptive effects, their severity, and duration
- Monitoring the current situation on scene and updating status changes, along with analysis of reported information
- Monitoring the current response-reaction operations underway on scene to cope with the incident
- Preliminary estimates of resources required to respond to the event
- Briefing decisionmakers in FEMA and senior executives of the Administration on the facts and implications of the event
- Developing strategy options and proposed courses of action to deal with the emergency
- Recommending augmentation of the EICC and activation of FEMA emergency action teams to manage response activities.

3.3.4 Decision Implementation Action (T.4)

This function sets in train the course of action adopted. It involves preparing and issuing orders and instruction tasking all of the agencies and organizations responsible for carrying

out the response operations decided upon. The function is time-sensitive, and different kinds of instructions may have to be given to many agencies.

3.3.5 Interim Coordination of Immediate Emergency Action (T.5)

In the interim, before the full response is implemented, some urgent crisis actions of immediate priority may have to be executed as soon as possible. These could be, for example, rescue and evacuation operations to save lives, damage control to prevent the situation from getting out of hand and turning into a large-scale catastrophe, and a variety of other efforts to preserve life and property. The function of coordinating such immediate actions at the outset of the emergency may temporarily have to be performed by the FEMA civil security staff.

3.3.6 Initiate Execution Planning, Asset Mobilization, and Readiness for Recovery (T.4)

Another function that civil security may temporarily have to perform is to begin preparations for recovery operations. Depending on the scenario, delay might prove costly. The function could include getting execution planning started, seeing to it that mobilization of necessary manpower and resources is underway, and initiating an appropriate state of readiness generally. Again, a considerable number of agencies and organizations might be involved. The staffing and coordination task would be correspondingly large and subject to time pressures.

3.3.7 Congressional and Public Affairs Update (T.7)

In any emergency there is always a great demand for information from many quarters. In collaboration with the EICC, the civil security staff would input that information, through briefings and status reports, to the FEMA Congressional relations staff

and the public affairs office. The latter would process and release it through their own channels to their respective audiences. The FEMA civil security staff would not itself deal directly with the news media or members of Congress.

3.3.8 Hand-off and Transition to FEMA Response Management Principals (T.8)

This function marks the termination of civil security's direct role in response management. Presumably at this stage, FEMA's regular response management principals would be actively taking over and in charge. The transition could come quite early in the emergency -- indeed could be the first step taken in the trans-event period. As soon as the hand-off was effected, civil security would retire to the background and enter into the next phase, where its post-event recovery functions become relatively peripheral to the main stream of FEMA activity in relation to the emergency.

3.4 Post-event Recovery Functions (R)

In the final phase, during post-event recovery, civil security is relegated to a subordinate role. Relatively few functions that are uniquely of a civil security nature remain to be performed. Most of the recovery responsibilities fall in other mission areas of FEMA, and the civil security staff is more or less on standby, though it does provide certain ancillary support to recovery management. Depending on scenario, some of these residual functions can nonetheless be important and of considerable scale. Figure 3.4 depicts the sequence of typical post-event recovery functions expected to be performed. Each is discussed in further detail in the subsections below.

(R) POST-EVENT RECOVERY (ANCILLARY MANAGEMENT SUPPORT FUNCTIONS)
R.1 ASSIST FEMA EICC AND STAFF ELEMENTS - PROVIDE CS STAFF EXPERTISE, AS REQUIRED - MAINTAIN LIAISON WITH CIVIL SECURITY COMMUNITY
R.2 ASSESS CONTINUING/FOLLOW-ON CS THREAT - RISK ANALYSIS (OTHER TARGETS, VULNERABILITY, CONSEQUENCES) - ADVISE ALL CONCERNED (INTRA-FEMA AND EXTERNAL)
R.3 MONITOR RECOVERY PHASE ACTIVITIES/PROGRESS (APPRISE INTERESTED AGENCIES)
R.4 DEVELOP AFTER-ACTION LESSONS LEARNED - SUBSTANTIVE PROBLEMS ENCOUNTERED - SYSTEMS DYSFUNCTIONALITIES EXPERIENCED
R.5 REAPPRAISE/ADJUST POLICY, PLANS, PROGRAMS

FIGURE 3.4

POST-EVENT RECOVERY FUNCTIONS

3.4.1 Assist FEMA EICC and Staff Elements (R.1)

A post-event function performed on a sustained basis is to provide timely specialized staff support regarding civil security matters to the EICC, the Office of Emergency Operations (OEO), and other elements of FEMA whenever such expert assistance is required. Many of the recovery operations can have significant civil security implications, and recovery management must take these considerations into account. Another aspect of the same function is maintaining active liaison with those agencies and organizations of the civil security community that may have continuing interest in the emergency event or may be affected by or have a role in recovery. An example would be law enforcement to prevent looting, or to cordon off dangerous areas. Much of the necessary coordination of this kind could be accomplished via such specialized liaison between the civil security staff and other groups involved in the recovery process.

3.4.2 Assess Continuing or Follow-on Threats (R.2)

A given emergency event confronting FEMA may be only one in a series of incidents, or part of a concerted larger campaign of threat actions to follow. Accordingly, an essential civil security function is intensive risk analysis to identify other vulnerable targets that might be affected, and also to estimate the likely consequences if these too were to be struck. In some senarios, this could be an extended iterative process requiring interaction with many agencies and organizations. The products of the risk-analysis function would be disseminated to all concerned, within FEMA and externally. The resulting alert notification might prove critical to those in charge of security for the national resource systems in particular.

3.4.3 Monitor Recovery Activities and Progress (R.3)

In the post-event phase, this function would be a continuation of the earlier monitoring of the emergency situation, but on a more summary level, and tracking the general progress of recovery operations. It would be performed derivitively, based on the primary monitoring being done by other elements of FEMA. The object is for the civil security staff to keep itself abreast of developments, and for it to apprise all other interested parties in the civil security community on the status of recovery.

3.4.4 Develop After-action Lessons Learned (R.4)

The experience gained in the course of the event offers a unique opportunity for drawing lessons that can be of great value for future emergencies. An important civil security function, therefore, is to reconstruct what happened, based on its active involvement, and see what can be learned. Evidence must be gathered and analyzed relating to all aspects of the emergency, from mitigation and preparedness prior to its occurrence through response and recovery. Things to look for would be problems encountered, both substantive and procedural. Attention should be given to identifying achievements as well as deficiencies, with special emphasis on systems performance. Structural dysfunctionalities may be revealed that might otherwise not be detected. Existing policy, plans, and organization can also be examined for adequacy and appropriatness. The potential benefits of such post mortem evaluations should be exploited to the fullest.

3.4.5 Reappraise and Adjust Policy, Plans and Programs (R.5)

The final post-event function is the feedback that closes the loop, leading again to the pre-event phase. In light of the lessons derived from the previous function, the FEMA civil security staff is now in a position to reappraise and, where necessary, adjust, refine, or amplify policy, plans, programs, and all the other functional components of its mitigation and preparedness mission. The kind and extent of adjustment resulting from this last function would depend on the nature of the event just concluded and the significance attributed to that experience.

4. INFORMATION REQUIRED TO SUPPORT FEMA CIVIL SECURITY FUNCTIONS

An essential step in the development of any operational information system is the translation of organizational functions into the types of information required to fulfill these functions. This chapter identifies the information needed to support the pre-event, trans-event, and post-event civil security functions discussed in the previous chapter.

4.1 Classes of Information Requirements

Figure 4.1 briefly outlines the major classes of civil security information requirements by time phases. These and other more specific information requirements will be discussed in greater detail in the subsequent sections.

4.2 Pre-event Information Needs

Identifed in this section are the categories of information required to fulfill the essential civil security functions during the pre-event mitigation and preparedness phase.

4.2.1 Tasking the Providers of Threat Assessments (P.1)

To acquire threat assessment products and other essential elements of information (EEIs), FEMA must have the authority to levy information requirements on relevant agencies and organizations in the intelligence community. Correspondingly, Civil Security Division personnel must be fully cognizant of the various statutes, executive orders, and memoranda of understanding that give them this authority. But the possession of this authority is not sufficient to ensure that the threat information will be obtained. In addition, civil security personnel must be fully aware of the range and types of threat data that can be made available to FEMA. This requires the

CLASSES OF INFORMATION REQUIREMENTS

PRE-EVENT
- THREAT
- RISK ANALYSIS
- NATIONAL POLICY
- PLANS
- PROGRAMS
- TECHNOLOGY

TRANS-EVENT
- ALERTING/WARNING
- POINTS OF CONTACT
- SITUATION
- ON-SCENE RESPONSE
- RECOVERY REQUIREMENTS

POST-EVENT
- RECOVERY PROGRESS
- HISTORICAL RECORD

FIGURE 4.1

MAJOR CLASSES OF INFORMATION REQUIREMENTS

maintenance of point-of-contact rosters for the primary intelligence, security, and law enforcement agencies, both public and private. It also requires a set of standard operating procedures (SOPs) for guiding the query-response transactions involved in gaining access to the relevant data bases. Thus the key information requirements for this function are as follows:

P.1.A Existing FEMA Authority for Levying Threat EEIs (Statutes, Executive Orders, Memoranda of Understanding)

P.1.B Roster of Threat Assessor POCs (Intelligence Community and Others)

P.1.C Query-Response SOPs

Where the authority for levying threat EEIs does not exist, FEMA must initiate the necessary action to establish such authority (see section 4.2.8).

4.2.2 Synthesis of Available Threat Assessment Products (P.2)

The variety of sources that must be tapped in formulating threat assessments is illustrated in Figure 4.2. This shows that a coverage of threats to the various national resource systems requires contacts with over 30 other Federal agencies in addition to the intelligence community at large. Thus one of the difficult tasks that the FEMA Civil Security Division must perform is to collate and synthesize many different EEI inputs in developing its threat assessments. The following categories of information are needed to fulfill this function:

P.2.A Source of Threat (Identity and Nature)

P.2.B Historical Profile (Objectives, Organization, Linkages, Support)

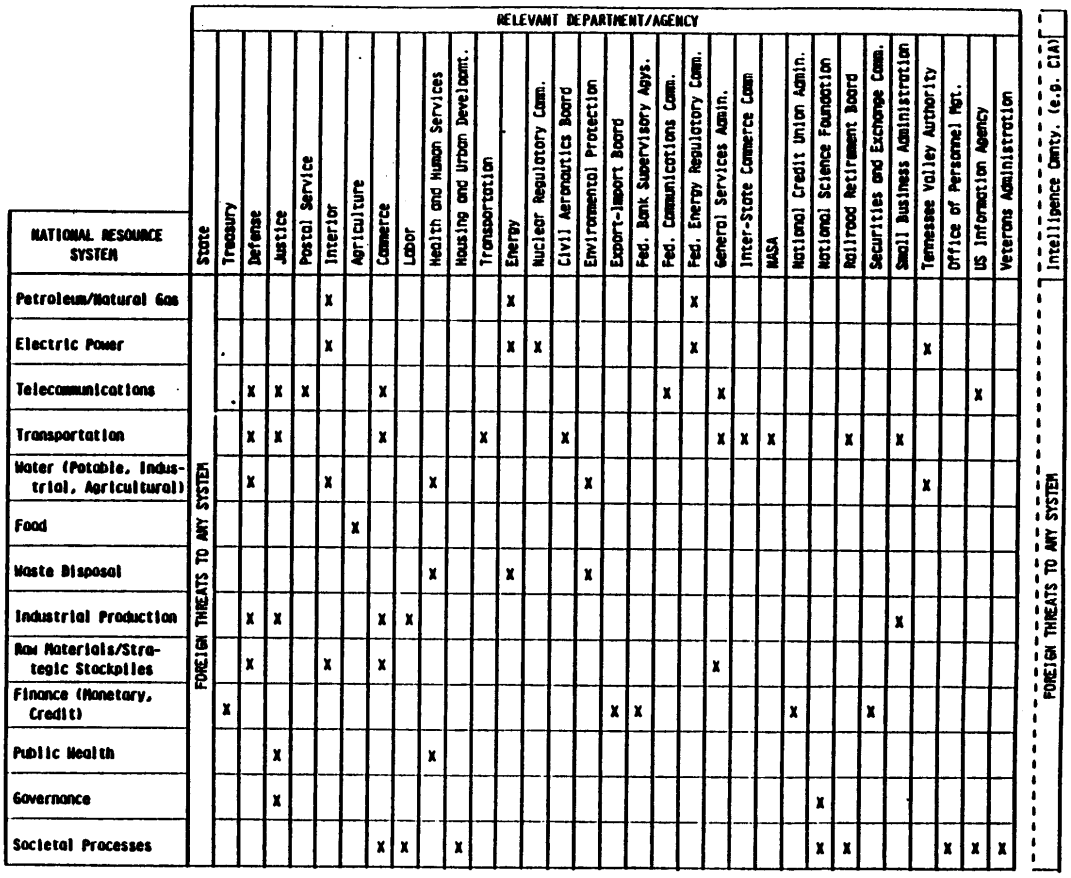


FIGURE 4.2

PRIMARY FEDERAL SOURCES OF THREAT INFORMATION ON NATIONAL RESOURCE SYSTEMS

P.2.C Method(s) of Operation (Tactics, Targets, Time Frames)

P.2.D Capabilities (Deployable Strength, Technical Skills, Resources)

P.2.E Geographic Data (Base of Operations, Staging Points, Pre-positioned Assets)

P.2.F Recent Activities (Type, Periodicity, Patterns/Trends)

P.2.G Extrapolation/Forecasts of Possible Threat Action

The complexity involved in this process is further illustrated in Figure 4.3. It shows, at the next level of detail, the major categories of data needed for these threat assessments, including some of the key data elements that must be taken into account in the evaluation of the threats.

4.2.3 Risk Analysis (P.3)

The development of risk analyses is a complicated process. It requires the mobilization of data on current civil security threats, and on the national resource systems at risk and their interdependencies. It also requires data on the likely targets for disruption, on the likely modes of attack, on the vulnerability of various targets, and on the potential consequences of an attack in terms of primary and secondary effects, severity, scope, and duration. The following information is needed to support this function:

P.3.A Current Threat Assessment Data

P.3.B National Resource System Descriptions (Structural Configuration and Operational Characteristics)

P.3.C Interdependencies among Systems

KEY DATA ELEMENTS	MAJOR CATEGORIES OF DATA					
	Source of Threat	Historical Profile	Method(s) of Operation	Capabilities	Recent Activities	Geographic Data
	• Major Adversary Group • International • Domestic - National - Local	• Group Objectives • Motivation • Organizational Structure • Links to Other Groups • Source(s) of Support • Primary Types of Targets	• Tactics Employed • Time Frame	• Deployable Strength • Technical Skills • Assets	• Targets • Timing • Level of Success	• Primary Base of Operations • Subgroup/Cell Locations • Debarkation/ Staging Points

FIGURE 4.3

CATEGORIES OF EXTERNAL THREAT ASSESSMENT DATA

P.3.D Likely Target Types for Disruption, by System (Critical Nodes/Choke Points, Essential Elements, Key Personnel)

P.3.E Applicable Attack Modes (Demolition, Arson, Seizure, Chemical/Biological, Etc.)

P.3.F Vulnerability Appraisals (Target Accessibility, Exposure, Value vs. Attack Feasibility/ Probability)

P.3.G Potential Consequences Estimates (Primary Impact/Secondary Effects) - Severity, Scope, Duration

Figure 4.4 expands on these requirements, showing some of the detailed information needed under each component for analyzing risks to the various national resource systems. Figure 4.5 outlines a requirements model showing the kind of algorithm that can be used for such a risk analysis and postulates an example illustrating its application in a hypothetical case, namely, risks to bridges and tunnels in the railway transportation resource system.

4.2.4 Policy Development (P.4)

In its role as a developer and coordinator of policy, FEMA must be aware of relevant civil security issues that need policy resolution or clarification. This requires knowledge of administration decisions, directives, and statements on goals, interests, and priorities. The sometimes overlapping Federal responsibilities, roles, and authorities (see Figure 4.2) must also be understood, and the views of interested parties must be solicited as input to any policy development. The following information requirements are encompassed in this civil security function:

Declassified in Part - Sanitized Copy Approved for Release 2011/12/09 : CIA-RDP89B01330R000600870001-6

	Risk Analysis Components			
National Resource System	Target Type	Attack Mode	Vulnerability	Potential Consequences
Petroleum/Natural Gas Electric Power Telecommunications Industrial Production Raw Materials/Strategic Stockpiles	• Character of System • Essential Elements • Inter-System Elements	• Physical Destruction/ Disruption • Technological Subversion • Threat of Attack	• Physical Security • Geographic Location • Geography • Nature of Essential Elements	• Duration • Severity • Scope • Political • Economic • Secondary Systems Affected
Transportation		• Physical Destruction/ Disruption • Subversion • Hostages/Hijackings • Threat of Attack	• Physical Security • Geography • Nature of Essential Elements • Value to Perpetrator	
Water Food Waste Disposal Public Health		• Physical Destruction/ Disruption • Chemical/Biological • Psychological • Threat of Attack	• Physical Security • Geographic Location • Geography • Nature of Essential Elements	
Finance (Monetary, Credit)		• Physical Disruption • Technological Subversion • Economic Subversion	• Technological Security • Nature of Essential Elements • Value to Perpetrator	
Governance Societal Processes		• Political Subversion • Rioting • Assassination/Hostages • Economic Subversion • Threat of Attack	• Physical Security • Nature of Essential Elements	

FIGURE 4.4

INFORMATION REQUIREMENTS FOR CONDUCTING RISK ANALYSIS OF NATIONAL RESOURCE SYSTEMS

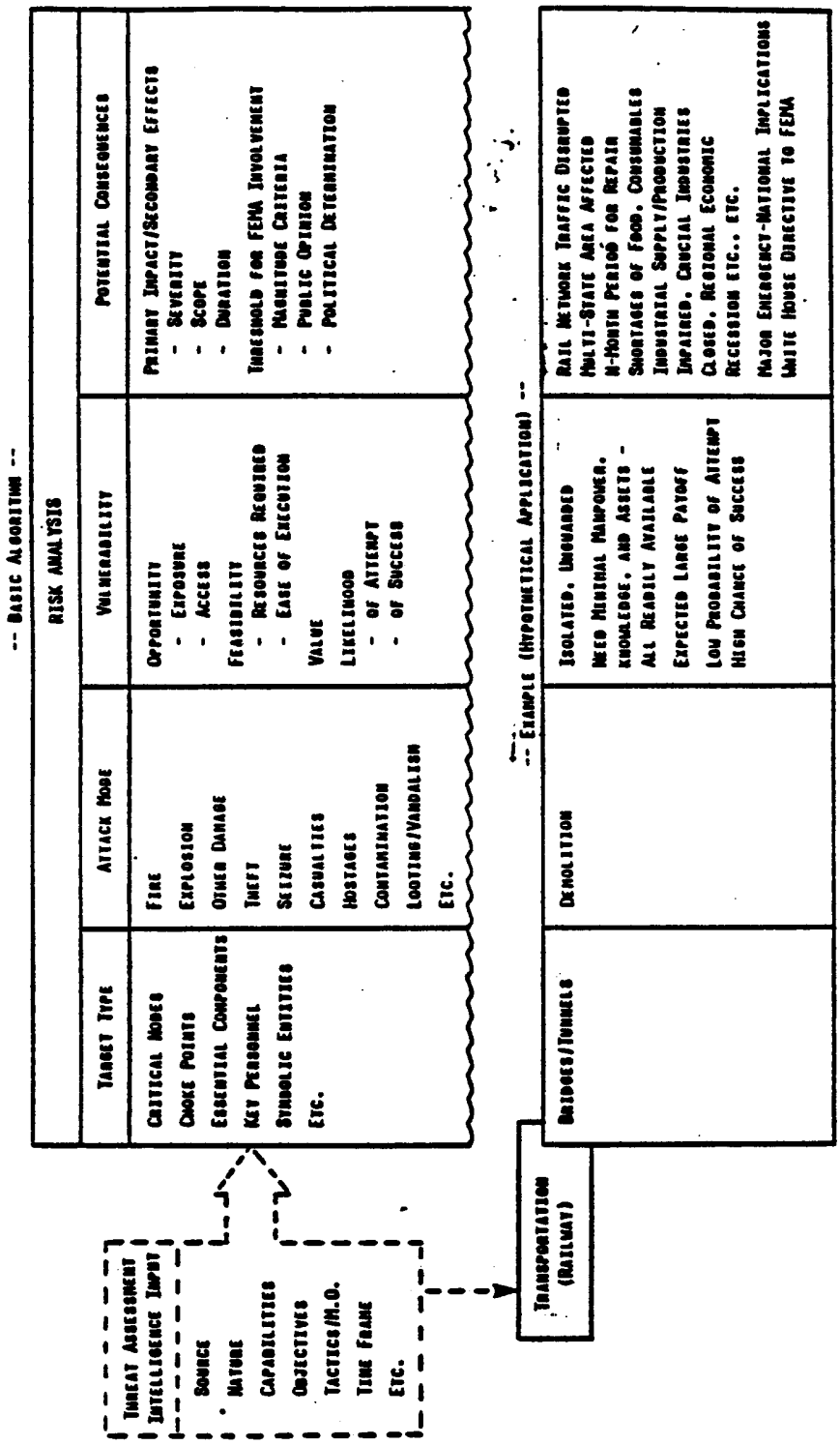


FIGURE 4.5

RISK ANALYSIS INFORMATION MODEL, WITH EXAMPLE

P.4.A Administration Statements/Decisions/Directives on National Civil Security Goals, Interests, Priorities

P.4.B Nature and Background of Issue(s) Needing Policy Resolution or Clarification

P.4.C National Resource System(s) Affected

P.4.D Agencies Involved

P.4.E Statutory Imperatives and Constraints (Responsibilities, Roles, Authority)

P.4.F Relevant Existing Policy and Memoranda of Understanding

P.4.G Views of Major Parties Concerned

P.4.H Policy Implementation Requirements

4.2.5 Planning Guidance (P.5)

The Civil Security Division provides guidance in the development of plans for dealing with threats to the national resource systems. As the information requirements below indicate, this guidance must take into account national strategies, the range of potential threats, and agency responsibilities and capabilities:

P.5.A National Policy Posture (Administration Strategy, Concepts, Desiderata)

P.5.B Statutory Mandates (Executive Orders, Legislative Authority)

P.5.C Range of Potential Threats

P.5.D Vulnerabilities of Threatened National Resource Systems

P.5.E Responsibilities Hierarchy/Network (Roles and Missions)

P.5.F Existing Plans, Memoranda of Understanding, Established Precedents

P.5.G Capabilities and Limitations of Agency(ies) Involved

P.5.H Resources Required, including Assets Available from Private Sector

4.2.6 Plans Review and Evaluation (P.6)

The Civil Security Division takes an active role in the review and evaluation of the civil security plans of other agencies and organizations. Among the information needs in satisfying this role are: a point of contact roster of those personnel in the responsible agencies who developed the plans, an identifier to locate the plan's custodian or repository, and an internal record of policy and guidance issued by FEMA regarding the respective plans. The information needs involved in this process are noted below:

P.6.A Master Inventory of Civil Security Plans/Annexes (Identity and Responsible Agency)

P.6.B POC Roster of Agency Planners

P.6.C Repository of Plan (Custodian)

P.6.D Orientation of Plan (Mitigation, Preparedness, Response, Recovery)

P.6.E Scope and Content (Summary of Provisions)

P.6.F Status (Completeness, Currency, Tested/Untested)

P.6.G Subordinate Related Plans (Regional/State/Local/ Private Sector)

P.6.H Interrelationships Among Plans (Convergence and Dependencies)

P.6.I Internal Record of Policy/Guidance Issued by FEMA

P.6.J Test/Exercise/Real-life Data on Plan Application

4.2.7 Program Coordination (P.7)

In addition to reviewing and evaluating plans, the Civil Security Division coordinates Federal, State, local, and private sector programs relevant to its mission. As noted in the following list, this involves the collection of information on relevant statutes, executive orders, and memoranda of understanding, the repertoire of mitigation, preparedness, response, and recovery techniques and technology in use, and program implementation, strategy, and schedules:

P.7.A Master List of Civil Security Programs (Identity, Purpose, Scope, Participating Agencies)

P.7.B Interrelationships/Dependencies Among Programs

P.7.C Relevant Statutes, Executive Orders, Memoranda of Understanding

P.7.D Formal Steering Committees, Working Groups, Panels Involved (Standing and Ad Hoc)

P.7.E Catalog of Major Program Components (Objectives, Priorities, Milestones)

P.7.F Responsibility Network for Each Program/Program Element (Federal, State, Local, Private Sector)

P.7.G Roster of Program Managers, Action Officers, Cognizant Staff (POCs)

P.7.H Repertoire of Mitigation, Preparedness, Response, and Recovery Techniques and Technology

P.7.I Program Implementation Strategy and Schedules

P.7.J Resource Requirements (Manpower, Special Skills, Equipment and Supplies, Funding Assistance)

P.7.K Status of Programs (Progress, Delays, Changes, Problems)

4.2.8 Initiate Proposed NSC/Legislative Action, as Warranted (P.8)

In conducting its mission, the Civil Security Division may encounter problems, conflicts, and the need for additional executive or legislative authority. Based on the information requirements stated below, FEMA may find it necessary to propose and initiate National Security Council or legislative action to resolve these problems:

P.8.A Nature and Background of Problem Needing such Remedy

P.8.B Pertinent Existing Directives/Legislation

P.8.C Internal Staff Views of Interested FEMA Elements

P.8.D Opinions and Views from Other Affected Agencies

P.8.E Legal and Political Considerations

4.2.9 Advisory Assistance (P.9)

A vital function to be performed by FEMA's Civil Security Division is to serve as a clearinghouse for information on threat technologies and vulnerabilities and the corresponding security technologies needed for dealing with them. The following information needs have been identified with this function:

P.9.A New Developments in Threat Technology (Instruments/Methods)

P.9.B New Technological Vulnerabilities in National Resource Systems

P.9.C State-of-the-Art Security Technology for Dealing with Threats/Vulnerabilities/Consequences

FEMA must keep abreast of new trends and developments that are likely to change the vulnerabilities of the various national resource systems. For example, as transportation systems become more dependent on electronic data processing for such functions as scheduling, routing, maintenance, and coordination, their computers become increasingly vulnerable targets.

4.2.10 Liaison with Civil Security Community (P.10)

The Civil Security Division is primarily a recipient and end-user of information supplied by other agencies and organizations in the civil security community. Its success is therefore largely dependent on developing and maintaining good relationships and effective liaison with other elements of this community. The following information needs serve this purpose:

P.10.A POC Lists of Reciprocal Liaison Counterparts, by Agency and Subject Area

P.10.B Updated Reference Material on Organizational Structure and Roles of Other Civil Security Elements

P.10.C Checklists/Briefs of Current Topics, Problems, Concerns of Mutual Interests

4.2.11 Represent FEMA on Interagency Civil Security Committees/Groups/Task Forces (P.11)

To enable the various agencies with civil security interests to discuss issues and problems and share viewpoints, many interagency committees, groups, and task forces have been or will be established. The FEMA Civil Security Division has a vital interest in being represented in these organizations, or at least being aware of their activities. As the following information requirements indicate, this representation requires knowledge of the agenda of each group, of FEMA's own position on various issues, and of the positions and viewpoints of other agencies:

P.11.A Master List of Interagency Groups concerned with Civil Security matters

P.11.B Agenda of Key Issues/Problems to be Addressed

P.11.C Participating Agencies, Structure of Committee, Members of Delegations

P.11.D Terms of Reference on FEMA Position to be Advocated, and Strategy

P.11.E Other Agencies' Positions and Views

P.11.F Cumulative Record of Proceedings (Proposals, Agreements, Impasses, etc.)

P.11.G Formal Products/Outcomes Resulting from Committee Action (Final or Incremental Findings/ Reports)

4.2.12 Training/Test/Exercise/Gaming Support (P.12)

For the FEMA Civil Security Division to support training, tests, exercises, and games related to civil security, it must have information on the following five subjects:

P.12.A Sponsor and Participants

P.12.B Planned Goals and Objectives

P.12.C Schedules/Time Frames

P.12.D Postulated Scenario/Syllabus to be Followed

P.12.E Control Mechanism Employed

The control mechanism refers to the management of exercises, for example, the operational constraints and degrees of freedom in running them, and the method of determining success or failure.

4.2.13 Periodic Strategic Net Appraisals of Civil Security (P.13)

A vital function and output product of the Civil Security Division is the appraisal of the Nation's civil security posture. This entails keeping abreast of the current threat climate, recent civil security incidents and their consequences, major shortcomings in civil security, and remedies underway to redress those shortcomings. The current civil security capabilities of Federal, State, and local governments, and the private sector must also be evaluated frequently, not only to ensure an adequate defensive posture and response mechanism but also to ensure that appropriate steps are being taken to mitigate and ameliorate adverse consequences. The list below reflects the information needed to satisfy this function:

P.13.A	Historical/Statistical Data on Changing Character, Patterns, Trends in Threat Climate (Domestic and Foreign)
P.13.B	Historical/Statistical Data on Nature, Frequency, Distribution, Consequences of Recent Civil Security Incidents Against National Resource Systems
P.13.C	Major Civil Security Problem Areas/Shortcomings Experienced (Mitigation, Preparedness, Response, Recovery)
P.13.D	Status of Remedial Measures Underway
P.13.E	Federal, State, Local and Private Sector Civil Security Capabilities and Readiness to Mitigate and Ameliorate Adverse Consequences

4.3 Trans-event Information Needs

Identified in this section are the information categories required to fulfill the essential civil security functions during the trans-event response period.

4.3.1 Verification of Occurrence (T.1)

When the Civil Security Division receives notification of a civil security event, activities are immediately initiated to provide verification of occurrence. The following three items of information are essential to this function:

T.1.A Report(s) of event (What, Where, When, How Serious)

T.1.B POC Roster for Verification/Corroboration/ Amplification

T.1.C News Media Bulletins/Accounts

The point-of-contact roster contains names of Federal, State, local, or private sector response-reaction principals whose timely input can provide an accurate assessment of the unfolding events.

4.3.2 Warning and Alerting Notification (T.2)

Once a civil security event has occurred and been verified, the Civil Security Division must ensure that priority need-to-know agencies, direction and control centers, and key personnel are notified in an orderly manner with minimal delay. This notification might actually be performed by the OEO/EICC. The following three information items are needed to fulfill this function:

T.2.A Priority Need-to-Know Agencies/Centers/Key Personnel

T.2.B Roster of POCs

T.2.C Checklist Notification Procedures

4.3.3 Decision Support (T.3)

During a civil security event, FEMA must provide timely estimates and assessments of the unfolding events to permit the key decision makers to make wise and effective decisions aimed at minimizing potential damage or ameliorating negative consequences. The civil security staff, depending on its degree of involvement, must therefore be prepared to acquire -- or assist the OEO/EICC in acquiring -- the following types of needed decision-support information:

T.3.A Direct Impact Damage/Disruption Incurred (Locus, Type, Systems Affected, Scale)

T.3.B Pertinent Pre-calculated Implications/Potential Consequences Extrapolation Data

T.3.C Status Updates on Situation/Changes

T.3.D Status Updates on Operational Response-Reaction Measures

T.3.E Relevant Policies, Doctrine, and Strategy Alternatives

T.3.F Matrix of Responsibility/Jurisdiction (Federal, State, Local, Private Sector)

T.3.G Readiness Posture/Capabilities of Response Elements Apt to be Involved

T.3.H Cumulative Requests for Assistance (Source, Status, Disposition)

T.3.I Agency Estimates of Likely Additional Requirements

T.3.J Resource Availability Data

T.3.K Views, Needs, Problems of Affected Agencies/Interested Parties

T.3.L Emergency Operations Procedures of Emergency Information and Coordination Center/Office of Emergency Operations

4.3.4 Decision Implementation Action (T.4)

The information required for implementing the decisions dictates that the FEMA Civil Security Division have at its disposal a master list of agencies having primary, coordinate, and support responsibilities and of the procedures for issuing requests and instructions for each agency. The Division will also need periodic updates of each agency's responsibilities and points-of-contact. Thus the following types of information are required:

T.4.A Master List of Agencies Having Primary/ Coordinate/Support Responsibilities

T.4.B Procedures for Issuing FEMA Tasking/Requests

T.4.C POCs in Affected Agencies

4.3.5 Interim Coordination of Immediate Emergency Actions (T.5)

As noted in Chapter 3, the civil security staff may temporarily have to coordinate, or assist OEO/EICC in coordinating, the Federal response at the outset of a major civil security event. The Division staff therefore has to be familiar with the primary points-of-contact in each agency and know the agency-specific procedures for orchestrating coordination. The conduct of this interim coordination function will require the following information:

T.5.A Emergency Action POC Roster and Procedure Checklist

T.5.B Existing Applicable Plans

T.5.C Operative Direction and Control Infrastructure

T.5.D Available Rescue/Evacuation Lift Assets

T.5.E Candidate Host Area/Safe Haven Relocation Sites (Shelter and Logistic Support Capacity)

T.5.F Available Damage Control/Containment Resources

T.5.G Available Protective Equipment, Supplies, Personnel

T.5.H Status of Priority Actions in Outside Agencies (Unilateral and Collaborative)

The status of priority actions by outside agencies is monitored to ensure prompt attention to activities deemed most critical.

4.3.6 Initiate Execution Planning/Asset Mobilization/ Readiness for Recovery (T.6)

During the trans-event response period, it may be necessary to initiate steps as early as possible for handling the needed recovery and stabilization measures. In preparing for this transition to the post-event recovery period, the Civil Security Division will require information on the following topics:

T.6.A Master List of Agencies Having Recovery Responsibilities

T.6.B Existing Recovery Agencies

T.6.C POCs within Recovery Agencies

T.6.D Readiness and Execution Procedures (Federal, State, Local, Private Sector)

T.6.E Recovery Resource Requirements Estimates

T.6.F Resource Location/Availability

4.3.7 Congressional and Public Affairs Update (T.7)

The Civil Security Division must be in a position to provide accurate, timely, and appropriate civil security-related information for dissemination through the public affairs and Congressional relations' staff of FEMA. This requires access to up-to-date information on the civil security activities of all agencies involved in the event. The internal FEMA procedures for preparing and briefing these staffs must be well understood by civil security program personnel.

T.7.A Accurate, Current Data on Event and Response

T.7.B Procedures/Criteria for Briefing/Updating FEMA Congressional Relations/Public Affairs Staffs

4.3.8 Hand-off and Transition to FEMA Response Management Principals (T.8)

As the trans-event response phase comes to an end, the Civil Security Division personnel need to prepare for the transfer of responsibilities to the FEMA response management principals. As noted before, such a transfer may occur earlier in the trans-event phase. Two information needs must be satisfied to achieve this transition:

T.8.A Matrix of Responsibilities within FEMA

T.8.B Record of FEMA Actions Completed, in Process, and Pending

Accurate records of the FEMA actions completed, in process, or pending are required to avoid duplication of effort and to expedite recovery measures.

4.4 Post-event Information Needs

This section identifies the information categories required to fulfill the essential civil security functions during the post-event recovery period.

4.4.1 Assist FEMA Emergency Information and Coordination Center/Office of Emergency Operations and Staff Elements (R.1)

During the post-event recovery period, Civil Security Division staff elements and resources must remain available to assist the Office of Emergency Operations, the Emergency Information and Coordination Center, and other FEMA staff members in addressing residual civil security concerns, recognizing potential civil security contingencies, and maintaining contacts within the civil security community involved or interested in the recovery phase. The list below covers the information required to perform this function:

- R.1.A Checklist of Potential Civil Security Contingencies During Recovery
- R.1.B Residual Civil Security Concerns of Agencies Involved in Aftermath of Event
- R.1.C POC Roster of Civil Security Community Involved/ Interested in Recovery Phase

4.4.2 Assess Continuing/Follow-on Civil Security Threat (R.2)

During the post-event recovery period, the Civil Security Division must recognize that additional targets and national resource systems might be threatened. Forecasts and risk analyses, combined with updated threat information, may be needed to cover these possibilities. This threat assessment activity requires the following information:

- R.2.A Updated Threat Information
- R.2.B Additional Possible Targets and Other National Resource Systems that Might be Affected
- R.2.C Projected Risk Analysis Estimates

R.2.D POC Roster for Threat/Risk Forecasts

R.2.E POC Roster of Parties to be Advised

4.4.3 Monitor Recovery Phase Activities/Progress (R.3)

Civil security personnel should monitor recovery phase activities and develop an overview of recovery operations to ensure that civil security concerns are being fully addressed. They should review and, when necessary, change FEMA's criteria and procedures for reporting to interested agencies. And they should update their point-of-contact rosters to reflect necessary changes in the communication network. This will require information on the following four topics:

R.3.A Summary Overview of Recovery Operations

R.3.B Status of Current and Planned Civil Security Related Actions

R.3.C Criteria/Procedures for Reporting to Interested Agencies

R.3.D POC Roster of Agencies Needing Civil Security Update

4.4.4 Develop After-Action Lessons Learned (R.4)

To assess the effectiveness of plans and programs, as well as overall national policy on civil security issues, it will be necessary for all agencies involved in the event to provide after-action reports to the FEMA Civil Security Division. These reports should include an assessment of successes, failures, and problems, accompanied by a critique of agency actions and suggested future improvements. FEMA civil security personnel will analyze these and their own after-action reports and prepare a summary document outlining the lessons learned and the needed remedial actions. The information requirements noted below are aimed at the fulfillment of this function:

R.4.A Reconstruction of Pre-Event Civil Security Posture

R.4.B Cumulative Archival Journal/Chronology of Event, Response, Recovery Experience

R.4.C Detailed Documentation of Salient Problems Encountered

R.4.D Logs, Records, and Observations on System Performance (Achievements and Deficiencies)

R.4.E Critique Reviews/Suggestions by Participants

4.4.5 Reappraise/Adjust Policy, Plans, Programs (R.5)

Section 4.4.4 mentioned the Civil Security Division's need to develop after-action lessons learned from a civil security event to adjust future policy, plans, and programs. This activity provides a feedback mechanism for improving mitigation and preparedness plans and programs, as well as future trans-event response and post-event recovery operations. Based on careful evaluation of the effectiveness and appropriateness of the policy, plans, and programs, as revealed by the after action reports on the recently managed emergency event, the Civil Security Division will initiate, coordinate, and ensure that important remedial adjustments are made internally within FEMA and by the other appropriate Federal agencies. The implementation of such adjustments requires the following information:

R.5.A Policy Issues Bearing on Civil Security Revealed by Emergency

R.5.B Appropriateness and Adequacy of Civil Security Plans to Cope with Event

R.5.C Civil Security Program Shortfalls Demonstrated

R.5.D Indicated Areas of Civil Security Information System Support Needing Improvement

5. INFORMATION PARAMETERS AND CONSTRAINTS

In the previous chapter, the types of information required to support the respective civil security functions were identified and discussed. The next step is the development of a more detailed characterization of the operational parameters and constraints associated with the types of information identified.

5.1 Attributes of Civil Security Information Requirements

The following attributes establish the framework for refining the character of the civil security information requirements: source of information, security classification, frequency, accessibility, and application.

5.1.1 Source

FEMA will have to task many different sources to ensure that the information needed to meet civil security functions is both available and complete. Other agencies have statutory responsibility for developing and implementing civil security plans and programs, for managing the response during an actual event, and for ensuring that appropriate security steps are taken. However, in its oversight and focal point roles, FEMA must recognize that the primary action agency may not be the singular supplier of civil security information. Additionally, Civil Security Division personnel must be able to synthesize the information from all sources to provide the most useful product for internal and external consumers. It should be noted that some sources will provide information only in support of pre-event preparedness activities. Other sources will be brought into play only during trans-event response or post-event recovery periods, depending on the nature of the event as it unfolds.

5.1.2 Security Classification

The security classification of civil security information can be expected to run the gamut from unclassified to top secret and, at times, will require various compartmentalized or code word intelligence clearances. The level of security classification will depend on the source, the specific content of the data, the sensitivity attached to it, and individual scenarios. Civil security and other FEMA personnel must constantly be aware of the potential need to reclassify the information that they produce as a result of data aggregation.

5.1.3 Frequency

The frequency with which civil security information is needed and the frequency with which this information requires updating will obviously vary in terms of the functions to be performed, the time being considered, and the urgency of operational requirements. In general, those functions that pertain to pre-event mitigation and preparedness measures will permit a more routinized flow of information, longer intervals between updates, and less urgency in securing new or updated data. In such cases, the entire process is likely to be fairly predictable, regularized, and controllable. During the occurrence of actual terrorist, civil disorder, sabotage, or subversion incidents, however, the information collection, interpretation, and dissemination processes are likely to change dramatically. In such trans-event periods, the frequency of need and frequency of update become dependent on situational imperatives that are inherently unpredictable. Thus the need for information and the update frequency are likely to be more dynamic--varying with the nature, scope, and pace of the individual event as it unfolds.

5.1.4 Accessibility

FEMA's access to civil security information may take three different forms: (1) routine; (2) limited; and (3) ad hoc requests. Routine information is received on a repetitive, regular, or periodic schedule from numerous governmental and private sector sources, and it is based on pre-established mutual understandings and procedures. Limited access refers to information that may be similarly programmed in advance, but which can only be obtained or received under stipulated conditions, depending on the nature of the particular event and the security classification of the information. Ad hoc requests refer to information that is obtained by FEMA on a case-by-case basis, that is, only when such information is expressly requested and the supplier agency agrees to respond.

5.1.5 Application

In a general sense, civil security information is utilized in two ways. First, some types of information are necessary to support internal civil security functions. Second, Civil Security Division personnel, after the receipt of information, will analyze, synthesize, and condense it. Output products may then be generated and sent to other FEMA elements or to agencies and organizations external to FEMA.

In the following sections of this chapter, each category of information required for a particular function is discussed within the context of these information attributes. Section 5.2 presents the parameters and constraints of information requirements to support pre-event preparedness functions. Section 5.3 presents a discussion of the parameters and constraints relating to information on trans-event response functions; and Section 5.4 deals with post-event recovery functions.

5.2 Pre-Event Phase - Information to Sustain Preparedness Activities

Section 2.3 notes that the audiences with whom FEMA must communicate in carrying out its mission are numerous and diverse. This statement is particularly true regarding civil security functional information requirements. The information to support preparedness functions forms the baseline for the communication process which is essential in carrying out civil security planning, oversight, liaison, and training activities. The following sub-sections present a discussion of the parameters and constraints relating to pre-event information needs. Further details on these parameters and constraints are presented in tables at the end of each subsection.

5.2.1 Tasking the Providers of Threat Assessments (P.1)

FEMA will have to look to the intelligence and law enforcement agencies as points-of-contact as well as to private security organizations. The FEMA Civil Security Division requires standard procedures for gaining access to the various data bases on a daily basis. FEMA's authority to task other agencies for this purpose will necessarily also provide for access to the various bodies of classified data. POC rosters will probably be used on a daily basis to maintain contact with agencies. Any changes in POCs should be transmitted to FEMA on a weekly basis.

5.2.2 Synthesis of Available Threat Assessment Products (P.2)

As can be seen in Table P.2, the primary sources of threat assessment products will be the agencies with intelligence and security missions as well as those with responsibilities for emergency management of the national resource systems. Supplemental data can also be provided by the private sector through

TABLE P.1 - TASKING THE PROVIDERS OF THREAT ASSESSMENTS

Functional Information Requirement		(1) Source		(2) Security Class'n	(3) Frequency		(4) Accessibility			(5) Application	
Code	Description	Primary	Secondary		Need	Update	Routine	Limited	Ad Hoc Request	Internal Use	Output Product
P.1.A	Authority to levy threat EEI tasking	Legislation, E.O., MOU, (NSC)PD		U-S	N/A	N/A	X			X	
P.1.B	POC roster	FBI, State, CIA, DIA, SS	Pvt. Sector, Media, State & Local Govt.	U-S	Daily	Weekly	X			X	
P.1.C	Query-Response SOP's	do*	do	U	Daily	Qrtly.	X			X	

*do = ditto

TABLE P.2 - SYNTHESIS OF AVAILABLE THREAT ASSESSMENT PRODUCTS

Functional Information Requirement		(1) Source		(2) Security Class'n	(3) Frequency		(4) Accessibility			(5) Application	
Code	Description	Primary	Secondary		Need	Update	Routine	Limited	Ad Hoc Request	Internal Use	Output Product
P.2.A	Source of threat	FBI, State, CIA, DIA, INS, DEA, DOT, DOE, HHS, NRC, DOC	Pvt. Sector, Media, State and Local Govt.	C-TS+	Monthly	Weekly		X		X	X
P.2.B	Historical profile	do	do	U-TS	Monthly	Monthly	X			X	X
P.2.C	M.O./tactics	do	do	C-TS	Monthly	Monthly	X			X	X
P.2.D	Capabilities	do	do	TS-TS+	Monthly	Monthly		X		X	X
P.2.E	Geographic data	do	do	TS-TS+	Monthly	Weekly		X		X	
P.2.F	Recent activities	do	do	C-TS	Weekly	Daily	X			X	
P.2.G	Forecasts of possible threat action	do	do	TS-TS+	Weekly	Daily		X		X	X

corporation security offices, the media, and the law enforcement arms of the State and local governments. In those instances where the security classification includes compartmentalized or code word intelligence, special arrangements will have to be made to ensure that FEMA civil security personnel have access to the essential threat assessment data. The Civil Security Division will synthesize these data and disseminate the information to the necessary recipients. Strategic-type studies should be reviewed by FEMA on a monthly basis. Weekly updates of recent activities and changes in forecasts will ensure currency of strategic threat information.

5.2.3 Risk Analysis (P.3)

The intelligence and law enforcement community will be the providers of information needed for civil security risk analysis activities. The nature of the data, the sensitivity associated with collection processes, and the potential value to hostile interests will place most information at the upper levels of security classification. The civil security staff should review risk analysis data on a regular basis. Monthly updates should ensure adequate currency. The classification level will necessitate restrictions or limitations on FEMA's access to risk assessment data maintained by other agencies. The finished products of risk analysis obviously have both internal and external application.

5.2.4 Policy Development (P.4)

Information will be provided by the various agencies and organizations involved in responding to policy and other regulatory issuances. Most information will be unclassified, but MOU's and some of the views of cognizant or affected agencies may fall into the classified arenas. Frequency of use and

TABLE F.3 - RISK ANALYSIS

Functional Information Requirement		(1) Source		(2) Security Class'n	(3) Frequency		(4) Accessibility			(5) Application	
Code	Description	Primary	Secondary		Need	Update	Routine	Limited	Ad Hoc Request	Internal Use	Output Product
F.3.A	Current threat assess. data	FBI, State, CIA, DIA, INS, DEA, DOT, DOE, NRC, DOC, NHS	Pvt. Sector, state & Local Govt., public information	C-TS+	Monthly	Weekly		X		X	
F.3.B	National resource system description	Cognizant Agency(ies)	Affected Agency(ies)	U-S	Monthly	Monthly	X			X	
F.3.C	Interdependencies	Legislative & Executive authorities, OMB, cognizant interagency committees	Atty General, General Counsel	U-S	Monthly	Monthly	X			X	
F.3.D	Target types, critical nodes, etc.	Cognizant Agency(ies)	Affected Agency(ies)	C-TS+	Monthly	Monthly		X		X	
F.3.E	Attack modes	do	do	C-TS+	Monthly	Monthly		X		X	
F.3.F	Vulnerability appraisals	do	do	C-TS+	Monthly	Monthly		X		X	X
F.3.G	Consequence estimates	do	do	C-TS+	Monthly	Monthly		X		X	X

TABLE P.4 - POLICY DEVELOPMENT

Functional Information Requirement		(1) Source		(2) Security Class'n	(3) Frequency		(4) Accessibility			(5) Application	
Code	Description	Primary	Secondary		Need	Update	Routine	Limited	Ad Hoc Request	Internal Use	Output Product
P.4.A	Admin. statements/ decisions/directives	NSC, EOP	Affected agencies	U	N/A	N/A	X			X	
P.4.B	Nature & background of issues needing resolution	Internal FEMA, affected/ cognizant agencies, interagency committees	General Counsel(s), Atty General	U	N/A	N/A	X			X	
P.4.C	Affected national resource systems	Legislation, cognizant agency(ies)	affected agency(ies)	U	N/A	N/A	X			X	
P.4.D	Agencies involved	Legislative mandates/ authority	Admin., EOP, NSC directives	U	N/A	N/A	X			X	
P.4.E	Statutory imperatives & constraints	do	do	U	N/A	N/A	X			X	
P.4.F	Relevant exist. policy & M.O.U's	Cognizant agency(ies), Legislative mandates	do	U-S	N/A	N/A	X			X	
P.4.G	Views of major parties concerned	Cognizant agency(ies)	Affected agency(ies)	U-S	N/A	N/A	X			X	X
P.4.H	Policy implementation requirements	do	do	U-S	N/A	N/A	X			X	X

update requirements are not predictable and will depend upon the priorities of each administration. FEMA should have no restrictions or limitations on access to required information. FEMA will produce a consolidation of the views of the major parties concerned and offer a summation of the policy implementation requirements for external use.

5.2.5 Planning Guidance (P.5)

FEMA will look to a variety of sources in providing civil security planning guidance to the executive agencies. The sources can be expected to range from Federal, State, and local governments to various public interest groups (National Governor's Association, Council of State Governments, National Association of Counties, National League of Cities, U.S. Conference of Mayors, etc.), and other private sector organizations. In most cases policy information will be unclassified. But information on threats and documents outlining detailed plans and giving the capabilities, limitations, and needed resources of agencies are likely to carry various levels of security classification. Since the Civil Security Division must be continually aware of national policy posture in all its activities, frequency of need and update is on-going rather than periodic. Some data, e.g., those on threat and vulnerability, are sufficiently dynamic to require review and updating at least monthly. The information required for planning guidance should be routinely accessible to authorized FEMA civil security personnel.

5.2.6 Plans Review and Evaluation (P.6)

As reviewers and evaluators of plans, civil security program personnel must have access to the civil security plans of

TABLE P.5 - PLANNING GUIDANCE

Functional Information Requirement		(1) Source		(2) Security Class'n	(3) Frequency		(4) Accessibility			(5) Application	
Code	Description	Primary	Secondary		Need	Update	Routine	Limited	Ad Hoc Request	Internal Use	Output Product
P.5.A	National policy posture	EOP,NSC	Cognizant agency(ies)	U	N/A	N/A	X			X	
P.5.B	Statutory mandates	Existing Legislation, MOU's, EOP	Atty General	U	N/A	N/A	X			X	
P.5.C	Range of potential threats	Cognizant agency(ies)	Affected agency(ies)	U-S	Monthly	Monthly	X			X	X
P.5.D	Vulnerabilities of national resource systems	do	do	U-S	Monthly	Monthly	X			X	X
P.5.E	Responsibility hierarchy/network	Existing Legislation, MOU's	Att. General	U	N/A	N/A	X			X	
P.5.F	Exist. plans, MOU's, precedents	do	do	U-S	Monthly	Monthly	X			X	X
P.5.G	Capabilities & limitations of involved agency(ies)	do	do	U-S	N/A	N/A	X			X	X
P.5.H	Resources required	Cognizant agency(ies)	Affected agency(ies), private ind.	U	Monthly	Monthly	X			X	X

TABLE P.6 - PLANS REVIEW AND EVALUATION

Functional Information Requirement		(1) Source		(2) Security Class'n	(3) Frequency		(4) Accessibility			(5) Application	
Code	Description	Primary	Secondary		Need	Update	Routine	Limited	Ad Hoc Request	Internal Use	Output Product
P.6.A	Inventory of CS plans/ annexes	Cognizant agency(ies) (State, local, Federal)	Affected agency(ies) (State, Federal, local)	U	S/D	Monthly	X			X	
P.6.B	P.O.C. roster of agency planners	do	do	U	S/D	Monthly	X			X	
P.6.C	Repository of plan	do	do	U	S/D	Monthly	X			X	
P.6.D	Orientation of plan	do	do	U	Monthly	Monthly	X			X	
P.6.E	Scope & content	do	do	U-TS+	Qrtly	Qrtly		X		X	
P.6.F	Status	do	do	U	Monthly	Monthly	X		X	X	X
P.6.G	Subordinate related plans	do	do	U-TS+	S/D	Qrtly		X		X	
P.6.H	Plans interrelationships	do	do	U-TS+	Qrtly	Qrtly		X		X	
P.6.I	Internal record of policy/guidance issued by FEMA	Internal FEMA	Affected Agency(ies)	U	Qrtly	Monthly	X			X	
P.6.J	Test/exercise/real-life data on plan application	Participating/ Affected agency(ies)	Cognizant agency(ies)	U-TS+	N/A	S/D		X		X	X

Federal, State, and local agencies. The security classification of information on plans will depend on the agency, its responsibilities, and the nature of postulated scenarios. Updating of points-of-contact should occur at least monthly, and updating of plans as required. FEMA personnel should have routine access to most civil security plans. It may be necessary to make ad hoc requests for certain sensitive plans, as well as for status reports when new plans or significant modifications are mandated, e.g., when there are changes in the regulatory base or changes in threat assessments.

5.2.7 Program Coordination (P.7)

As in the case of program guidance and plan review and evaluation, information will be needed from all the Federal, State, and local agencies that have responsibility for, cognizance of, or are affected by civil security actions. This information will generally fall in the unclassified to secret range, with some in compartmented levels. Access to information on program coordination should generally be routine. Some limitations or restrictions may be imposed when compartmented information is required. Most of the information will be used by FEMA personnel on an internal basis. Such items as the comprehensive catalog of programs and a master roster of program managers should be made available to the various agency program managers. A basic catalog of mitigation and preparedness techniques and technology should be produced and distributed, as required. Finally, status reports will be provided to FEMA senior management and be used for the formulation of the periodic Director's report to the President.

5.2.8 Initiate Proposed NSC/Legislative Action (P.8)

The need to seek National Security Council (NSC) or legislative assistance in resolving problems will require information on

TABLE P.7 - PROGRAM COORDINATION

Functional Information Requirement		(1) Source		(2) Security Class'n	(3) Frequency		(4) Accessibility			(5) Application	
Code	Description	Primary	Secondary		Need	Update	Routine	Limited	Ad Hoc Request	Internal Use	Output Product
P.7.A	Master list of CS programs	Cognizant agency(ies) (State/local/ private agencies), NSC	Public information sources	C-S	Monthly	Monthly	X			X	X
P.7.B	Interrelationships/ dependencies among programs	do	do	U-S	Monthly	Monthly	X			X	
P.7.C	Relevant statutes, EO's, MOU's	Existing legislation, Cognizant agency(ies), NSC, EOP	Affected agency(ies)	U-S	Monthly	Monthly	X			X	
P.7.D	Formal steering committees, working groups, panels	Cognizant Agency(ies), State/local/ private agency's	Affected Agency(ies)	U	Monthly	Monthly	X			X	
P.7.E	Catalog of major program components	do	do	C-S	Monthly	Monthly	X			X	X
P.7.F	Responsibility network	do	do	U-C	Weekly	Monthly	X			X	
P.7.G	Roster of program managers etc.	do	do	U	Weekly	Daily	X			X	X
P.7.H	Repertoire of mitigation preparedness techniques & technology	do	do	C-TS+	Monthly	Monthly	X	X		X	X

TABLE P.7 - PROGRAM COORDINATION (Concluded)

Functional Information Requirement		(1) Source		(2) Security Class'n	(3) Frequency		(4) Accessibility			(5) Application	
Code	Description	Primary	Secondary		Need	Update	Routine	Limited	Ad Hoc Request	Internal Use	Output Product
P.7.I	Program implementation strategy & schedules	Cognizent agency(ies), cognizant state/local/ private elements	Affected agency(ies)	C-S	Monthly	Monthly		X		X	
P.7.J	Resource requirements	do	do	C-S	Monthly	Monthly		X		X	
P.7.K	Status of programs	do	do	C-S	Monthly	Monthly	X			X	X

TABLE P.8 - INITIATE PROPOSED NSC/LEGISLATIVE ACTION, AS WARRANTED

Functional Information Requirement		(1) Source		(2) Security Class'n	(3) Frequency		(4) Accessibility			(5) Application	
Code	Description	Primary	Secondary		Need	Update	Routine	Limited	Ad Hoc Request	Internal Use	Output Product
P.8.A	Nature & background of problem	Affected agency(ies), NSC	Cognizant agency(ies)	U	N/A	N/A			X	X	X
P.8.B	Existing directives/ legislation	Affected agency(ies), NSC, MOU's, EOP	Cognizant agency(ies), Agency counsels	U-S	N/A	N/A			X	X	X
P.8.C	FEMA internal staff views	Internal FEMA	—	U-C	N/A	N/A			X	X	X
P.8.D	Opinions, views from other affected agency(ies)	Affected agency(ies)	Cognizant agency(ies)	U-C	N/A	N/A			X	X	X
P.8.E	Legal & political considerations	EOP, NSC, DOJ, Congressional liaison	—	U-C	N/A	N/A			X	X	X

the opinions and views of the affected agencies, as well as internal staff views of interested FEMA elements. Depending on the nature of the problem and the agencies involved, the information may require security classification. The priorities of the administration will determine the frequency with which FEMA requires the information to support this functional area. While some of the information may be obtained via other programmatic activities, it is anticipated that much of the information will be requested by FEMA on an ad hoc basis. FEMA will analyze the available data, summarize the nature of the problem, and recommend a proposed course of action to be submitted to the NSC or appropriate legislative offices.

5.2.9 Advisory Assistance (P.9)

The primary sources will be those agencies that furnish intelligence and security (e.g. law enforcement) information. Much of this information will be highly classified. Frequency of need will be dependent on the release of new developments in technology, the responsiveness of the security community in developing countermeasures, and the ability of the intelligence community to maintain currency on the activities of adversary groups. The Civil Security Division will provide reports on new threats and security technologies to authorized organizations.

5.2.10 Liaison with Civil Security Community (P.10)

The FEMA civil security program will require that information on points-of-contact, organizational structures, current topics, problems, and issues be furnished by each of the cognizant agencies. Most information will be at the unclassified and confidential levels. Since information will be used frequently, it should be updated often enough to ensure

TABLE P.9 - ADVISORY ASSISTANCE

Functional Information Requirement		(1) Source		(2) Security Class'n	(3) Frequency		(4) Accessibility			(5) Application	
Code	Description	Primary	Secondary		Need	Update	Routine	Limited	Ad Hoc Request	Internal Use	Output Product
P.9.A	New developments in threat technology	FBI, NRC, TVA, SEC, GSA, FCC, FERC, DOE, DOT, DOC	NSA, CIA, Public info. sources, Cognizant agency(ies)	U-TS+	S/D	Weekly		X	X	X	X
P.9.B	New tech. vulnerabilities in national resource systems	do	do	U-TS+	S/D	Weekly		X	X	X	X
P.9.C	Security technology for dealing with threats/ vulnerabilities/ consequences	do	do	U-TS+	S/D	Weekly		X	X	X	X

TABLE P.10 - LIAISON WITH CIVIL SECURITY COMMUNITY (FEDERAL AGENCIES/STATE/PRIVATE SECTOR)

Functional Information Requirement		(1) Source		(2) Security Class'n	(3) Frequency		(4) Accessibility			(5) Application	
Code	Description	Primary	Secondary		Need	Update	Routine	Limited	Ad Hoc Request	Internal Use	Output Product
P.10.A	P.O.C. lists of liaison counterparts by agency & subject	Cognizant agency(ies) (state, local, Federal), Private sector	--	U	S/D	Daily	X			X	X
P.10.B	Updated ref. material on org structure & roles of other CS elements	do	--	U	Monthly	Monthly	X			X	X
P.10.C	Checklists/briefs of current topics, problems, concerns of mutual interest	do	--	U-C	Monthly	Monthly		X		X	X

currency, particularly with respect to changes in points-of-contact. FEMA should require and expect fairly routine access, with some limitations imposed in the areas of agency-specific or unique civil security concerns. Information utilized by FEMA civil security personnel should generally be made available to other agencies in the civil security community.

5.2.11 Represent FEMA on Interagency Civil Security Committees/Groups/Task Forces (P.11)

The Civil Security Division will require input from within FEMA concerning the FEMA position on a variety of topics. Information from other agencies that participate in interagency meetings will be required to ensure that the FEMA position is conceptually correct and current. The security classification will generally be at the secret level. Since most groups can be expected to meet on a monthly basis, the Civil Security Division should review and update its data monthly. Any products, i.e., reports, studies, and meeting minutes, may be transmitted to other FEMA staff elements on a selective basis. Accessibility to outside agencies will probably be constrained in such areas as agency internal positions and viewpoints.

5.2.12 Training, Test, Exercise, and Gaming Support (Civil Security-Related Aspects) (P.12)

The Civil Security Division will require information from the sponsor of these activities, from participating agencies, and from other involved FEMA elements. These same sources will be tasked to provide the Division with relevant data on test goals, schedules, scenarios, etc. The Division will evaluate the pertinence and applicability of the civil security aspects and provide pre-test feedback to concerned players. Some information, such as goals, objectives, and scenarios, will fall into the confidential and secret classification levels.

TABLE P,11 - REPRESENT FEMA ON INTERAGENCY CS COMMITTEES/GROUPS/TASK FORCES

Functional Information Requirement		(1) Source		(2) Security Class'n	(3) Frequency		(4) Accessibility			(5) Application	
Code	Description	Primary	Secondary		Need	Update	Routine	Limited	Ad Hoc Request	Internal Use	Output Product
P.11.A	Master list of inter-agency groups with FEMA CS representation	Cognizant agency(ies), OMB, EOP, NSC	--	U	Monthly	Monthly	X			X	
P.11.B	Agenda of key issues/ problems to be addressed	affected interagency committee/ group/task force	--	U-S	S/D	Monthly		X		X	
P.11.C	Participating agencies, structure of committee, members of delegation	do	--	U	Monthly	Monthly	X			X	
P.11.D	Terms of reference on FEMA position	Internal FEMA	--	U-S	Monthly	Monthly		X		X	
P.11.E	Other agency(ies) positions & views	Cognizant agency(ies)	--	U-S	Monthly	Monthly		X		X	
P.11.F	Cumulative record of proceedings	Affected interagency committee/ group/task force	--	U-S	Monthly	Monthly		X		X	
P.11.G	Formal products/outcomes from committee action	do	--	U-S	Monthly	Monthly		X		X	

TABLE P,12 - TRAINING/TEST/EXERCISE/GAMING SUPPORT (CS-RELATED ASPECTS)

Functional Information Requirement		(1) Source		(2) Security Class'n	(3) Frequency		(4) Accessibility			(5) Application	
Code	Description	Primary	Secondary		Need	Update	Routine	Limited	Ad Hoc Request	Internal Use	Output Product
P.12.A	Sponsor & participants	Affected Agency(ies), Internal FEMA	Cognizant Agency(ies), Private Sector	U	S/D	Daily	X			X	
P.12.B	Planned goals & objectives	do	do	U-S	S/D	Daily	X			X	X
P.12.C	Schedules/timeframe	do	do	U-C	S/D	Daily	X			X	
P.12.D	Scenario/syllabus	do	do	U-S	S/D	Daily		X		X	X
P.12.E	Control mechanism	do	do	U	S/D	Daily	X			X	

The need for information will depend on the timing of planned training. Updates and the civil security aspects of tests will be required daily during the execution of tests. Access will generally be on a routine basis with some limitations imposed on test scenarios because of their security classification. The Civil Security Divison will generate civil security goals and objectives for inclusion in test scenarios.

5.2.13 Periodic Strategic Net Appraisals of Civil Security (P.13)

The sources available to FEMA in developing consolidated net appraisals include internal FEMA elements, cognizant agencies, the National Security Council, and the relevant intelligence and security communities. A substantial portion of the information will be dealing with the threat climate, including civil security problem areas and shortcomings. The security classification can therefore be expected to extend into compartmented intelligence levels, with commensurate access restrictions. The Civil Security Divison should review appraisals monthly. Problems and shortcomings should be forwarded from the affected agencies as they are discussed. Remedial measure status reports, prepared on a weekly basis, will ensure that the Division is able to maintain currency. Information concerning civil security problems, remedial measures status, and organizational civil security capabilities will be documented and distributed to authorized civil security community personnel.

5.3 Trans-Event Phase - Information for Response Management

Depending on the amount of warning received prior to an event and the nature and scope of the event, the Civil Security Division may either play a significant initial role in event response or merely act as an advisor on the civil security aspects of an event. The information needed during this

TABLE P.13 - PERIODIC STRATEGIC NET APPRAISALS OF CIVIL SECURITY

Functional Information Requirement		(1) Source		(2) Security Class'n	(3) Frequency		(4) Accessibility			(5) Application	
Code	Description	Primary	Secondary		Need	Update	Routine	Limited	Ad Hoc Request	Internal Use	Output Product
P.13.A	Historical/statistical data on threat climate	Internal FEMA, cognizant agency(ies), NSC	State/local agency(ies), Private Sector	U	Monthly	Monthly	X			X	
P.13.B	Historical/statistical data on national resource systems	do	do	U	Monthly	Monthly	X			X	
P.13.C	Major CS problem areas/ shortcomings	do	do	C-TS+	S/D	Daily		X		X	X
P.13.D	Status of remedial measures underway	do	do	C-TS+	Weekly	Daily		X		X	X
P.13.E	Federal, state, local, private sector CS capabilities	Cognizant agency(ies), NSC, state & local EOC's & agency(ies), private sector	Public information sources, interagency/ interdis-ciplinary committees	U-TS+	Monthly	Monthly		X		X	X

phase--in terms of frequency of use and updating, classification, and source--will vary dramatically based on the event scenario. As a result, the Civil Security Division must ensure that the information processes are in place to support the easy flow of information under varying conditions. The need for an information system that can accomodate a variety of demands and yet be flexible enough to ensure comprehensive access to a broad spectrum of information is underscored in the following discussion of the detailed parameters and constraints associated with response management information requirements.

5.3.1 Verification of Occurrence (T.1)

The primary sources of information for an impending event or an event-in-progress will usually be the agencies with tactical indications and warning centers. The nature of the event, the target, and the type of perpetrator will determine the security classification. For example, information regarding an impending massive demonstration with a potential for large-scale disruption, will probably be unclassified; but a threat of assassination against the President or other elected officials would be handled through classified channels of communication. Regardless of classification, information about impending or actual events that impact the civil security program should be routinely made available to the Civil Security Division. Where the Division is the first activity notified within FEMA, it will transmit the notification to the other relevant FEMA elements. POC rosters will be consulted frequently during the event as it unfolds, so the rosters will be current. They should be updated at least daily, preferably with immediate notification of changes in key personnel. Depending on the nature of the event, the radio, TV, and the wire services may be in the best position to provide immediate information on the

TABLE T.1 - VERIFICATION OF OCCURRENCE

Functional Information Requirement		(1) Source		(2) Security Class'n	(3) Frequency		(4) Accessibility			(5) Application	
Code	Description	Primary	Secondary		Need	Update	Routine	Limited	Ad Hoc Request	Internal Use	Output Product
T.1.A	Report(s) of event	State/local response principals, Affected agency operations center	Public information, EICC, FEMA regional offices	U	S/D	Minutes	X			X	X
T.1.B	P.O.C. roster for verification/coroboration amplification	State/local response principals, State EOC's, cognizant agency(ies)	do	U	S/D	Daily	X			X	
T.1.C	News media bulletins/ accounts	Network radio & TV wire services	-	U	S/D	Minutes	X			X	X

occurrence of an event. A periodic summary of news media information should be sent to FEMA emergency response management elements by the Civil Security Division.

5.3.2 Warning and Alerting Notification (T.2)

Each agency should provide FEMA with information on its key personnel. During an event, the points-of-contact roster should be checked at least daily to ensure currency. To make sure that all affected agencies can be contacted by FEMA personnel, each agency should inform FEMA of any unique notification procedures. Because of the classification level of key personnel and POC rosters, procedures within some agencies may be classified. Thus FEMA may have to conform to certain restrictions or limitations on access. The information will be used internally to make certain that the affected agencies can be notified of an event by FEMA on a timely basis.

5.3.3 Decision Support (T.3)

Sources with direct and tangential responsibility must be in a position to support FEMA's civil security activities in the response period. For example, there is an obvious interdependence between information concerning the damage and disruption incurred and the potential consequences. Depending on the nature of the event scenario, the information classifications will range from unclassified through at least secret levels. Information required by civil security will be accessed frequently. It should be updated at least hourly in the early stages of the event. The scenario will ultimately determine the need and frequency of update. Current emergency procedures that define the Civil Security Division-Emergency Information and Coordination Center interface should be in place and reviewed at least monthly by the civil security staff. They

TABLE T.2 - WARNING/ALERTING NOTIFICATION

Functional Information Requirement		(1) Source		(2) Security Class'n	(3) Frequency		(4) Accessibility			(5) Application	
Code	Description	Primary	Secondary		Need	Update	Routine	Limited	Ad Hoc Request	Internal Use	Output Product
T.2.A	Priority need-to-know agencies/centers/key personnel	Affected agency(ies)	Cognizant agency(ies), Internal FEMA	U	Weekly	Monthly	X			X	
T.2.B	Roster of P.O.C.'s	do	do	U	Daily	Daily	X			X	
T.2.C.	Checklist notification procedures	Affected agency(ies)	do	U-S	Monthly	Monthly	X	X		X	

TABLE T.3 - DECISION SUPPORT

Functional Information Requirement		(1) Source		(2) Security Classn	(3) Frequency		(4) Accessibility			(5) Application	
Code	Description	Primary	Secondary		Need	Update	Routine	Limited	Ad Hoc Request	Internal Use	Output Product
T.3.A	Damage/disruption incurred	Response, principals, FEMA regions/ EICC, Affected agency(ies)	Congnizant agency(ies), public information	U	S/D	Hourly			X	X	X
T.3.B	Implications/ consequences	Affected agency(ies), NSC, EOP, intelligence agencies	Cognizant agency(ies)	U-S	Hourly	Hourly		X	X	X	X
T.3.C	Status updates on situations/changes	Response principals, Affected agency(ies)	Cognizant agency(ies), intelligence agency(ies)	U	S/D	Hourly			X	X	X
T.3.D	Status updates on response-reaction measures	do	do	U-S	S/D	Hourly	X	X		X	X
T.3.E	Policy/doctrine/strategy alternatives	Affected agency(ies)	Cognizant agency(ies), FEMA-NPP	U-S	Daily	Hourly	X	X		X	X
T.3.F	Matrix of responsibility	Legislative authorities, MOU's, EO's	-	U	S/D	Hourly	X			X	

Declassified in Part - Sanitized Copy Approved for Release 2011/12/09 : CIA-RDP89B01330R000600870001-6

TABLE T.3 - DECISION SUPPORT (Concluded)

Functional Information Requirement		(1) Source		(2) Security Classin	(3) Frequency		(4) Accessibility			(5) Application	
Code	Description	Primary	Secondary		Need	Update	Routine	Limited	Ad Hoc Request	Internal Use	Output Product
T.3.G	Readiness posture	Affected agency(ies), response elements, NSC	Cognizant agency(ies), private sector	U-S	S/D	Daily	X	X		X	
T.3.H	Requests for assistance	FEMA regions, response principals, Affected agency(ies), State EOC's	Cognizant agency(ies), private sector	U	S/D	Hourly			X	X	X
T.3.I	Estimates of likely additional requirements	Affected agency(ies)	FEMA regions	U	S/D	Hourly			X	X	X
T.3.J	Resource availability	Response principals, affected agency(ies), State EOC's, FEMA regions	Cognizant agency(ies), private sector	U	Daily	Hourly	X			X	X
T.3.K	Views, needs, problems of affected agencies	Affected agency(ies)	FEMA regions	U-S	Daily	Hourly	X	X		X	X
T.3.L	Emergency operations procedures of EICC/OEO	EICC/OEO	-	U-S	Monthly	Monthly	X			X	

should also be updated monthly. The rapidity with which the event unfolds will probably dictate the need for ad hoc requests in the early stages of the event. Because the information may be highly classified, some access limitations can be anticipated. The Civil Security Division will also be required to provide decision makers with consolidated information on the civil security resources required during and immediately following the actual event.

5.3.4 Decision Implementation Action (T.4)

The Civil Security Division will require information on specific delegations of responsibility within each affected agency. Information on tasking procedures should be provided by other FEMA elements. The event scenario will determine frequency of need. The Division will also need periodic updates of each agency's responsibilities and points-of-contact. Most information to support FEMA's functions in this area should be available on a routine access basis because it will be unclassified.

5.3.5 Interim Coordination of Immediate Emergency Actions (T.5)

During the trans-event phase, the Civil Security Division must have information on the primary civil security points-of-contact from each agency. It will frequently refer to information on rescue and evacuation assets, resources for damage control and containment, and the status of emergency actions to date. The frequency of updates will be dictated by the nature of the scenario. The Division staff should have ready access, although access to some information will be limited by high-level security classification. The Division, in collaboration with OEO, will prepare up-to-date summaries of information on the civil securityrelated aspects of response operations, such

TABLE T-4 - DECISION IMPLEMENTATION ACTION

Functional Information Requirement		(1) Source		(2) Security Classification	(3) Frequency		(4) Accessibility			(5) Application	
Code	Description	Primary	Secondary		Need	Update	Routine	Limited	Ad Hoc Request	Internal Use	Output Product
T.4.A	List of agencies having primary/coordinate/ support responsibilities	Affected/ cognisant agency(ies), Legislative authorization, MOU's, EO's	FEMA-NPP	U	S/D	Monthly	X			X	
T.4.B	Procedures for issuing FEMA tasking/requests	Internal FEMA	-	U	S/D	Yearly	X			X	
T.4.C.	P.O.C.'s in affected agency(ies)	Affected agency(ies)	FEMA regions	U	S/D	Daily	X			X	

TABLE T.5 - INTERIM COORDINATION OF IMMEDIATE EMERGENCY ACTIONS

Functional Information Requirement		(1) Source		(2) Security Class'n	(3) Frequency		(4) Accessibility			(5) Application	
Code	Description	Primary	Secondary		Need	Update	Routine	Limited	Ad Hoc Request	Internal Use	Output Product
T.5.A	Emergency action P.O.C. roster and procedures	Affected agency(ies), State EOC's, Response principals, FEMA, EICC, NPP	Cognizant agency(ies),	U	S/D	Daily	X			X	
T.5.B	Existing applicable plans	Affected agency(ies), FEMA, NPP, SLP, State EOC's	do	U-S	S/D	Monthly	X	X		X	
T.5.C	Direction and control infrastructure	do	do	U	S/D	Monthly	X			X	
T.5.D	Rescue/evacuation assets	do	do	U-C	S/D	Hourly	X	X		X	X
T.5.E	Relocation sites	do	do	U-C	S/D	Daily	X	X		X	X
T.5.F	Damage control/ containment resources	do	do	U	S/D	Daily	X			X	X
T.5.G.	Protective equipment, supplies, personnel	do	do	U	S/D	Daily	X			X	X
T.5.H.	Status of agency actions	do	do	U-S	Daily	Hourly	X	X		X	

Declassified in Part - Sanitized Copy Approved for Release 2011/12/09 : CIA-RDP89B01330R000600870001-6

as relocation sites, special protective equipment, supplies, and skilled personnel, to the affected agencies.

5.3.6 Initiate Execution Planning, Asset Mobilization, and Readiness for Recovery (T.6)

Agencies that are responsible for recovery activities should provide the Civil Security Division with relevant information on plans, procedures, and resources for post-event recovery. While most of the information should have been provided as part of preparedness activities, the nature and scope of the event requires that agencies give the Division necessary updates and changes. Most of the information should be routinely available to FEMA, although the security classification may dictate some restrictions. As information on recovery requirements and resource location is compiled, it should be transmitted to the affected agencies.

5.3.7 Congressional and Public Affairs Updates (T.7)

The Civil Security Division must have access to up-to-date information on the civil security activities of all agencies involved in the event. The internal FEMA procedures for preparing and briefing information for the FEMA Congressional relations and public affairs staffs will be used frequently during the event. Classified data on current events may have to be accessed and transmitted to the Congressional.

5.3.8 Hand-off/Transition to FEMA Recovery Management Principals (T.8)

The Office of Emergency Operations should inform the Civil Security Division of those FEMA elements that will ultimately assume response management. In turn the Division will provide the EICC/OEO with a record of its actions during its initial

TABLE T.6 - INITIATE EXECUTION PLANNING/ASSET MOBILIZATION/READINESS FOR RECOVERY

Functional Information Requirement		(1) Source		(2) Security Class'n	(3) Frequency		(4) Accessibility			(5) Application	
Code	Description	Primary	Secondary		Need	Update	Routine	Limited	Ad Hoc Request	Internal Use	Output Product
T.6.A	List of agency(ies) with recovery responsibilities	Affected agencies, Legislative mandates, MOU's, EO's	Cognizant agency(ies), FEMA regions, NPP	U-S	S/D	Daily	X	X		X	
T.6.B	Recovery plans	Responsible agency(ies) and organizations	Cognizant agency(ies), FEMA regions, Private sector	U-S	S/D	Daily	X	X		X	
T.6.C	P.O.C's within recovery agency(ies)	do	-	U	S/D	Daily	X			X	
T.6.D	Readiness and execution procedures	do	Cognizant agency(ies), private sector, FEMA regions	U-S	S/D	Daily	X	X		X	
T.6.E	Recovery resource requirements estimates	do	do	U-S	S/D	Daily	X	X		X	X
T.6.F	Resource location/ availability	do	do	U-S	S/D	Daily	X	X		X	X

Declassified in Part - Sanitized Copy Approved for Release 2011/12/09 : CIA-RDP89B01330R000600870001-6

TABLE T.7 - CONGRESSIONAL AND PUBLIC AFFAIRS UPDATE

Functional Information Requirement		(1) Source		(2) Security Class'n	(3) Frequency		(4) Accessibility			(5) Application	
Code	Description	Primary	Secondary		Need	Update	Routine	Limited	Ad Hoc Request	Internal Use	Output Product
T.7.A	Accurate, current data on event	FEMA EICC, Response principals, Affected/ cognizant agency(ies), OEO	Public information sources	U-S	S/D	Hourly	X	X		X	X
T.7.B	Procedures for briefing/ updating congress	Internal FEMA, Congressional liaison	-	U	S/D	Daily	X			X	

TABLE T.8 - HAND-OFF/TRANSITION TO FEMA RESPONSE MANAGEMENT PRINCIPALS

Functional Information Requirement		(1) Source		(2) Security Class'n	(3) Frequency		(4) Accessibility			(5) Application	
Code	Description	Primary	Secondary		Need	Update	Routine	Limited	Ad Hoc Request	Internal Use	Output Product
T.8.A	FEMA matrix of responsibilites	Internal FEMA	-	U	S/D	S/D	X			X	
T.8.B.	Record of FEMA actions completed, in process, pending	do	-	U-TS+	S/D	Hourly	X	X	X	X	X

period of event management. It will also provide hourly updates of its activities related to event response. Information on responsibilities will likely be unclassified and routinely available to the Division. Notification of changes should be furnished to the Division as frequently as necessary.

5.4 Post-Event Phase - Information Associated with Recovery

In the recovery phase, the Civil Security Division has two generic information tasks: (a) addressing civil security-related issues associated with the event or with the recovery operations, and (b) evaluating the overall effectivenesss of the Federal, State, local and private sector civil security activities during the emergency. As noted in Chapter 4, the information required to support recovery activities involves maintaining communication with all agencies that were participants in the event and documentation of their actions. The specific items and sources of information will vary, depending on the nature of the event. The parameters and constraints discussed in this section continue to underscore the need for data gathering and information dissemination that is sufficiently flexibile to allow for varied sources, classification, and frequency of use.

5.4.1 Assist FEMA Emergency Information and Coordination Center/Office of Emergency Operations and Staff Elements (R.1)

Information on possible civil security problems arising from or impinging upon recovery must be acquired from the agencies affected and conveyed to all interested parties. Most of the information collected and transmitted during this phase will have a maximum security classification of secret and should be accessible on a routine basis. Information on potential new

TABLE R.1 - ASSIST FEMA EICC/OEO AND STAFF ELEMENTS

Functional Information Requirement		(1) Source		(2) Security Classn	(3) Frequency		(4) Accessibility			(5) Application	
Code	Description	Primary	Secondary		Need	Update	Routine	Limited	Ad Hoc Request	Internal Use	Output Product
R.1.A	Checklist of potential CS contingencies during recovery	Agencies participating in event	Non-participating observers, private sector, news media	U-S	Daily	Daily	X			X	
R.1.B	Residual concerns of CS agencies in aftermath of event	Affected agencies	S/D	U-S	Daily	Daily			X	X	X
R.1.C	POC roster of CS community involved/interested in recovery phase	do	do	U	Daily	Daily	X			X	X

contingencies and residual on concerns must be available on at least a daily basis. When there is a significant potential for secondary or tertiary effects (which may alter the scale or character of recovery demands), the Civil Security Divison should receive and disseminate information on civil security concerns to the EICC/OEO elements on a daily basis, or more frequently if circumstances warrant.

5.4.2 Assess Continuing/Follow-on Civil Security Threat (R.2)

Assessment information on additional targets and resource systems must be furnished by the intelligence and security communities. They should also furnish threat information and estimates updates. To ensure that the Civil Security Division can maintain flexibility and be prepared to modify its civil security operations and network of communication channels, POC rosters must be updated daily. Information for these activities will cover the entire range of security classification. Reports on civil security threats must be disseminated to affected members of the intelligence and security community.

5.4.3 Monitor Recovery Phase Activities/Progress (R.3)

Civil security personnel should monitor recovery phase activities based on information from all agencies involved. FEMA should provide procedures for reporting to interested agencies. Agency point-of-contact rosters should be provided to the Civil Security Division, and updates should be forwarded daily. Since most of the information on this subject will be classified secret or below, access by FEMA should be on a routine basis.

5.4.4 Develop After-Action Lessons Learned (R.4)

All agencies involved in the event should prepare after-action reports for the FEMA Civil Security Division. During the

TABLE R.2 - ASSESS CONTINUING FOLLOW-ON CS THREAT

Functional Information Requirement		(1) Source		(2) Security Class'n	(3) Frequency		(4) Accessibility			(5) Application	
Code	Description	Primary	Secondary		Need	Update	Routine	Limited	Ad Hoc Request	Internal Use	Output Product
R.2.A	Updated threat information	FBI, STATE, CIA, DIA, DEA, DOT, DOE, INS, NRC, DOC, HHS	Pvt sector, media, state & local agencies	C-TS+	Daily	Daily	X	X		X	X
R.2.B	Additional probable targets and other national resources that might be affected	do	do	U-TS+	do	do	X	X		X	X
R.2.C	Projected risk analysis estimates	do	do	C-TS+	do	do	X	X		X	X
R.2.D	POC roster for threat/ risk forecasts	do	do	U-S	do	do	X			X	
R.2.E	POC roster of parties to be advised	do	do	U-S	do	do	X			X	X

Declassified in Part - Sanitized Copy Approved for Release 2011/12/09 : CIA-RDP89B01330R000600870001-6

TABLE R-3 - MONITOR RECOVERY PHASE ACTIVITIES/PROGRESS

Functional Information Requirement		(1) Source		(2) Security Class'n	(3) Frequency		(4) Accessibility			(5) Application	
Code	Description	Primary	Secondary		Need	Update	Routine	Limited	Ad Hoc Request	Internal Use	Output Product
R.3.A	Summary overview of recovery operations	primary action agencies	FEMA regions, State and local agencies, private sector	U-S	Daily	Daily	X			X	
R.3.B	Status of current and planned CS-related actions	do	do	U-S	Daily	Daily	X			X	X
R.3.C	Criteria for reporting to interested agencies	Federal, State & local agencies	FEMA-OEO, FEMA regions	U	N/A	Monthly	X			X	
R.3.D	POC roster of agencies needing CS update	do	do	U	Daily	Daily	X			X	X

Declassified in Part - Sanitized Copy Approved for Release 2011/12/09 : CIA-RDP89B01330R000600870001-6

TABLE R.4 - DEVELOP AFTER-ACTION LESSONS LEARNED

Functional Information Requirement		(1) Source		(2) Security Class'n	(3) Frequency		(4) Accessibility			(5) Application	
Code	Description	Primary	Secondary		Need	Update	Routine	Limited	Ad Hoc Request	Internal Use	Output Product
R.4.A	Reconstruction of pre-event CS posture	Agencies involved in event	FEMA Regions, observers, private sector, news media	U-S	Daily	S/D	X	X		X	
R.4.B	Cumulative archival journal/chronology of event, response, recovery experience	do	do	U-S	Daily	S/D	X	X		X	
R.4.C	Detailed documentation of salient problems encountered	do	do	U-S	Daily	S/D	X	X		X	
R.4.D	Logs, records, and observations on system performance (achievements and deficiencies)	do	do	U-S	Daily	S/D	X	X		X	
R.4.E	Critique reviews/ suggestions by participants	do	do	U-S	Daily	S/D	X	X		X	X

Declassified in Part - Sanitized Copy Approved for Release 2011/12/09 : CIA-RDP89B01330R000600870001-6

recovery period, the Division will need such historical information on a daily basis as it consolidates and summarizes the record of what transpired. Agencies should furnished updates whenever there are significant changes in their activities. Much of this information will be security sensitive and will require appropriate classification and commensurate restrictions on access. Copies of these summaries, including appropriate recommendations, should be disseminated to all appropriate agencies and organizations in the civil security community.

5.4.5 Reappraise/Adjust Policy, Plans, and Programs (R.5)

All agencies involved in the event must provide the Civil Security Division with after action reports on the event. As in the case of after-action reports, much of the information on needed adjustments and improvements in civil security policy, plans, and programs will be security sensitive and will therefore require appropriate classification and restriction on access. Recommendations on improvements needed will be forwarded to affected agencies.

TABLE R.5 - REAPPRAISE/ADJUST POLICY, PLANS, PROGRAMS

Functional Information Requirement		(1) Source		(2) Security Class'n	(3) Frequency		(4) Accessibility			(5) Application	
Code	Description	Primary	Secondary		Need	Update	Routine	Limited	Ad Hoc Request	Internal Use	Output Product
R.5.A	Policy issues bearing on CS surfaced by emergency	Law, EO, MOU, (NSC) PD		U-S	N/A	N/A	X			X	
R.5.B	Appropriateness and adequacy of CS plans to cope with event	Fed, State, & local agencies involved in event	FEMA Region private sector	U-S	S/D	S/D	X			X	
R.5.C	CS program shortfalls demonstrated	do	do	U-S	S/D	S/D	X			X	
R.5.D	Indicated areas of CS information system support needing improvement	do	do	U-S	S/D	S/D	X			X	X

Declassified in Part - Sanitized Copy Approved for Release 2011/12/09 : CIA-RDP89B01330R000600870001-6

APPENDIX A

GLOSSARY

CIA	Central Intelligence Agency
Choke Points	Functional/logistic areas of highest vulnerability within a national resource system
Civil Security	Mitigation, preparedness, response, and recovery activities to reduce the consequences of terrorism, civil disorder, sabotage, and subversion
Civil Security Division	Division under the Office of Mobilization Preparedness within the National Preparedness Programs Directorate of FEMA concerned with civil security matters
Code Word	A specific security classification above Top Secret
Compartmented	A specific security classification above Top Secret
Control Mechanism	In an exercise, test, or game, the method by which it is managed, the operational constraints and degrees of freedom, and the method for determining success or failure
Critical Nodes	Functional/logistic areas of highest vulnerability within a national resource system
CS	Civil Security
CSD	Civil Security Division of FEMA
DEA	Drug Enforcement Administration
DIA	Defense Intelligence Agency
DOC	Department of Commerce
DOE	Department of Energy
DOJ	Department of Justice
DOT	Department of Transportation

EEI	Essential element(s) of information
EICC	Emergency Information and Coordination Center within FEMA
EO	Executive order
EOP	Executive Office of the President
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FEMA Regions	The ten geographic regions of FEMA in the United States, each under a regional office
FERC	Federal Energy Regulatory Commission
FPC	Federal Power Commission (now FERC)
GSA	General Services Administration
HHS	Department of Health and Human Services
INS	Immigration and Naturalization Service
Management Information System	A computer-based organizational information system which provides data to support management activities and functions
Matrix of Responsibilies	A method of graphically relating agencies to their respective areas of responsibility
MOU	Memorandum of understanding
National Resource Systems	The thirteen categories, defined in Figure 2.2, potentially vulnerable to disruption by terrorism, civil disorder, sabotage, and subversion
NEMS	National Emergency Management System
NIE	National Intelligence Estimate

NPP	National Preparedness Programs Directorate in FEMA
NRC	Nuclear Regulatory Commission
NSA	National Security Agency
NSC	National Security Council
OEO	Office of Emergency Operations in FEMA
OMB	Office of Management and Budget
PD	Presidential directive
POC	Point(s) of contact
POL	Petroleum, oil, and lubricants
Post-Event Recovery Phase	The period of activity, following a civil security event, in which recovery operations occur
Pre-event Preparedness Phase	The period of continuous, on-going activity in preparation for and prior to a civil security event
Readiness Posture	The capabilities for dealing with a contingency
Responsibility Network	The interrelationships and overlap among agencies' responsibilities
SEC	Securities and Exchange Commission
S/D	Scenario Dependent
SLP	State and Local Programs and Support Directorate in FEMA
SNIE	Special National Intelligence Estimate
SS	Secret Service
Straw Man	A technique used to test the applicability, relevance, and usefulness of a proposed central idea

WHSR	**White House Situation Room**
Threat Climate	**Appraisals of the likelihood, context, and form of terrorism, civil disorder, sabotage, or subversion**
Trans-event Response Phase	**the period of activity during and immediately following a civil security event in which immediate reaction-response measures are taken**
TVA	**Tennessee Valley Authority**

DISTRIBUTION LIST

Internal

W-20 F. Holland
J. Nuneville

W-21 C. Fritz
T. Hunzeker
E. Janicik (5)
H. Strong
W-21 File (2)

W-27 F. Tompkins
W-30 W. M. Hall
W-50 M. Scholl
W-73 S. R. Hirsch
W-74 D. R. Friedman

Document Control
Mitre/Metrek Library
Records and Resources

External

C. Light (20)
D. Ray