SECTION FIVE: COMMUNICATIONS ISSUES

Table of Contents

Table 1: Congressional Grants of Authority Regarding Information Sharing to Respond to an Emergency or Major Disaster involving Weapons of Mass Destruction

Reference & Section	Affected Entity	Principal Focus
Presidential Documents		
Homeland Security Presidential Directive 3	White House	Created the Homeland Security Advisory System
Executive Order 12333	White House	Ensures that the United States will receive the best intelligence available
Executive Order 12382	White House	Established the National Security Telecommunications Advisory Committee, composed of industry leaders, to advise President Reagan on communications policy
Executive Order 12472	White House	Defines the mission of the NCS as "the coordination of the planning for and provision of national security and emergency preparedness communications for the Federal government under all circumstances, including crisis or emergency, attack, recovery and reconstitution
Executive Order 12958, as amended	White House	Provides uniform system for classifying, safeguarding, and declassifying national security information, including transnational terrorism
Executive Order 13010	White House	Established the President's Commission on Critical Infrastructure Protection
Executive Order 13228	White House	Information infrastructure protection functions assigned to the OHS
Executive Order 13231	White House	Revoked Executive Order 13010 and established the President's Critical Infrastructure Protection Board, a replacement body for the National Coordinator established by PDD 63
United States Code		
28 U.S.C. §1346, Federal Tort Claims Act	Federal	General waiver of immunity for federal government in tort
42 U.S.C. §5121 et seq., The Stafford Act, 42 U.S.C. §5132, 42 U.S.C. §5185, 42 U.S.C. §5196(d)	Federal, State, Local	Identifies roles, responsibilities in emergencies and major disasters requiring Federal assistance; Illustrates the authority allocated to the President regarding disaster warning; Authorizes the President to establish temporary communications systems; Provides funding for disaster response
50 U.S.C. §401 et seq., The National Security Act	Federal	Provides policies and procedures for DoD components relating to national security issues
50 U.S.C. §1801 et seq., FISA	Federal	Governs the collection of intelligence in the United States
5 U.S.C. §552, 5 U.S.C. §552(b), 5 U.S.C. §552(c)	Federal	Requires federal agencies to release specified information in their control to any person that makes a request in writing that reasonably describes the documents sought. Nine exemptions to the Freedom of Information Act. Three exclusions to the Freedom of Information Act.
18 U.S.C. §2517	Federal	Authorization for disclosure and use of intercepted wire, electronic or oral communications
18 U.S.C. §2518	Federal	Procedure for interception of wire, electronic or oral communications
18 U.S.C. §2520	Federal	Recovery of civil damages for unlawful disclosure of wire, electronic, or oral communication
18 U.S.C. §2702	Federal	Voluntary disclosure of customer communications or records
28 U.S.C. §2680	Federal	Exceptions to the Federal Tort Claims Act; i.e. circumstances under which the United States cannot be named as a defendant in tort actions
42 U.S.C. §2011-§2259	Federal, State, Local	Ensures the proper management of source, special nuclear, and byproduct material
47 U.S.C. §308	FCC	Allows the Federal Communications Commission (FCC) to grant permits and licenses or modify or renew such during a period of war or a national emergency declared by Congress or the President

Reference & Section	Affected Entity	Principal Focus
47 U.S.C. §606	Executive	Authorizes the President, during a current war, to give preference and priority with any communications carrier, as he deems necessary for the national defense and security
USCS Fed. Rules Crim. Proc 6	Federal	Addresses grand jury secrecy
Atty Gen Ashcroft's FOIA Memorandum, Oct 12, 2001	DOJ	Directs agencies to deny any requests for documents at any time that it is legally possible
Pub. L. 107-56, USA PATRIOT Act	Federal, State, Local	Provides the government with enhanced capabilities to share criminal investigative information
Public Law 107-188, Public Health Security and Bioterrorism Preparedness and Response Act of 2002	Federal, State, Local	Authorizes the Secretary to establish an advisory committee named the Emergency Public Information and Communications Advisory Committee
Public Law 107-296, Homeland Security Act; Public Law 107-296, §211-215, Critical Infrastructure Information Act of 2002; Public Law 107-296, §891et seq, Homeland Security Information Sharing Act	Federal, State, Local	Loosened restrictions on the sharing of classified information between Federal departments and agencies. Protects voluntarily shared critical infrastructure information. Directs the President to establish a system whereby homeland security information may be shared among federal agencies, as well as with State and local officials.
CFR		
47 CFR Part 201.2		Defines applicable telecommunications terminology
Department of Defense Directives		
DoDD 5240.1-R, Activities of DoD Intelligence Components that Affect United States Persons	DoD	Provides procedures by DoD Intelligence Components for the "identification, investigation, and reporting of questionable intelligence activities" concerning US citizens
DoDD 5240.1	DoD	Prohibits military components from disseminating information and strictly limits the collection and retention of information about legal U.S. residents
DoDD 5200.27, Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense	DoD	Establishes for the Defense Investigative Program general policy, limitations, procedures, and operational guidance pertaining to the collection, processing, storing and dissemination of information concerning persons and organizations *not* affiliated with the Department of Defense
Case Law		
Douglas Oil Company of CA v. Petrol Stops of Northwest et. Al 441 U.S. 211	Federal, State, Local	Addresses Fed. Rule Crim. Proc. 6(e)(3)(D) regarding grand jury secrecy

I. Introduction

Facilitating communications is a critical function of WMD incident response. A WMD incident may cause significant, widespread damage to telecommunications facilities, hindering efforts to manage the government's response.[1] Moreover, a WMD incident likely will involve a criminal investigation requiring the sharing of criminal investigative information. This could raise the possibility of having to handle and share classified or sensitive information. The uniquely devastating nature of a WMD incident may also cause citizens and non-governmental officials to request or demand information that the government may wish or need to protect. In sum, the need to communicate in the aftermath of a WMD incident will force a tension between the legal authorities and mechanisms that exist to facilitate communications during such contingencies and those authorities and mechanisms in place to protect sensitive or classified information.

This section organizes communications issues regarding a WMD incident into three broad categories:

- Continuity of the Federal government's telecommunications capability;
- Homeland security information sharing between Federal agencies and with State and local officials; and
- Obligations to disclose information to the public versus obligations to protect sensitive or classified information.

II. Ensuring the Continuity of the Government's Telecommunications Capability

A. The National Communications System

A reliable telecommunications infrastructure is necessary to successfully respond to a domestic WMD incident. As the Federal Response Plan recognizes, telecommunications facilities may be severely damaged during a WMD incident and "when the need for real-time electronically processed information is greatest, the capability to acquire it may be seriously restricted or nonexistent."[2] The National Communications System (NCS) is integral to ensuring the Federal government's telecommunications capability. Established by President Kennedy in 1963, the NCS' mission is to assist the President, the National Security Council, the Director of the Office of Science and Technology Policy and the Director of the Office of Management and Budget in: 1) the exercise of telecommunications functions and responsibilities; and 2) coordination of the planning for and provision of national security and emergency preparedness communications capability for the Federal government under all circumstances.

In 1984, President Reagan issued Executive Order 12472, "Assignment of National Security and

[1] The Office of Science and Technology Policy in rules governing the National Communications System defines "telecommunications" as "any transmission, emission, or reception of signs, signals, writing, images, graphics, and sounds or intelligence of any nature by wire, radio, optical, or other electromagnetic systems." 47 CFR §201.2(k).
[2] Interim Federal Response Plan, January 2003, ESF#2-2.

Emergency Preparedness Functions."[3] Executive Order 12472 expanded the membership of the NCS from six members under President Kennedy to an interagency group of 23 Federal departments and agencies with the Secretary of Defense as the Executive Agent. The Homeland Security Act of 2002 transferred the NCS and the Secretary of Defense's executive agent responsibilities to the Department of Homeland Security.[4] Accordingly, the Secretary of Homeland Security is responsible for: assigning a Manager; guaranteeing that NCS prepares and functions properly to assure that both international and domestic national security and emergency preparedness telecommunications needs of the Federal government are met; and ensuring that the NCS acts in compliance with emergency management activities of Federal Emergency Management Agency (FEMA).

The NCS consists of the telecommunications assets of the entities represented on the NCS Committee of Principals. Membership on the Committee of Principals includes Federal agencies, designated by the President, which lease or own telecommunications facilities or services of significance to national security or emergency preparedness. Under Executive Order 12472, the NCS Manager is responsible for developing and maintaining plans for an evolving telecommunications architecture to meet current and Federal government national security and emergency preparedness telecommunications requirements. Additionally, the Manager serves as the focal point for joint industry-government planning, including the dissemination of technical information concerning the national security or emergency preparedness telecommunications requirements of the Federal government.[5]

The NCS is ultimately responsible for ensuring that a national telecommunications infrastructure exists to address the national security and emergency preparedness needs of the President and Federal departments.[6] To fulfill this responsibility, NCS acts as the hub for joint industry-government national security and emergency preparedness telecommunications preparation. Moreover, the NCS maintains a joint industry-government National Coordinating Center that is capable of assisting in the initiation, coordination, restoration, and reconstitution of national security or emergency preparedness telecommunications services under all conditions of crisis or emergency.[7]

Although the NCS' role in the occurrence of a major disaster or emergency is critical, it assigns responsibility to other departments and agencies to secure support and increase the ability to fulfill the national security and emergency preparedness telecommunications needs of the Federal government, State and local governments, private industry and volunteer organizations. The Departments of Homeland Security, Commerce, State, Defense, and Justice, the Central Intelligence Agency, General Services Administration, Federal Communications Commission and other entities of the Federal government all have allocated roles and duties that are to be performed to secure the NCS' response to a major disaster or emergency and ensure.[8]

---

[3] Executive Order 12472, "Assignment of National Security and Emergency Preparedness Telecommunications Functions," April 3, 1984, as amended by Executive Order 13286.
[4] Public Law 107-296, Homeland Security Act of 2002, §201(g) [herein The Homeland Security Act].
[5] Executive Order 12472, *supra* note 3, sec. 1(g).
[6] *Id.* at sec. 1(c).
[7] *Id.* at sec. 1(d).
[8] *Id.*

Another critical component to the NCS is the President's National Security Telecommunications Advisory Committee (NSTAC), established by Executive Order 12382.[9] The NSTAC is composed of no more than 30 members from the nation's telecommunications industry, who have particular knowledge and expertise in the field of telecommunications. The NSTAC is tasked with providing the President with information and advice, from the perspective of the telecommunications industry. The NSTAC provides information and recommendations to the President concerning the viability of employing particular measures in order to enhance the telecommunications facet of our national security position. Additionally, the NSTAC supplies technical information and advice in the recognition and resolution of problems that the Committee determines will influence national security telecommunications capability. The NSTAC periodically reports on the above subjects to the President and to the Secretary of Homeland Security.[10]

B. The National Plan for Telecommunications Support in Non-Wartime Emergencies and the Telecommunications Service Priority System

The National Plan for Telecommunications Support in Non-wartime Emergencies[11] establishes procedures for planning and using national telecommunications assets pursuant to Presidentially-declared major disasters and emergencies under the Stafford Act (discussed in **Paragraph D-1** below). Authority for the Office of Science and Technology Policy (OSTP) to develop the plan derives from Executive Order 12472,[12] which also authorizes the Director of OSTP to provide guidance and assistance to the President and Federal departments and agencies responsible for the provision, management, or allocation of telecommunications resources during non-wartime emergencies.

The impact of the addition of the Initial National Response Plan (NRP) and the Draft National Incident Management System (NIMS) on the provision of telecommunications support during a WMD incident is not yet fully apparent.[13] The Initial NRP seeks to harmonize the operational processes, procedures and protocols detailed in specific Federal interagency incident management plans.[14] However, because the Initial NRP and Draft NIMS do not yet specifically address the provision of telecommunications support in any great detail, it is necessary to refer to the National Plan for Telecommunications Support and its foundational authorities to attain a more detailed sense of the legalities involved with marshalling communications assets to respond to a WMD incident.

During a WMD incident, the Principal Federal Official Representative (PFOR), typically the DHS Regional Administrator, will have a Federal Communications Manager (FCM) under his or her supervision to serve as the single Federal point of contact to the communications industry.[15] In this capacity, the FCM will have responsibility for coordinating the entire Federal emergency

---

[9] Executive Order 12382, President's National Security Telecommunications Advisory Committee, September 13, 1982.
[10] *Id.*
[11] National Plan for Telecommunications Support in Non-Wartime Emergencies, Office of Science and Technology Policy, January 1992.
[12] Executive Order 12472, *supra* note 3.
[13] Draft National Incident Management System, "Initial System," July 18, 2003 [Draft NIMS].
[14] Initial National Response Plan, September 30, 2003, p. 2.
[15] Draft NIMS, *supra* note 13.

telecommunications response in the disaster area.[16] The FCM will evaluate the status of telecommunications in the disaster area and the telecommunications necessary to support the disaster response. Recovery activities will be established utilizing surviving commercial capabilities through the application of Telecommunications Service Priority (TSP) System rules.[17]

Under TSP system rules, service vendors are authorized and required to provide and restore services with TSP assignments before services that do not have such assignments. TSP rules ensure priority treatment of the telecommunications services that serve the United States national security leadership; national security posture; warning the U.S. population; public health, safety, and maintenance of law and order; and public welfare and maintenance of the national economic posture. The Federal Communications Commission (FCC) is responsible for promulgating TSP system rules under authority granted to it by the Communications Act of 1934.[18] The Communications Act of 1934 also grants authority to the President to supersede FCC regulations, including TSP rules, in the event of a disaster or national emergency, and to tailor the provisioning of telecommunications assets to the disaster at hand. [19] It also authorizes the President to provide for the use or control of communications assets by any department of the Government upon just compensation to the owners.[20]

C. Public Health Security and Bioterrorism Preparedness & Response Act of 2002

Section 104 of Public Law 107-188 authorizes the Secretary of Homeland Security to establish the Emergency Public Information and Communications Advisory Committee (EPIC Advisory Committee).[21] This committee advises the Secretary and a working group on preparedness for acts of bioterrorism that was also established by Public Law 107-188. Additionally, the responsibilities of this committee are to find suitable ways to report public health information regarding bioterrorism and other public health emergencies. The EPIC Advisory Committee is comprised of individuals who have particular knowledge and expertise in the fields of public health, medicine, communications, behavioral psychology as well as any other domains deemed suitable by the Secretary. The Secretary is tasked with reviewing the information provided by the EPIC Advisory Committee as well as ensuring that proper information is released to the public.

Also in this section is the call for a study to be conducted by the Secretary of Health and Human Services, in conjunction with the FCC, the National Telecommunications and Information Administration, and other Federal agencies. The objective of the study is to determine "whether local public health entities have the ability to maintain communications in the event of a

---

[16] National Plan for Telecommunications Support in Non-Wartime Emergencies, *supra* note 11, p. 5. Note that although the National Plan delegates authority to the Federal Emergency Communications Coordinator (FECC) for coordinating the entire Federal emergency telecommunications response in the disaster area, the NIMS lists the Federal Communications Manager (FCM) as acting as the sole point of contact with the communications industry. Therefore, it is likely that the FCM will take on the responsibilities of the FECC under the new response structure.
[17] 47 CFR Part 64, App. A, "Telecommunications Service Priority (TSP) System for National Security Emergency Preparedness (NSEP)."
[18] Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 154(i), 201-205 and 303(r).
[19] 47 U.S.C. §606(c) (2002).
[20] 47 U.S.C. §606(e)
[21] Pub. L. 107-188, Public Health Security and Bioterrorism Preparedness and Response Act of 2002, §104.

bioterrorist attack or other public health emergency." It will consider whether more factors are needed in the telecommunications system, especially regarding mobile communications, in order for public health units to maintain systems operability and connectivity during a bioterrorist emergency. The study will also include recommendations to industry and public health entities concerning how to implement the possible additional factors.

D. Authority and Resources to Warn the Public

1. The Stafford Act

The Stafford Act[22] enables the President to marshal communications assets for the purpose of warning civilians endangered by the disaster and to provide communications assistance to State and local governments. Specifically, Section 5132 directs the President to ensure that Federal agencies are prepared to issue warnings of disasters to State and local officials.[23] It allows the President to utilize and to make available to Federal, State, and local agencies, the facilities of the civil defense communications system or any other Federal communications system for the purpose of warning governmental authorities and the civilian population in areas endangered by disasters.[24] The Act also authorizes the President to enter into agreements with officers or agents of private or commercial communications systems who volunteer the use of their systems on a reimbursable or non-reimbursable basis for the purpose of providing warning to governmental authorities and civilian populations endangered by disasters.[25]

Section 5185 authorizes the President to establish temporary communications systems and to make communications available to State and local government officials during, or in anticipation of, an emergency or major disaster.[26] The Act also authorizes the FEMA Director (DHS Under-Secretary for Emergency Preparedness and Response) to provide for emergency preparedness communications and for dissemination of warnings to the civilian population of an emergency.[27]

2. The Homeland Security Advisory System

The government's initiative to expand incident management activities into the Awareness phase within the National Response Plan is evident through the creation of the Homeland Security Advisory System. The Homeland Security Advisory System was established by Homeland Security Presidential Directive 3 (HSPD-3), with the intent to provide a comprehensive, effective means to disseminate information regarding the risk of terrorist acts to Federal, State, and local authorities, as well as to private citizens.[28]

The system is comprised of five Threat Conditions, each identified by a description and corresponding color. The higher the Threat Condition, the greater the risk of a terrorist attack.

---

[22] The Robert T. Stafford Disaster Assistance and Emergency Relief Act, as amended, 42 U.S.C. §5121, *et seq*. (2002).
[23] 42 U.S.C. §5132(a).
[24] 42 U.S.C. §5132(c).
[25] 42 U.S.C. §5132(d).
[26] 42 U.S.C. §5185.
[27] 42 U.S.C. §5196(d).
[28] Homeland Security Presidential Directive 3, "Directive on the Homeland Security Advisory System," March 11, 2002.

The directive defines risk as "probability of an attack occurring and its potential gravity."[29] This system is intended to expedite communicating the nature of the threat, likely targets, and likely actors. The possibility of advance warning can provide some lead time which could allow potential targets to take the protective measures laid out in HSPD-3 which might successfully safeguard their facilities and personnel. If a communications facility is the target, this warning could mean the difference between total system failure and averting such a hazard. The Homeland Security Act of 2002 assigned responsibility for administering the Homeland Security Advisory System to the Under Secretary of Homeland Security for Information Analysis and Infrastructure Protection.[30]

III. Information Sharing among Federal, State, and Local Governments

A. The National Security Act of 1947and Executive Order 12958, as amended

The National Security Act of 1947, as amended, is the foundational document governing access to classified information.[31] Section 435 of the Act required the President to issue procedures governing access to classified information that is binding upon all departments, agencies, and offices of the executive branch of government. Additionally, Classified National Security Information policy has been established through Executive Orders, starting with Executive Order 8381 signed by President Roosevelt in 1940. Executive Order 12958, as amended, is the 9th Executive Order covering this topic. It was first signed by President Clinton in April 1995, and was significantly amended in March 2003 by Executive Order 13292, signed by President George W. Bush.

Classified information is defined as "information that has been determined…to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form."[32] Information may be classified at one of three levels: "Top Secret," "Secret," and "Confidential."[33] Pursuant to Executive Order 12958, one's access to classified information is generally restricted to: 1) receipt of a favorable determination of eligibility for access by an agency head or his or her designee; 2) signature of a non-disclosure agreement by the persons receiving access; and 3) justification of a "need-to-know" about the information.[34] In an emergency situation such as a WMD event, Section 4.2 (b) of Executive Order 12958, as amended, contains a provision that empowers an agency head or his designee to disclose information to those not otherwise eligible for access, with specific outlined limitations.

B. Federal Agencies and Intelligence Information Sharing Guidelines

In the event of a WMD incident, it would be necessary to be able to probe into various sources of

---

[29] *Id.*
[30] The Homeland Security Act, *supra* note 4, §201(d)(7).
[31] 50 U.S.C. §§401– 442 (2002).
[32] Executive Order 12958, "Classified National Security Information," April 17, 1985, as amended.
[33] *Id.,* sec. 1.4. "Top Secret" information is classified as such because the unauthorized disclosure of which could be expected to cause "exceptionally grave damage to the national security" of the United States. "Secret" information is classified as such because the unauthorized disclosure of which could be expected to cause "serious damage to the national security" of the United States. "Confidential" information is classified as such because the unauthorized disclosure of which could be expected to cause "damage to the national security" of the United States.
[34] Executive Order 12958, *supra* note 32, §4.1.

intelligence information in order to determine the likely participants of the attack. Executive Order 12333 and the Foreign Intelligence Surveillance Act (FISA) provide two appropriate avenues for the collection and dissemination of intelligence information.

1. Executive Order 12333

Executive Order 12333 sets out to ensure that the United States will receive the best intelligence available. The objective is to obtain timely and accurate information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons and their agents. In conjunction with the National Security Act of 1947, as amended, EO 12333 helps to provide for the effective conduct of U.S. intelligence activities and the protection of constitutional rights of United States citizens.

The goal of the U.S. intelligence effort is to "provide the President and the National Security Council with the necessary information on which to base decisions concerning the conduct and development of foreign, defense and economic policy, and the protection of United States national interests from foreign security threats."[35] All departments and agencies will cooperate to ensure this goal is met. Specifically, the heads of all Executive Branch departments:

> shall…give the Director of Central Intelligence access to all information relevant to the national intelligence needs of the United States, and shall give due consideration to the requests from the Director of Central Intelligence for appropriate support for Intelligence Community activities.[36]

The goal of such information sharing is that "all agencies and departments should seek to ensure full and free exchange of information in order to derive maximum benefit from the United States intelligence effort."[37] Benefits of information sharing would include enhancing the ability to detect and deter possible actors in a WMD incident.

2. Foreign Intelligence Surveillance Act (FISA)

The Foreign Intelligence Surveillance Act (FISA) governs the collection of intelligence in the United States, protecting the constitutional right to privacy of U.S. citizens.[38] Communications issues involving FISA may arise over the course of WMD incident management if the U.S. government collects, through lawful surveillance of foreign operatives, information on United States persons.

Provisions relevant to WMD incident management are illustrated in several sections within Title 50. Sections 1806(a) and 1825(a) require that information about United States persons collected under FISA be disclosed by Federal officers and employees only if minimization procedures are followed. Minimization procedures, established in 50 U.S.C. §1801(h), demand minimal acquisition and retention of such information and prohibit dissemination of information not available to the public concerning un-consenting United States persons. Similarly, Section 1806(a) pertains to information collected through electronic surveillance, while Section 1825(a) pertains to information collected through physical searches. The disclosure of information

[35] Executive Order 12333, "United States Intelligence Activities," December 4, 1981.
[36] *Id.* at 1.6(a).
[37] *Id.* at 1.1(d).
[38] 50 U.S.C. §1801, *et seq.* (2002).

obtained under FISA is prohibited by sections 1806(b), 1825(c), and1845(b), unless the disclosure is accompanied by a statement pledging that the information will only be used for a criminal proceeding with the advance authorization of the Attorney General. If a physical search involves the residence of a United States person and at any time after the search the Attorney General determines there is no national security interest in continuing to maintain the secrecy of the search, the Attorney General must provide notice to the U.S. person whose residence was searched.[39] If the United States collects information against a U.S. person pursuant to a physical search, pen register, or trap and trace device under FISA, the United States must notify the person that the United States intends to disclose or use the obtained information.[40] If an emergency execution of a physical search is authorized under Section 1824(e) of FISA and the Attorney General does not obtain a subsequent order approving the search, the judge shall notify the U.S. person subject to the search: the fact that the application was made; the period of the search; and the fact that during the period information was or was not obtained.[41]

Most importantly, Section 1825(k) provides Federal officers, who conduct physical searches in order to acquire foreign intelligence information, the authority to consult with Federal, State, or local law enforcement officers to coordinate efforts to investigate or protect against: A) actual or potential attack or other hostile acts by a foreign power against the United States, B) sabotage or international terrorism by a foreign power or its agent, C) clandestine intelligence activities by an intelligence service or network of a foreign power or by a foreign power's agent.[42] This provision facilitates information sharing among federal agencies in order to protect against hostile acts by foreign agents.

Section 1861 provides the FBI with an avenue for obtaining "any tangible thing," including business records, books, and documents for obtaining intelligence information.[43] When the FBI has obtained access to business records to combat terrorism or clandestine intelligence activities under FISA, the persons providing the information are prohibited from disclosing to others that the FBI has sought or obtained such business records.[44]

3. Modifications to FISA by the USA PATRIOT Act

The USA PATRIOT Act (discussed further below in **Paragraph IV**) amended several portions of FISA. One of the more controversial changes involves the extension of search warrant duration. Under the amendment, Section 1805(e) is modified to permit an order for surveillance of a target for a period up to 120 days – an extension of an additional month.[45] Additionally, Section 1824(d) is amended to allow an order for a physical search to be valid for 90 days, doubling the period in which the warrant can be executed.[46] For both of these types of orders, the government can extend the order for up to one year.[47] These modifications permit those

[39] 50 U.S.C. §1825(b).
[40] *Id.* at §1825(d) and §1845(d).
[41] *Id.* at §1825(j).
[42] *Id.* at §1825(k).
[43] *Id.* at §1861(a)(1).
[44] *Id.* at §1861(d).
[45] Pub. L. 107-56, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), §207(a)(1)(B).
[46] *Id.* at §207(a)(2)(A).
[47] *Id.* at §207(b)(1)(B).

investigating a larger window of time in which to gather information and potentially prevent an act of aggression.

Perhaps most relevant to communications issues are the modifications for the use of a pen register or trap and trace device and immunity for compliance with a wiretap under FISA. The language providing authorization for using either device was broadened from "any investigation to gather foreign intelligence information or information concerning international terrorism" to include:

> any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

This language provides a broader basis for authorizing use of these devices to monitor communications by targets. Similarly, the language authorizing the use of these devices during emergencies (Section 403 of FISA) was amended with the same language; thus, broadening the basis for authorization during emergencies as well.

Section 225 of the USA PATRIOT Act modified the basis for immunity for a provider who complies with a FISA wiretap. Under Section 105 of FISA,[48] a clause was added that provides:

> No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance.[49]

By providing immunity to the communication provider, it facilitates the provider's willingness to assist the government in its investigation. An additional result of this amendment is that, because providers will be more cooperative in the investigation, the government will be able to acquire more information regarding the target and therefore will be better able to determine potential plans and actions.

C. Department of Defense Directives Addressing Information Sharing

The Department of Defense (DoD) has established its own procedures for sharing information which is applicable to WMD incident management. As part of its own intelligence gathering procedures, DoD has established criteria for dissemination of information which may ultimately be relevant in managing or determining the source of a WMD incident. By sharing such information, services may be more quickly restored as well as resolving the crisis more rapidly. Additionally, the restrictions placed on dissemination of information ensure that the privacy rights of the person or persons concerned are effectively protected.

Department of Defense Directive (DoDD) 5240.1, originally issued in 1932 and reissued in 1988, provides guidance regarding the various DoD intelligence components ability to "collect,

[48] 50 U.S.C. 1805 (2002).
[49] Pub. L. 107-56, *supra* note 45, §225.

retain, or disseminate information concerning U.S. persons."[50] Specific procedures to be used in such information collection are detailed in DoDD 5240.1-R.[51] Although these directives apply only to intelligence gathering by DoD personnel, this latter Directive does allow dissemination of the information to the "appropriate law enforcement agency" when the investigation "establishes reasonable belief that a crime has been committed."[52] Additionally, under Procedure 4, the Directive further details the criteria to be used in determining when the intelligence information can be shared. The applicable condition for dissemination is when:

> the recipient is reasonably believed to have a need to receive such information for the performance of a lawful governmental function and is… a law enforcement entity of federal, state, or local government and the information may indicate involvement in activities which may violate laws which the recipient is responsible to enforce.[53]

In order to manage the crisis, other Federal, State or local agencies are likely to require the intelligence information gathered by DoD intelligence. Since a WMD incident could constitute a criminal act, the distribution of information would assist not only in later prosecution of the actors, but it would also assist Federal, State, and local authorities in determining the source of the incident and set in motion the restoration of lost services and perhaps prevent further losses.

Another applicable directive is DoDD 5200.27. This directive provides guidance on intelligence gathering procedures, specifically regarding persons and organizations not affiliated with DoD. This directive applies to DoD Components, which consist of: the Office of the Secretary of Defense; Military Departments; Office of the Joint Chiefs of Staff; Unified and Specified Commands; and the defense agencies, but exempts the DoD intelligence components, which are governed by DoDD 5240.1.[54] These DoD components are authorized to gather information which is relevant to defense missions. One applicable mission is to protect DoD Functions and Property.[55] This permits information gathering about "activities threatening defense, military, and civilian personnel and defense activities and installations, including vessels, aircraft, communications equipment, and supplies," which includes: "theft of arms, ammunition, or equipment, or destruction or sabotage of facilities, equipment, or records belonging to DoD units or installations."[56] This directive covers many DoD Functions and Property areas, but by permitting this broad gathering of information, the information obtained will be more accurate and all encompassing, leading to quicker crisis resolution.

D. Atomic Energy Act

The Atomic Energy Act of 1954, as amended, governs the development and control of atomic energy by the United States.[57] One purpose of the Act was to create a program for the dissemination of unclassified scientific and technical information related to atomic energy as

---

[50] DoD Directive 5240.1, "DoD Intelligence Activities," §A. 2, April 25, 1988.
[51] DoD Directive 5240.1-R, "Procedures Governing Activities of DOD Intelligence Components that Affect United States Persons," December 1982.
[52] *Id.*, §A. 3.
[53] *Id.*, B. §2. b.
[54] DoD Directive 5200.27, "Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense," January 7, 1980; see also DoDD 5240.1-R, *supra* note 51.
[55] *Id.,* §4.1.
[56] *Id.*, §§4.1 & 4.1.1.
[57] 42 U.S.C. §§2011-2297 (2002).

well as provide for the control, dissemination, and declassification of Restricted Data.[58] The policy of the Commission (Department Of Energy (DOE)) is characterized in Section 2161, which states that DOE will control the distribution and declassification of Restricted Data in a way that ensures the common defense and security. In order to accomplish this goal, two principles apply:

> i) [u]ntil effective and enforceable international safeguards against the use of atomic energy for destructive purposes have been established by an international arrangement, there shall be no exchange of Restricted Data with other nations except as authorized by section 2164 of this title; and ii) the dissemination of scientific and technical information relating to atomic energy should be permitted and encouraged so as to provide that free interchange of ideas and criticism which is essential to scientific and industrial progress and public understanding and to enlarge the fund of technical information.

The Atomic Energy Act defines "Restricted Data" as "all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category."[59] Access to Restricted Data is contingent upon passage of a background investigation and receipt of an appropriate security clearance.[60] Section 2162 further details the process for the "Classification and Declassification of Restricted Data." Restricted Data and Formerly Restricted Data are excluded from the provisions of Executive Order 12958, as amended (Sec. 6.2 (a)). Periodically the DOE will review the data, with respect to the definition of Restricted Data, in order to determine what can be published. Once data is published, it is declassified and removed from the Restricted Data class. The DOE is also tasked with continuing a review of Restricted Data as well as any Classification Guides distributed.

Determining if Restricted Data relates primarily to the military utilization of atomic weapons lies jointly with the DOE and the DoD. Furthermore, the same two entities are the only authorities involved in the decision to publish the Restricted Data. The decision to publish is determined by whether the possibility that the release of the data would bring about unreasonable risk to the common defense and security. In a case where an agreement cannot be made, the determination lies with the President. The same rules apply when deciding to remove the Restricted Data protections from the category. The decision to release data from the Restricted Data category lies in the data being adequately safeguarded as defense information. No such data removed from the category will be transmitted, or made available, to any nation or regional defense organization, while the same said data is still defense information, unless it applies to another agreement for cooperation entered into in accordance with subsection (b) or (d) of §2164. Lastly, the DOE and the Director of Central Intelligence together will determine removal of information, from the Restricted Data category, concerning the atomic energy programs of other nations. This will be done in order to carry out the provisions of §403(d) of Title 50 and can be safeguarded as defense information.

Information regarding nuclear material is explicitly protected in Section 2167 of Title 42,

[58] 42 U.S.C. §2013(b).
[59] See 42 U.S.C. §2014(y).
[60] 42 U.S.C. §§2163, 2165.

specifically: "confidentiality of certain types of information; issuance of regulations and orders; considerations for exercise of Commission's authority; disclosure of routes and quantities of shipment; civil penalties; withholding of information from Congressional committees."[61] The DOE will determine the parameters, after notice and after the public has had an opportunity to comment, that are obligatory in order to disallow the unauthorized disclosure of protected information that distinctively identifies a licensee's or applicant's detail. Security measures are to be maintained by the DOE with the intention of protecting a possessor of special nuclear material, source material or by product material, wherever the person may be. Furthermore, the DOE is responsible for the physical protection of certain plant equipment vital to the safety of production or utilization facilities involving nuclear materials, as well as its location. It is also responsible for its physical protection when the nuclear material could be stolen or sabotaged.

However, the applicability of the Act to domestic WMD incident management is limited to the involvement of a U.S. nuclear weapon in the incident. That is, the Atomic Energy Act restricts the provision of information to the public that pertains to the design, manufacture, or utilization of atomic weapons or the production of special nuclear material. Consequently, if there is a terrorist attack on U.S. government personnel who have custody of a nuclear weapon, disclosure of information pertaining to the weapon would likely be governed by Subchapter XI of the Act - "Control of Information" - depending on the scenario.[62]

The Atomic Energy Act also grants authority to the Secretary of Energy to promulgate regulations to prohibit dissemination of unclassified information pertaining to facilities design; security measures; or the design manufacture, or utilization of weapon components that were previously declassified or removed from the Restricted Data category if the Secretary of Energy believes that dissemination could result in the illegal production of nuclear weapons or the theft, diversion or sabotage of nuclear materials, equipment, or facilities.[63] Notably, the Atomic Energy Act prescribes criminal penalties for the unlawful communication of Restricted Data with the intent or reason to believe that communication of such information will harm the United States.[64] Due to the likelihood of the presence of Restricted Data, the involvement of a U.S. nuclear weapon in a WMD incident complicates communications during response efforts.

IV. Homeland Security Information Sharing

A. Homeland Security Information Sharing Act: Expanding Information Sharing among Federal Departments and Agencies and with State and Local Personnel

The Homeland Security Information Sharing Act directs the President to establish a system whereby homeland security information may be shared among federal agencies, as well as with State and local officials.[65] The Act defines "homeland security information" as "information possessed by a Federal, State, or local agency that relates to the threat of terrorist activity; relates to the ability to prevent, interdict, or disrupt terrorist activity; would improve the identification or

[61] 42 U.S.C. §2167(a).
[62] 42 U.S.C. §§2161-2169.
[63] 42 U.S.C. 2168.
[64] 42 U.S.C. 2274.
[65] Publ. L. 107-296, *supra* note 4, §§481-484.

investigation of a suspected terrorist or terrorist organization; or would improve the response to a terrorist act."[66] The information sharing procedures to be implemented by the President are to apply to all agencies of the Federal government, including the intelligence community.[67] Further, the Act mandates that substantive requirements for the classification and safeguarding of classified information not be changed by the information sharing procedures that the President establishes.[68]

The Act also seeks to loosen restrictions on sharing classified information and sensitive but unclassified information with State and local personnel. It requires the President to prescribe procedures under which Federal agencies may share "with appropriate State and local personnel" homeland security information that is classified or otherwise protected.[69] With respect to State and local personnel receiving such information, the procedures may require security clearance investigations or entering into nondisclosure agreements.[70] Information shared with State and local personnel must remain under Federal control, notwithstanding State and local laws to the contrary.[71] Once information sharing procedures have been implemented, the head of each Federal agency will be responsible for designating an official responsible for administering procedures pursuant to the Act.

B. Secretary of Homeland Security's Access to Information

The Homeland Security Act of 2002 provides the Secretary of Homeland Security with complete and full access to information related to threats of terrorism against the United States and the United States vulnerabilities to terrorism, except as otherwise directed by the President.[72] It also authorizes the Secretary of Homeland Security to enter into cooperative information sharing arrangements with other Federal departments and agencies while obligating other agencies to supply the Secretary with information pertaining to homeland security even if the Secretary has not already entered into cooperative information sharing agreements.[73]

In addition to the Secretary's broad access to information, the Homeland Security Act treats the Secretary as "a Federal law enforcement, intelligence, protective, national defense, immigration, or national security official" under the USA PATRIOT Act of 2001 (hereinafter PATRIOT Act), Section 2517(6) of Title 18, and Rule 6(e)(3)(C) of the Federal Rules of Criminal Procedure.[74] This designation is significant because it provides the Secretary of Homeland Security with wide access to criminal investigative information. Such access is evidence of the melding of crisis and consequence management functions under the new national response paradigm pursuant to HSPD-5, the NRP and NIMS. Under Title 18, criminal investigative information obtained from any wire, oral, or electronic communication may be shared with the Secretary of Homeland Security.[75] The Federal Rules of Criminal Procedure allow government attorneys to disclose grand-jury information pertaining to foreign intelligence, counterintelligence, or foreign

---

[66] *Id.*, §482(f).
[67] *Id.*, §482(b).
[68] *Id.*, §482(a).
[69] Pub. L. No. 107-296, *supra* note 4, §892(a)(1)(a).
[70] *Id.*,§ 482(c).
[71] *Id.*, §482(e).
[72] *Id.*, §102.
[73] *Id.*, §102(b).
[74] *Id.*, §102(c).
[75] See 18 USC §2517(6).

intelligence information to the Secretary of Homeland Security.[76]

C. Sharing of Criminal Investigative Information Pursuant to the USA PATRIOT Act

1. Sharing Grand Jury Information

The USA PATRIOT Act provides the government with enhanced capabilities to share criminal investigative information within the walls of government. Section 203 of the Act amended Rule 6(e) of the Federal Rules of Criminal Procedure to permit a government attorney to disclose grand-jury matters involving foreign intelligence or counterintelligence to other Federal officials, in order to assist those officials in performing their duties.[77] Disclosures may be made to any federal law enforcement, intelligence, protective, immigration, national defense, or national security official.

The amended Rule 6(e) allows for such disclosures without requiring prior judicial authorization.[78] This is significant because requiring judicial approval prior to such disclosures has been a traditional safeguard of grand jury secrecy. Indeed, the Supreme Court has consistently recognized that the proper functioning of the grand jury system depends upon the secrecy of the grand jury proceedings.[79] Further, the Supreme Court has recognized many interests served by safeguarding the confidentiality of grand jury proceedings. In particular, if grand jury proceedings were made public, many prospective witnesses would be hesitant to come forward voluntarily, knowing that those against whom they testify could become aware of the testimony.[80] Further, witnesses who appeared before the grand jury might be less likely to offer full and frank testimony for fear of retribution and inducements.[81]

Nonetheless, the USA PATRIOT Act's alteration to Rule 6(e) may have minimal impact on the proper functioning of the grand jury system because it limits disclosures to certain government officials and retains the information within the walls of government. Moreover, the amendments to Rule 6(e) are not without logic; if a United States Attorney were to gain information on an upcoming WMD attack over the course of grand jury proceedings, it is sensible that the United States Attorney should share that information immediately with the Federal Bureau of Investigation. In sum, the amended Rule 6(e) merely allows law enforcement to assume a proactive stance towards sharing criminal investigative information to prevent future terrorist attacks.

2. Sharing of Foreign Intelligence and Counterintelligence Information from Wire, Oral, and Electronic Communications

The USA PATRIOT Act also allows for greater sharing of foreign intelligence and

---

[76] Federal Rules of Criminal Procedure, Rule 6(e)(3), December 1, 2001.
[77] Pub. L. No. 107-56, *supra* note 45, §203.
[78] The following subsection was added to Rule 6(e)(3)(D)(ii) by the USA PATRIOT Act: Within a reasonable time after such disclosure, an attorney for the government shall file under seal a notice with the court stating the fact that such information was disclosed and the departments, agencies, or entities to which the disclosure was made. *Id.*, §203(a)(1)(C)(iii).
[79] *Douglas Oil Co. v. Petrol Stops Northwest*, 441 U.S. 211, 218 (1979).
[80] *Id*. at 219.
[81] *Id.*

counterintelligence between government officials obtained through intercepted wire, oral, and electronic communications. Section 203(b) of the Act added a new subsection to Title 18, section 2517 to enable law enforcement officers or government attorneys to disclose information to other Federal law enforcement, intelligence, protective, immigration, national defense, or national security officials.[82] These officials include members of the National Intelligence Council; CIA; NSA; DIA; NIMA; NRO; other offices within DoD that maintain intelligence programs; and the intelligence elements of the Services, the FBI, the Coast Guard, and the Departments of Treasury, Energy, State, and Homeland Security.[83]

Additionally, Section 203(d) states:

> Notwithstanding any other provision of law, it shall be lawful for foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)) or foreign intelligence information obtained as part of a criminal investigation to be disclosed to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties.[84]

This section loosens the restrictions on foreign intelligence information sharing in order to facilitate intergovernmental communication regarding potential threats.

The USA PATRIOT Act allows electronic communication and remote computing service providers to make emergency disclosures of customer electronic communications and customer records to a governmental entity if such disclosures will protect life and limb.[85]

D. Civil Liability

The USA PATRIOT Act also amended the federal criminal code to provide for administrative discipline of Federal officers or employees who violate prohibitions against unauthorized disclosures of information gathered under the PATRIOT Act.[86] Title 18, section 2520 provides for civil damages against persons engaging in the unlawful disclosure of intercepted wire, oral or electronic communications.[87] Thus, the privacy rights of targeted individuals can be protected against unlawful disclosures of information.

Although government officials can be held civilly liable, the code also provides absolute defenses. An absolute defense exists if the official acts with good faith reliance on, among other things, a warrant or statutory authorization or a request by a law enforcement officer who has determined that an emergency situation involving national security exists.[88] These provisions provide greater protection to government officials and facilitate decision-making in times of crisis.

---

[82] Pub. L. 107-56, *supra* note 46, 203(b); 18 U.S.C. §2517(6).
[83] 50 U.S.C. §401(a) (2002).
[84] Pub. L. No. 107-56, *supra* note 46, §206(d).
[85] *Id.,* §212; 18 U.S.C. §2702.
[86] *Id.,* §223.
[87] 18 U.S.C. §2520 (2002).
[88] 18 U.S.C. §2518(7)(a)(ii).

V. Disclosure and Non-Disclosure of Information

A. Public Access to Information: The Freedom of Information Act (FOIA)

The Freedom of Information Act (FOIA) requires Federal agencies to release information in their control to any person that makes a request in writing that reasonably describes the documents sought.[89] There are nine exemptions contained in FOIA that are designed to protect sensitive information. All of the exemptions are relevant in some way to WMD incident management. Exemptions include: 1) information specifically authorized by executive order to be kept secret in the interest of national defense or foreign policy; 2) information the disclosure of which would risk circumvention of a statute or agency regulation; 3) information specifically exempted from disclosure by statute;[90] 4) trade secrets and commercial or financial information obtained from a person; 5) inter-agency or intra-agency memoranda or letters which would not be available by law to a party other than an agency in litigation with the agency; 6) information contained in personnel and medical files and similar files where the release of information would create a clearly unwarranted invasion of privacy; 7) records or information compiled for law enforcement purposes; 8) reports related to the supervision of financial institutions; and 9) geological and geophysical information and data, including maps, concerning wells.[91]

The first exemption applies to classified national security information which is completely exempt from disclosure under FOIA.[92] The second exemption, concerning information related solely to the internal personnel rules and practices of any agency, protects information, the disclosure of which could allow the requestor to circumvent the law.[93] The protection of trade secrets is related to the protection of critical infrastructure, discussed further below. The fifth exemption, privileged interagency or intra-agency memoranda or letters, is significant to the Federal government's information sharing because it ensures candid and complete deliberations without fear that they will be made public.[94] The seventh exemption includes any data which is compiled by the government for any law enforcement purpose. This could include information about suspected terrorists and their targets or the weapons the suspects plan to use – including WMD.

Three exclusions are included in FOIA, in addition to the exemptions. These exclusions permit an agency to treat specified records, otherwise exempt from disclosure, as if FOIA were inapplicable to them. These records include information that is exempt because disclosure could reasonably be expected to interfere with a current law enforcement investigation; informant records maintained by a criminal law enforcement agency under the informant's name or personal identifier; and records maintained by the Federal Bureau of Investigation, which pertain to foreign intelligence, counterintelligence, or international terrorism.[95] An agency need not

---

[89] 5 U.S.C. §552(a)(3)(A).
[90] This exemption is relevant to the Atomic Energy Act, described later in this section.
[91] 5 U.S.C. §552(b).
[92] Executive Order 12958, *supra* note 32. Sec. 6.1(h) defines "classified national security information" as "information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form."
[93] See 141 A.L.R. Fed. 531 (1997) (describing examples of information protected from disclosure under this exemption).
[94] 5 U.S.C. §552(b).
[95] 5 U.S.C. §552(c).

confirm the existence of these specified categories of these records and may respond to a FOIA request for such records with a statement that there are no records, which can be disclosed pertaining to the request.

1. New Standard for Litigating FOIA Disputes

In 2001, Attorney General John Ashcroft issued a Memorandum directing all heads of Federal agencies and departments to carefully consider the "institutional, commercial, and personal privacy interests" that could be implicated when making discretionary decisions regarding disclosure of information under FOIA.[96] More importantly, Ashcroft instituted a "sound legal basis" standard as the threshold for the Department of Justice to defend agencies' discretionary disclosure decisions under FOIA. Prior to the Ashcroft memorandum, agencies dealt with information sharing by considering if there was any "foreseeable harm" in releasing the information to the requesting party.

2. Restrictions on Public Access to Information

Managing the consequences of a WMD incident may demand on-site responders and elements of the federal bureaucracy to have access to classified information or sensitive but unclassified information. Classified information may be in the form of intelligence information, vulnerability and/or threat assessments, operational plans, or technical-scientific information, the disclosure of which would represent a threat to U.S. national security. It is thus necessary to understand the authorities governing access to classified information.

3. Critical Infrastructure Information Act

The Critical Infrastructure Information Act of 2002[97] renders exempt from disclosure under FOIA, proprietary data, related to the nation's critical infrastructure, voluntarily shared with DHS for homeland security purposes. Critical infrastructure is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[98] Accordingly, private functions, such as banking, telecommunications, utilities, and transportation, fall under the definition of the nation's "critical infrastructure."

Because of the importance of these private assets to our national security, DHS officials are seeking information from operators of the private banking, telecommunications, utilities, and transportation infrastructures. The FOIA exemption provided by the Critical Infrastructure Information Act provides the incentive for private operators to disclose such information without fearing that proprietary information will be released to the public. Information being sought by the government includes assessments regarding the security vulnerability of the infrastructure, operational problems or solutions related to the security of the infrastructure, and any threat to the infrastructure.

---

[96] Attorney John Ashcroft's Memorandum for Heads of all Federal Departments and Agencies Regarding The Freedom of Information Act, October 12, 2002.
[97] Pub. L. No. 107-296, *supra* note 4, §§211-215. See 6 U.S.C.A. §133.
[98] *Id.*

B. Disclosure Liability

In order to enhance protection of disclosure decisions by the federal government, the two Acts discussed below contain provisions, which prevent actions against the government. These provisions are critical to ensure the efficient and effective functioning of the government in all situations, but especially during crises. During a WMD incident, government officials will be forced to make the best decisions possible with the facts they have at the time without the benefit of hindsight. In order to regain communications services or to ensure continuity of service, government officials will likely be required to make hasty decisions; facilitating this requirement by protecting them from the possibility of lawsuits is imperative to smooth incident management.

1. The Federal Tort Claims Act

The Federal Tort Claims Act (FTCA) of 1946provides a general waiver of immunity for the Federal government to tort suits.[99] The FTCA's waiver of immunity is subject to thirteen exceptions.[100] The purposes of the exceptions are to "prevent judicial 'second-guessing' of legislative and administrative decisions grounded in social, economic, and political policy through the medium of an action in tort."[101] A complaint that falls within any of these exceptions may not proceed. The exception most applicable to WMD incident management is the "discretionary function" exception. It precludes claims from being brought based upon:

> the act or omission of an employee of the Government, exercising due care, in the execution of a statue or regulation, whether or not such statute or regulations be valid, or based upon the exercise or performance or the failure to exercise or perform a discretionary function or duty on the part of a federal agency or an employee of the Government.[102]

The discretionary function exception covers acts that "involve an element of judgment or choice."[103] The judgment or choice requirement is not satisfied if a "federal statute, regulation, or policy specifically prescribes a course of action for an employee to follow because the employee has no rightful option but to adhere to that directive."[104] Therefore, if a statute, regulation or policy governing WMD incident management affords choice or judgment for the employee to carry out the statute, regulation, or policy, insulation from liability will typically exist.

2. The Stafford Act

Similar to the FTCA, Section 5148 of the Stafford Act, insulates the Federal government and its employees from liability for claims "based upon the exercise or performance of or the failure to exercise or perform a discretionary function or duty" in carrying out the provisions of the Stafford Act.[105] This provision of the Stafford Act encompasses all duties under the Stafford Act, communications functions included. Because WMD incident management will entail judgments under pressure, it is foreseeable that incident management functions will fall into the

---

[99] 28 U.S.C. §§1346, 1402, 1504, 2110, 2401, 2402, 2411, 2412, 2671, 2672, 2674-80.
[100] 28 U.S.C. §2680.
[101] *United States v. S.A. Empresa de Viacao Aerea Rio Grandense,* 467 U.S. 797 at 813 (1984).
[102] 28 U.S.C. §2680(a).
[103] *United States v. Gaubert,* 499 U.S. 315 at 322 (1991), quoting *Berkovitz v. United States,* 486 U.S. 531 at 536 (1988).
[104] *Berkovitz*, *supra* note 103 at 536.
[105] 42 U.S.C. §5148.

"discretionary function" exemption.[106] As illustrated above, the Stafford Act directs the President to ensure the readiness of the Federal agencies to issue warnings to State and local officials, provide technical assistance for effective warnings, use governmental and civil communication systems to issue warnings, and establish temporary communication systems for use by State and local governments.[107] Further, the Act authorizes the FEMA Director (DHS Under-Secretary for Emergency Preparedness and Response) to provide "for necessary emergency preparedness communications and for dissemination of warnings to the civilian population of a hazard."[108] Because the execution of these provisions will ultimately involve policy judgments, any claim challenging the actions of the government will likely be prohibited by the discretionary function exemption.

3. Summary

As this Section has outlined, communications management is critical during national security, WMD, or other emergency situations. Facilitating continuity of communications and information sharing is fundamental to a successful and rapid resolution of the crisis. The various committees, directives, and plans in place provide a solid strategy to delegate functions and responsibilities among the various governmental entities during a communications system failure brought on by a WMD incident. Quick restoration of services will provide exponential benefits in resolving the crisis as a whole, protecting citizens, and seeking out the responsible actors for prosecution.

Since September 11th, various pieces of legislation have been enacted to facilitate government information sharing. The USA PATRIOT Act and Homeland Security Information Sharing Act are examples of how the government's ability to share information at various levels has been enhanced. Citizens are still provided protection for unlawful disclosures because government officials can, in some instances, be held liable. Additionally, FOIA provides access to certain categories of government information for any requesting individual. These sources illustrate the spectrum of issues that could arise in the communication or information-sharing arena during a WMD incident.

---

[106] See Barry Kellmans, *Managing Terrorism's Consequences: Legal Issues*, Memorial Institute for the Prevention of Terrorism, Ch. 4, pg. 5, March 5, 2002.
[107] 42 U.S.C. §§5132, 5185.
[108] 42 U.S.C. §5196(d).

VI. Appendix: Citation Excerpts

Executive Order 12382, September 13,1982

President's National Security Telecommunications Advisory Committee

By the authority vested in me as President by the Constitution of the United States of America, and in order to establish, in accordance with the provisions of the Federal Advisory Committee Act, as amended (5 U.S.C. App. I), an advisory committee on National Security Telecommunications, it is hereby ordered as follows:

Section 1. Establishment. (a) There is established the President's National Security Telecommunications Advisory Committee which shall be composed of no more than 30 members. These members shall have particular knowledge and expertise in the field of telecommunications and represent elements of the Nation's telecommunications industry. Members of the Committee shall be appointed by the President.

(b) The President shall annually designate a Chairman and a Vice Chairman from among the members of the Committee.

(c) To assist the Committee in carrying out its functions, the Committee may establish appropriate subcommittees or working groups composed, in whole or in part, of individuals who are not members of the Committee.

Sec. 2. Functions. (a) The Committee shall provide to the President, among other things, information and advice from the perspective of the telecommunications industry with respect to the implementation of Presidential Directive 53 (PD/NSC - 53), National Security Telecommunications Policy.

(b) The Committee shall provide information and advice to the President regarding the feasibility of implementing specific measures to improve the telecommunications aspects of our national security posture.

(c) The Committee shall provide technical information and advice in the identification and solution of problems which the Committee considers will affect national security telecommunications capability.

(d) In the performance of its advisory duties, the Committee shall conduct reviews and assessments of the effectiveness of the implementation of PD/NSC - 53, National Security Telecommunications Policy.

(e) The Committee shall periodically report on matters in this Section to the President and to the Secretary of Defense in his capacity as Executive Agent for the National Communications System.

Sec. 3. Administration. (a) The heads of Executive agencies shall, to the extent permitted by law, provide the Committee such information with respect to national security telecommunications matters as it may require for the purpose of carrying out its functions. Information supplied to the Committee shall not, to the extent permitted by law, be available for public inspection.

(b) Members of the Committee shall serve without any compensation for their work on the Committee. However, to the extent permitted by law, they shall be entitled to travel expenses, including per diem in lieu of subsistence.

(c) Any expenses of the Committee shall, to the extent permitted by law, be paid from funds available to the Secretary of Defense.

Sec. 4. General. (a) Notwithstanding any other Executive Order, the functions of the President under the Federal Advisory Committee Act, as amended (5 U.S.C. App. I), except that of reporting annually to the Congress, which are applicable to the Committee, shall be performed by the Secretary of Defense, in accord with guidelines and procedures established by the Administrator of General Services.

(b) In accordance with the Federal Advisory Committee Act, as amended, the Committee shall terminate on December 31, 1982, unless sooner extended.

UPDATE

Executive Order 13286, Amendment of Executive Orders, and Other Actions, in Connection With the Transfer of Certain Functions to the Secretary of Homeland Security, February 28, 2003

Sec. 47. Executive Order 12382 of September 13, 1982 (``President's National Security Telecommunications Advisory Committee''), as amended, is further amended by:

(a) inserting ``through the Secretary of Homeland Security,'' after ``the President,'' in sections 2(a) and 2(b);

(b) striking ``and to the Secretary of Defense'' in section 2(e) and inserting ``, through the Secretary of Homeland Security,'' in lieu thereof; and

(c) striking ``the Secretary of Defense'' in sections 3(c) and 4(a) and inserting ``the Secretary of Homeland Security'' in lieu thereof.

Executive Order 13316, Continuance of Certain Federal Advisory Committees, September 23, 2003

Section 1. Each advisory committee listed below is continued until September 30, 2005.

(m) President's National Security Telecommunications Advisory Committee; Executive Order 12382, as amended (Department of Homeland Security).

Executive Order 12333, December 4, 1981

United States Intelligence Activities

This document is included in its entirety on the Deskbook CD-ROM.

Goals, Direction, Duties and Responsibilities With Respect to the National Intelligence Effort

1.1Goals. The United States intelligence effort shall provide the President and the National Security Council with the necessary information on which to base decisions concerning the conduct and development of foreign, defense and economic policy, and the protection of United States national interests from foreign security threats. All departments and agencies shall cooperate fully to fulfill this goal.
(a) Maximum emphasis should be given to fostering analytical competition among appropriate elements of the Intelligence Community.
(b) All means, consistent with applicable United States law and this Order, and with full consideration of the rights of United States persons, shall be used to develop intelligence information for the President and the National Security Council. A balanced approach between technical collection efforts and other means should be maintained and encouraged.
(c) Special emphasis should be given to detecting and countering espionage and other threats and activities directed by foreign intelligence services against the United States Government, or United States corporations, establishments, or persons.
(d) To the greatest extent possible consistent with applicable United States law and this Order, and with full consideration of the rights of United States persons, all agencies and departments should seek to ensure full and free exchange of information in order to derive maximum benefit from the United States intelligence effort.

1.6 Duties and Responsibilities of the Heads of Executive Branch Departments and Agencies.
(a) The heads of all Executive Branch departments and agencies shall, in accordance with law and relevant procedures approved by the Attorney General under this Order, give the Director of Central Intelligence access to all information relevant to the national intelligence needs of the United States, and shall give due consideration to the requests from the Director of Central Intelligence for appropriate support for Intelligence Community activities.

UPDATES

Executive Order 13284, Amendment of Executive Orders, and Other Actions, in Connection With the Establishment of the Department of Homeland Security, January 23, 2003

Sec. 18. Executive Order 12333 of December 4, 1981 (''United States Intelligence Activities''), is amended in Part 3.4(f) by:
(a) striking ''and'' at the end of subpart 3.4(f)(6);
(b) striking the period and inserting ''; and'' at the end of subpart 3.4(f)(7);
and
(c) adding a new subpart 3.4(f)(8) to read as follows: ''(8) Those elements of the Department of Homeland Security that are supervised by the Department's Under Secretary for Information Analysis and Infrastructure Protection through the Department's Assistant Secretary for Information Analysis, with the exception of those functions that involve no analysis of foreign intelligence information.''

Sec. 19. Functions of Certain Officials in the Department of Homeland Security.
The Secretary of Homeland Security, the Deputy Secretary of Homeland Security, the Under Secretary for Information Analysis and Infrastructure Protection, Department of Homeland Security, and the Assistant Secretary for Information Analysis, Department of Homeland Security, each shall be considered a ''Senior Official of the Intelligence Community'' for purposes of Executive Order 12333, and all other relevant authorities, and shall:
(a) recognize and give effect to all current clearances for access to classified information held by those who become employees of the Department of Homeland Security by operation of law pursuant to the Homeland Security Act of 2002 or by Presidential appointment;
(b) recognize and give effect to all current clearances for access to classified information held by those in the private sector with whom employees of the Department of Homeland Security may seek to interact in the discharge of their homeland security-related responsibilities;
(c) make all clearance and access determinations pursuant to Executive Order 12968 of August 2, 1995, or any successor Executive Order, as to employees of, and applicants for employment in, the Department of Homeland Security who do not then hold a current clearance for access to classified information; and
(d) ensure all clearance and access determinations for those in the private sector with whom employees of the Department of Homeland Security may seek to interact in the discharge of their homeland security-related responsibilities are made in accordance with Executive Order 12829 of January 6, 1993.

Executive Order 12472 (1984)

Assignment of National Security and Emergency Preparedness Telecommunications Functions

This document is included in its entirety on the Deskbook CD-ROM.

By the authority vested in me as President by the Constitution and laws of the United States of America, including the Communications Act of 1934, as amended (47 U.S.C. 151), the National Security Act of 1947, as amended, the Defense Production Act of 1950, as amended (50 U.S.C. App. 2061), the Federal Civil Defense Act of 1950, as amended (50 U.S.C. App. 2251), the Disaster Relief Act of 1974 (42 U.S.C. 5121), Section 5 of Reorganization Plan No. 1 of 1977 (3 C.F.R. 197, 1978 Comp.[1]), and Section 203 of Reorganization Plan No. 3 of 1978 (3 C.F.R. 389, 1978 Comp.[2]), and in order to provide for the consolidation of assignment and responsibility for improved execution of national security and emergency preparedness telecommunications functions, it is hereby ordered as follows:

Section 1. The National Communications System.
(a) There is hereby established the National Communications System (NCS). The NCS shall consist of the telecommunications assets of the entities represented on the NCS Committee of Principals and an administrative structure consisting of the Executive Agent, the NCS Committee of Principals and the Manager. The NCS Committee of Principals shall consist of representatives from those Federal departments, agencies or entities, designated by the President, which lease or own telecommunications facilities or services of significance to national security or emergency preparedness, and, to the extent permitted by law, other Executive entities which bear policy, regulatory or enforcement responsibilities of importance to national security or emergency preparedness telecommunications capabilities.
(b) The mission of the NCS shall be to assist the President, the National Security Council, the Director of the Office of Science and Technology Policy and the Director of the Office of Management and Budget in:
(1) the exercise of the telecommunications functions and responsibilities set forth in Section 2 of this Order; and
(2) the coordination of the planning for and provision of national security and emergency preparedness communications for the Federal government under all circumstances, including crisis or emergency, attack, recovery and reconstitution.
(c) The NCS shall seek to ensure that a national telecommunications infrastructure is developed which:
(1) Is responsive to the national security and emergency preparedness needs of the President and the Federal departments, agencies and other entities, including telecommunications in support of national security leadership and continuity of government;
(2) Is capable of satisfying priority telecommunications requirements under all circumstances through use of commercial, government and privately owned telecommunications resources;
(3) Incorporates the necessary combination of hardness, redundancy, mobility, connectivity, interoperability, restorability and security to obtain, to the maximum extent practicable, the survivability of national security and emergency preparedness telecommunications in all circumstances, including conditions of crisis or emergency; and
(4) Is consistent, to the maximum extent practicable, with other national telecommunications policies.
(d) To assist in accomplishing its mission, the NCS shall:
(1) serve as a focal point for joint industry-government national security and emergency preparedness telecommunications planning; and
(2) establish a joint industry-government National Coordinating Center which is capable of assisting in the initiation, coordination, restoration and reconstitution of national security or emergency preparedness telecommunications services or facilities under all conditions of crisis or emergency.
(e) The Secretary of Defense is designated as the Executive Agent for the NCS. The Executive Agent shall:
(1) Designate the Manager of the NCS;
(2) Ensure that the NCS conducts unified planning and operations, in order to coordinate the development and maintenance of an effective and responsive capability for meeting the domestic and international national security and emergency preparedness telecommunications needs of the Federal government;
(3) Ensure that the activities of the NCS are conducted in conjunction with the emergency management activities of the Federal Emergency Management Agency;
(4) Recommend, in consultation with the NCS Committee of Principals, to the National Security Council, the Director of the Office of Science and Technology Policy, or the Director of the Office of Management and Budget, as appropriate:
a. The assignment of implementation or other responsibilities to NCS member entities;
b. New initiatives to assist in the exercise of the functions specified in Section 2; and
c. Changes in the composition or structure of the NCS;
(5) Oversee the activities of and provide personnel and administrative support to the Manager of the NCS;
(6) Provide staff support and technical assistance to the National Security Telecommunications Advisory Committee established by Executive Order No. 12382, as amended; and
(7) Perform such other duties as are from time to time assigned by the President or his authorized designee.

Executive Order 12472 (1984)

(f) The NCS Committee of Principals shall:
(1) Serve as the forum in which each member of the Committee may review, evaluate, and present views, information and recommendations concerning ongoing or prospective national security or emergency preparedness telecommunications programs or activities of the NCS and the entities represented on the Committee;
(2) Serve as the forum in which each member of the Committee shall report on and explain ongoing or prospective telecommunications plans and programs developed or designed to achieve national security or emergency preparedness telecommunications objectives;
(3) Provide comments or recommendations, as appropriate, to the National Security Council, the Director of the Office of Science and Technology Policy, the Director of the Office of Management and Budget, the Executive Agent, or the Manager of the NCS, regarding ongoing or prospective activities of the NCS; and
(4) Perform such other duties as are from time to time assigned by the President or his authorized designee.
(g) The Manager of the NCS shall:
(1) Develop for consideration by the NCS Committee of Principals and the Executive Agent:
a. A recommended evolutionary telecommunications architecture designed to meet current and future Federal government national security and emergency preparedness telecommunications requirements;
b. Plans and procedures for the management, allocation and use, including the establishment of priorities or preferences, of Federally owned or leased telecommunications assets under all conditions of crisis or emergency;
c. Plans, procedures and standards for minimizing or removing technical impediments to the interoperability of government-owned and/or commercially-provided telecommunications systems;
d. Test and exercise programs and procedures for the evaluation of the capability of the Nation's telecommunications resources to meet national security or emergency preparedness telecommunications requirements; and
e. Alternative mechanisms for funding, through the budget review process, national security or emergency preparedness telecommunications initiatives which benefit multiple Federal departments, agencies, or entities. Those mechanisms recommended by the NCS Committee of Principals and the Executive Agent shall be submitted to the Director of the Office of Management and Budget.
(2) Implement and administer any approved plans or programs as assigned, including any system of priorities and preferences for the provision of communications service, in consultation with the NCS Committee of Principals and the Federal Communications Commission, to the extent practicable or otherwise required by law or regulation;
(3) Chair the NCS Committee of Principals and provide staff support and technical assistance thereto;
(4) Serve as a focal point for joint industry-government planning, including the dissemination of technical information, concerning the national security or emergency preparedness telecommunications requirements of the Federal government;
(5) Conduct technical studies or analyses, and examine research and development programs, for the purpose of identifying, for consideration by the NCS Committee of Principals and the Executive Agent, improved approaches which may assist Federal entities in fulfilling national security or emergency preparedness telecommunications objectives;
(6) Pursuant to the Federal Standardization Program of the General Services Administration, and in consultation with other appropriate entities of the Federal government including the NCS Committee of Principals, manage the Federal Telecommunications Standards Program, ensuring wherever feasible that existing or evolving industry, national, and international standards are used as the basis for Federal telecommunications standards; and
(7) Provide such reports and perform such other duties as are from time to time assigned by the President or his authorized designee, the Executive Agent, or the NCS Committee of Principals. Any such assignments of responsibility to, or reports made by, the Manager shall be transmitted through the Executive Agent.

Sec. 2. Executive Office Responsibilities.
(a) Wartime Emergency Functions.
(1) The National Security Council shall provide policy direction for the exercise of the war power functions of the President under Section 606 of the Communications Act of 1934, as amended (47 U.S.C. 606), should the President issue implementing instructions in accordance with the National Emergencies Act (50 U.S.C. 1601).
(2) The Director of the Office of Science and Technology Policy shall direct the exercise of the war power functions of the President under Section 606(a), (c)-(e), of the Communications Act of 1934, as amended (47 U.S.C. 606), should the President issue implementing instructions in accordance with the National Emergencies Act (50 U.S.C. 1601).
(b) Non-Wartime Emergency Functions.
(1) The National Security Council shall:
a. Advise and assist the President in coordinating the development of policy, plans, programs and standards within the Federal government for the identification, allocation, and use of the Nation's telecommunications resources by the Federal government, and by State and local governments, private industry and volunteer organizations upon request, to the extent practicable and otherwise consistent with law, during those crises or emergencies in which the exercise of the President's war power functions is not required or permitted by law; and

Executive Order 12472 (1984)

b. Provide policy direction for the exercise of the President's non-wartime emergency telecommunications functions, should the President so instruct.
(2) The Director of the Office of Science and Technology Policy shall provide information, advice, guidance and assistance, as appropriate, to the President and to those Federal departments and agencies with responsibilities for the provision, management, or allocation of telecommunications resources, during those crises or emergencies in which the exercise of the President's war power functions is not required or permitted by law;
(3) The Director of the Office of Science and Technology Policy shall establish a Joint Telecommunications Resources Board (JTRB) to assist him in the exercise of the functions specified in this subsection. The Director of the Office of Science and Technology Policy shall serve as chairman of the JTRB; select those Federal departments, agencies, or entities which shall be members of the JTRB; and specify the functions it shall perform.
(c) Planning and Oversight Responsibilities.
(1) The National Security Council shall advise and assist the President in:
a. Coordinating the development of policy, plans, programs and standards for the mobilization and use of the Nation's commercial, government, and privately owned telecommunications resources, in order to meet national security or emergency preparedness requirements;
b. Providing policy oversight and direction of the activities of the NCS; and
c. Providing policy oversight and guidance for the execution of the responsibilities assigned to the Federal departments and agencies by this Order.
(2) The Director of the Office of Science and Technology Policy shall make recommendations to the President with respect to the test, exercise and evaluation of the capability of existing and planned communications systems, networks or facilities to meet national security or emergency preparedness requirements and report the results of any such tests or evaluations and any recommended remedial actions to the President and to the National Security Council;
(3) The Director of the Office of Science and Technology Policy or his designee shall advise and assist the President in the administration of a system of radio spectrum priorities for those spectrum dependent telecommunications resources of the Federal government which support national security or emergency preparedness functions. The Director also shall certify or approve priorities for radio spectrum use by the Federal government, including the resolution of any conflicts in or among priorities, under all conditions of crisis or emergency; and
(4) The National Security Council, the Director of the Office of Science and Technology Policy and the Director of the Office of Management and Budget shall, in consultation with the Executive Agent for the NCS and the NCS Committee of Principals, determine what constitutes national security and emergency preparedness telecommunications requirements.
(d) *Consultation with Federal Departments and Agencies.* In performing the functions assigned under this Order, the National Security Council and the Director of the Office of Science and Technology Policy, in consultation with each other, shall:
(1) Consult, as appropriate, with the Director of the Office of Management and Budget; the Director of the Federal Emergency Management Agency with respect to the emergency management responsibilities assigned pursuant to Executive Order No. 12148, as amended; the Secretary of Commerce, with respect to responsibilities assigned pursuant to Executive Order No. 12046; the Secretary of Defense, with respect to communications security responsibilities assigned pursuant to Executive Order No. 12333; and the Chairman of the Federal Communications Commission or his authorized designee; and
(2) Establish arrangements for consultation among all interested Federal departments, agencies or entities to ensure that the national security and emergency preparedness communications needs of all Federal government entities are identified; that mechanisms to address such needs are incorporated into pertinent plans and procedures; and that such needs are met in a manner consistent, to the maximum extent practicable, with other national telecommunications policies.
(e) *Budgetary Guidelines.* The Director of the Office of Management and Budget, in consultation with the National Security Council and the NCS, will prescribe general guidelines and procedures for reviewing the financing of the NCS within the budgetary process and for preparation of budget estimates by participating agencies. These guidelines and procedures may provide for mechanisms for funding, through the budget review process, national security and emergency preparedness telecommunications initiatives which benefit multiple Federal departments, agencies, or entities.

Sec. 3. *Assignment of Responsibilities to Other Departments and Agencies.* In order to support and enhance the capability to satisfy the national security and emergency preparedness telecommunications needs of the Federal government, State and local governments, private industry and volunteer organizations, under all circumstances including those of crisis or emergency, the Federal departments and agencies shall perform the following functions:
(a) *Department of Commerce.* The Secretary of Commerce shall, for all conditions of crisis or emergency:
(1) Develop plans and procedures concerning radio spectrum assignments, priorities and allocations for use by Federal departments, agencies and entities; and
(2) Develop, maintain and publish policy, plans, and procedures for the control and allocation of frequency assignments, including the authority to amend, modify or revoke such assignments, in those parts of the electromagnetic spectrum assigned to the Federal

Executive Order 12472 (1984)

government.
(b) *Federal Emergency Management Agency.* The Director of the Federal Emergency Management Agency shall:
(1) Plan for and provide, operate and maintain telecommunications services and facilities, as part of its National Emergency Management System, adequate to support its assigned emergency management responsibilities;
(2) Advise and assist State and local governments and volunteer organizations, upon request and to the extent consistent with law, in developing plans and procedures for identifying and satisfying their national security or emergency preparedness telecommunications requirements;
(3) Ensure, to the maximum extent practicable, that national security and emergency preparedness telecommunications planning by State and local governments and volunteer organizations is mutually supportive and consistent with the planning of the Federal government; and
(4) Develop, upon request and to the extent consistent with law and in consonance with regulations promulgated by and agreements with the Federal Communications Commission, plans and capabilities for, and provide policy and management oversight of, the Emergency Broadcast System, and advise and assist private radio licensees of the Commission in developing emergency communications plans, procedures and capabilities.
(c) *Department of State.* The Secretary of State, in accordance with assigned responsibilities within the Diplomatic Telecommunications System, shall plan for and provide, operate and maintain rapid, reliable and secure telecommunications services to those Federal entities represented at United States diplomatic missions and consular offices overseas. This responsibility shall include the provision and operation of domestic telecommunications in support of assigned national security or emergency preparedness responsibilities.
(d) *Department of Defense.* In addition to the other responsibilities assigned by this Order, the Secretary of Defense shall:
(1) Plan for and provide, operate and maintain telecommunications services and facilities adequate to support the National Command Authorities and to execute the responsibilities assigned by Executive Order No. 12333; and
(2) Ensure that the Director of the National Security Agency provides the technical support necessary to develop and maintain plans adequate to provide for the security and protection of national security and emergency preparedness telecommunications.
(e) *Department of Justice.* The Attorney General shall, as necessary, review for legal sufficiency, including consistency with the antitrust laws, all policies, plans or procedures developed pursuant to responsibilities assigned by this Order.
(f) *Central Intelligence Agency.* The Director of Central Intelligence shall plan for and provide, operate, and maintain telecommunications services adequate to support its assigned responsibilities, including the dissemination of intelligence within the Federal government.
(g) *General Services Administration.* Except as otherwise assigned by this Order, the Administrator of General Services, consistent with policy guidance provided by the Director of the Office of Management and Budget, shall ensure that Federally owned or managed domestic communications facilities and services meet the national security and emergency preparedness requirements of the Federal civilian departments, agencies and entities.
(h) *Federal Communications Commission.* The Federal Communications Commission shall, consistent with Section 4(c) of this Order:
(1) Review the policies, plans and procedures of all entities licensed or regulated by the Commission that are developed to provide national security or emergency preparedness communications services, in order to ensure that such policies, plans and procedures are consistent with the public interest, convenience and necessity;
(2) Perform such functions as required by law with respect to all entities licensed or regulated by the Commission, including (but not limited to) the extension, discontinuance or reduction of common carrier facilities or services; the control of common carrier rates, charges, practices and classifications; the construction, authorization, activation, deactivation or closing of radio stations, services and facilities; the assignment of radio frequencies to Commission licensees; the investigation of violations of pertinent law and regulation; and the initiation of appropriate enforcement actions;
(3) Develop policy, plans and procedures adequate to execute the responsibilities assigned in this Order under all conditions or crisis or emergency; and
(4) Consult as appropriate with the Executive Agent for the NCS and the NCS Committee of Principals to ensure continued coordination of their respective national security and emergency preparedness activities.
(i) All Federal departments and agencies, to the extent consistent with law (including those authorities and responsibilities set forth in Section 4(c) of this Order), shall:
(1) Determine their national security and emergency preparedness telecommunications requirements, and provide information regarding such requirements to the Manager of the NCS;
(2) Prepare policies, plans and procedures concerning telecommunications facilities, services or equipment under their management or operational control to maximize their capability of responding to the national security or emergency preparedness needs of the Federal government;
(3) Provide, after consultation with the Director of the Office of Management and Budget, resources to support their respective requirements for national security and emergency preparedness telecommunications; and provide personnel and staff support to the Manager of the NCS as required by the President;
(4) Make information available to, and consult with, the Manager of the NCS regarding agency telecommunications activities in support of

Executive Order 12472 (1984)

national security or emergency preparedness;
(5) Consult, consistent with the provisions of Executive Order No. 12046, as amended, and in conjunction with the Manager of the NCS, with the Federal Communications Commission regarding execution of responsibilities assigned by this Order;
(6) Submit reports annually, or as otherwise requested, to the Manager of the NCS, regarding agency national security or emergency preparedness telecommunications activities; and
(7) Cooperate with and assist the Executive Agent for the NCS, the NCS Committee of Principals, the Manager of the NCS, and other departments and agencies in the execution of the functions set forth in this Order, furnishing them such information, support and assistance as may be required.
(j) Each Federal department or agency shall execute the responsibilities assigned by this Order in conjunction with the emergency management activities of the Federal Emergency Management Agency, and in regular consultation with the Executive Agent for the NCS and the NCS Committee of Principals to ensure continued coordination of NCS and individual agency telecommunications activities.

Sec. 4. General Provisions.
(a) All Executive departments and agencies may issue such rules and regulations as may be necessary to carry out the functions assigned under this Order.
(b) In order to reflect the assignments of responsibility provided by this Order,
(1) Sections 2-414, 4-102, 4-103, 4-202, 4-302, 5-3, and 6-101 of Executive Order No. 12046, as amended, are revoked;
(2) The Presidential Memorandum of August 21, 1963, as amended, entitled "Establishment of the National Communications System", is hereby superseded; and
(3) [Deleted]
(c) Nothing in this Order shall be deemed to affect the authorities or responsibilities of the Director of the Office of Management and Budget, or any Office or official thereof; or reassign any function assigned any agency under the Federal Property and Administrative Services Act of 1949, as amended; or under any other law; or any function vested by law in the Federal Communications Commission.
[Sec. 4(b)(3) amends Executive Order 12046 of Mar. 27, 1978, Chapter 47. The amendment has been incorporated into that order.]
Sec. 5. This Order shall be effective upon publication in the Federal Register.[3]

[1] Note: The citation is 3 CFR 1977 Comp., p. 198.
[2] Note: The citation is 3 CFR 1978 Comp., p. 330.
[3] Note: Published in the Federal Register of April 5, 1984.

UPDATE

Executive Order 13286, Executive Order Amendment of Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security, February 28, 2003

Sec. 46. Executive Order 12472 of April 3, 1984 ("Assignment of National Security and Emergency Preparedness Telecommunications Functions"), is amended by:
(a) inserting "the Homeland Security Council," after "National Security Council," in sections 1(b), 1(e)(4), 1(f)(3), and 2(c)(4);
(b) striking "The Secretary of Defense" in section 1(e) and inserting "The Secretary of Homeland Security" in lieu thereof;
(c) striking "Federal Emergency Management Agency" in sections 1(e)(3) and 3(j) and inserting "Department of Homeland Security" in lieu thereof;
(d) inserting ", in consultation with the Homeland Security Council," after "National Security Council" in section 2(b)(1);
(e) inserting ", the Homeland Security Council," after "National Security Council" in sections 2(d) and 2(e);
(f) striking "the Director of the Federal Emergency Management Agency" in section 2(d)(1) and inserting "the Secretary of Homeland Security" in lieu thereof;
(g) striking "Federal Emergency Management Agency. The Director of the Federal Emergency Management Agency shall:" in section 3(b) and inserting "Department of Homeland Security. The Secretary of Homeland Security shall:" in lieu thereof; and
(h) adding at the end of section 3(d) the following new paragraph: "(3) Nothing in this order shall be construed to impair or otherwise affect the authority of the Secretary of Defense with respect to the Department of Defense, including the chain of command for the armed forces of the United States under section 162(b) of title 10, United States Code, and the authority of the Secretary of Defense with respect to the Department of Defense under section 113(b) of that title."

Executive Order 13010, July 15, 1996

Critical Infrastructure Protection

Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government.

Threats to these critical infrastructures fall into two categories: physical threats to tangible property ("physical threats"), and threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures ("cyber threats"). Because

many of these critical infrastructures are owned and operated by the private sector, it is essential that the government and private sector work together to develop a strategy for protecting them and assuring their

continued operation.

NOW, THEREFORE, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. *Establishment.* There is hereby established the President's Commission on Critical Infrastructure Protection ("Commission").

(a) *Chair.* A qualified individual from outside the Federal Government shall be appointed by the President to serve as Chair of the Commission. The Commission Chair shall be employed on a full-time basis.

(b) *Members.* The head of each of the following executive branch departments and agencies shall nominate not more than two full-time members of the Commission:

(i) Department of the Treasury;
(ii) Department of Justice;
(iii) Department of Defense;
(iv) Department of Commerce;
(v) Department of Transportation;
(vi) Department of Energy;
(vii) Central Intelligence Agency;
(viii) Federal Emergency Management Agency;
(ix) Federal Bureau of Investigation;
(x) National Security Agency.

One of the nominees of each agency may be an individual from outside the Federal Government who shall be employed by the agency on a fulltime basis. Each nominee must be approved by the Steering Committee.

Sec. 2. *The Principals Committee.* The Commission shall report to the President through a Principals Committee ("Principals Committee"), which shall review any reports or recommendations before submission to the President. The Principals Committee shall comprise the:

(i) Secretary of the Treasury;
(ii) Secretary of Defense;
(iii) Attorney General;
(iv) Secretary of Commerce;
(v) Secretary of Transportation;
(vi) Secretary of Energy;
(vii) Director of Central Intelligence;
(viii) Director of the Office of Management and Budget;
(ix) Director of the Federal Emergency Management Agency;
(x) Assistant to the President for National Security Affairs;
(xi) Assistant to the Vice President for National Security Affairs.

Sec. 3. *The Steering Committee of the President's Commission on Critical Infrastructure Protection.* A Steering Committee ("Steering Committee") shall oversee the work of the Commission on behalf of the Principals Committee. The Steering Committee shall comprise four members appointed by the President. One of the members shall be the Chair of the Commission and one shall be an employee of the Executive Office of the President. The Steering Committee will receive regular reports on the progress of the Commission's work and approve the submission of reports to the Principals Committee.

Sec. 4. *Mission.* The Commission shall: (a) within 30 days of this order, produce a statement of its mission objectives, which will elaborate the general objectives set forth in this order, and a detailed schedule for addressing each mission objective, for approval by the Steering Committee;

(b) identify and consult with: (i) elements of the public and private sectors that conduct, support, or contribute to infrastructure assurance; (ii) owners and operators of the critical infrastructures; and (iii) other elements of the public and private sectors, including the Congress,

Executive Order 13010, July 15, 1996

that have an interest in critical infrastructure assurance issues and that may have differing perspectives on these issues;
(c) assess the scope and nature of the vulnerabilities of, and threats to, critical infrastructures;
(d) determine what legal and policy issues are raised by efforts to protect critical infrastructures and assess how these issues should be addressed;
(e) recommend a comprehensive national policy and implementation strategy for protecting critical infrastructures from physical and cyber threats and assuring their continued operation;
(f) propose any statutory or regulatory changes necessary to effect its recommendations; and
(g) produce reports and recommendations to the Steering Committee as they become available; it shall not limit itself to producing one final report.
Sec. 5. Advisory Committee to the President's Commission on Critical Infrastructure
Protection. (a) The Commission shall receive advice from an advisory committee ("Advisory Committee") composed of no more than ten individuals appointed by the President from the private sector who are knowledgeable about critical infrastructures. The Advisory Committee shall advise the Commission on the subjects of the Commission's mission in whatever manner the Advisory Committee, the Commission Chair, and the Steering Committee deem appropriate.
(b) A Chair shall be designated by the President from among the members of the Advisory Committee.
(c) The Advisory Committee shall be established in compliance with the Federal Advisory Committee Act, as amended (5 U.S.C. App.). The Department of Defense shall perform the functions of the President under the Federal Advisory Committee Act for the Advisory Committee, except that of reporting to the Congress, in accordance with the guidelines and procedures established by the Administrator of General Services.
Sec. 6. *Administration.* (a) All executive departments and agencies shall cooperate with the Commission and provide such assistance, information, and advice to the Commission as it may request, to the extent permitted by law.
(b) The Commission and the Advisory Committee may hold open and closed hearings, conduct inquiries, and establish subcommittees, as necessary.
(c) Members of the Advisory Committee shall serve without compensation for their work on the Advisory Committee. While engaged in the work of the Advisory Committee, members may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in the government service.
(d) To the extent permitted by law, and subject to the availability of appropriations, the Department of Defense shall provide the Commission and the Advisory Committee with administrative services, staff, other support services, and such funds as may be necessary for the performance of its functions and shall reimburse the executive branch components that provide representatives to the Commission for the compensation of those representatives.
(e) In order to augment the expertise of the Commission, the Department of Defense may, at the Commission's request, contract for the services of nongovernmental consultants who may prepare analyses, reports, background papers, and other materials for consideration by the Commission. In addition, at the Commission's request, executive departments and agencies shall request that existing Federal advisory committees consider and provide advice on issues of critical infrastructure protection, to the extent permitted by law.
(f) The Commission, the Principals Committee, the Steering Committee, and the Advisory Committee shall terminate 1 year from the date of this order, unless extended by the President prior to that date.
Sec. 7. *Interim Coordinating Mission.* (a) While the Commission is conducting its analysis and until the President has an opportunity to consider and act on its recommendations, there is a need to increase coordination of existing infrastructure protection efforts in order to better address, and prevent, crises that would have a debilitating regional or national impact. There is hereby established an Infrastructure Protection Task Force ("IPTF") within the Department of Justice, chaired by the Federal Bureau of Investigation, to undertake this interim coordinating mission.
(b) The IPTF will not supplant any existing programs or organizations.
(c) The Steering Committee shall oversee the work of the IPTF.
(d) The IPTF shall include at least one full-time member each from the Federal Bureau of Investigation, the Department of Defense, and the National Security Agency. It shall also receive part-time assistance from other executive branch departments and agencies. Members shall be designated by their departments or agencies on the basis of their expertise in the protection of critical infrastructures. IPTF members' compensation shall be paid by their parent agency or department.
(e) The IPTF's function is to identify and coordinate existing expertise, inside and outside of the Federal Government, to:
(i) provide, or facilitate and coordinate the provision of, expert guidance to critical infrastructures to detect, prevent, halt, or confine an attack and to recover and restore service;
(ii) issue threat and warning notices in the event advance information is obtained about a threat;
(iii) provide training and education on methods of reducing vulnerabilities and responding to attacks on critical infrastructures;
(iv) conduct after-action analysis to determine possible future threats, targets, or methods of attack; and
(v) coordinate with the pertinent law enforcement authorities during or after an attack to facilitate any resulting criminal investigation.
(f) All executive departments and agencies shall cooperate with the IPTF and provide such assistance, information, and advice as the

Executive Order 13010, July 15, 1996
IPTF may request, to the extent permitted by law. (g) All executive departments and agencies shall share with the IPTF information about threats and warning of attacks, and about actual attacks on critical infrastructures, to the extent permitted by law. (h) The IPTF shall terminate no later than 180 days after the termination of the Commission, unless extended by the President prior to that date. Sec. 8. *General.* (a) This order is not intended to change any existing statutes or Executive orders. (b) This order is not intended to create any right, benefit, trust, or responsibility, substantive or procedural, enforceable at law or equity by a party against the United States, its agencies, its officers, or any person.
UPDATE
Executive Order 13138, Continuance of Certain Federal Advisory Committees, September 30, 1999
Sec. 3. The following Executive orders, or sections thereof, which established committees that have terminated and whose work is completed, are revoked: (c) Section 5 and that part of section 6(f) of Executive Order 13010, as amended by section 3 of Executive Order 13025, Executive Order 13041, sections 1, 2, and that part of section 3 of Executive Order 13064, and Executive Order 13077, establishing the Advisory Committee to the President's Commission on Critical Infrastructure Protection

Executive Order 13231, October 16, 2001

Critical Infrastructure Protection in the Information Age

This document is included in its entirety on the Deskbook CD-ROM.

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to ensure protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems, in the information age, it is hereby ordered as follows:

Section 1. Policy.
(a) The information technology revolution has changed the way business is transacted, government operates, and national defense is conducted. Those three functions now depend on an interdependent network of critical information infrastructures. The protection program authorized by this order shall consist of continuous efforts to secure information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems. Protection of these systems is essential to the telecommunications, energy, financial services, manufacturing, water, transportation, health care, and emergency services sectors.
(b) It is the policy of the United States to protect against disruption of the operation of information systems for critical infrastructure and thereby help to protect the people, economy, essential human and government services, and national security of the United States, and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible. The implementation of this policy shall include a voluntary public-private partnership, involving corporate and nongovernmental organizations.

Sec. 2. Scope. To achieve this policy, there shall be a senior executive branch board to coordinate and have cognizance of Federal efforts and programs that relate to protection of information systems and involve:
(a) cooperation with and protection of private sector critical infrastructure, State and local governments' critical infrastructure, and supporting programs in corporate and academic organizations;
(b) protection of Federal departments' and agencies' critical infrastructure;
and
(c) related national security programs.

Sec. 3. Establishment. I hereby establish the ''President's Critical Infrastructure Protection Board'' (the ''Board'').

UPDATES

Executive Order 13284, Amendment of Executive Orders, and Other Actions, in Connection With the Establishment of the Department of Homeland Security, January 23, 2003

Sec. 2. Executive Order 13231 of October 16, 2001 (''Critical Infrastructure Protection in the Information Age''), is amended by:
(a) inserting ''(i) Secretary of Homeland Security;'' after ''or their designees:'' in section 6(a); and
(b) renumbering the subsequent subsections in section 6(a) appropriately.

Executive Order 13286, Amendment of Executive Orders, and Other Actions, in Connection With the Transfer of Certain Functions to the Secretary of Homeland Security.

Sec. 7. Executive Order 13231 of October 16, 2001 (''Critical Infrastructure Protection in the Information Age''), as amended, is further amended to read in its entirety as follows:
''Critical Infrastructure Protection in the Information Age"
By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to ensure protection of information systems for critical infrastructure, including emergency preparedness communications and the physical assets that support such systems, in the information age, it is hereby ordered as follows:

Section 1. Policy. The information technology revolution has changed the way business is transacted, government operates, and national defense is conducted. Those three functions now depend on an interdependent network of critical information infrastructures. It is the policy of the United States to protect against disruption of the operation of information systems for critical infrastructure and thereby help to protect the people, economy, essential human and government services, and national security of the United States, and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible. The implementation of this policy shall include a voluntary public-private partnership, involving corporate and nongovernmental organizations.

Sec. 2. Continuing Authorities. This order does not alter the existing authorities or roles of United States Government departments and agencies. Authorities set forth in 44 U.S.C. chapter 35, and other applicable law, provide senior officials with responsibility for the security of Federal Government information systems.
(a) Executive Branch Information Systems Security. The Director of the Office of Management and Budget (OMB) has the responsibility

Executive Order 13231, October 16, 2001

Critical Infrastructure Protection in the Information Age

to develop and oversee the implementation of government-wide policies, principles, standards, and guidelines for the security of information systems that support the executive branch departments and agencies, except those noted in section 2(b) of this order. The Director of OMB shall advise the President and the appropriate department or agency head when there is a critical deficiency in the security practices within the purview of this section in an executive branch department or agency.

(b) National Security Information Systems. The Secretary of Defense and the Director of Central Intelligence (DCI) shall have responsibility to oversee, develop, and ensure implementation of policies, principles, standards, and guidelines for the security of information systems that support the operations under their respective control. In consultation with the Assistant to the President for National Security Affairs and the affected departments and agencies, the Secretary of Defense and the DCI shall develop policies, principles, standards, and guidelines for the security of national security information systems that support the operations of other executive branch departments and agencies with national security information.

(i) Policies, principles, standards, and guidelines developed under this subsection may require more stringent protection than those developed in accordance with section 2(a) of this order.
(ii) The Assistant to the President for National Security Affairs shall advise the President and the appropriate department or agency when there is a critical deficiency in the security practices of a department or agency within the purview of this section.
(iii) National Security Systems. The National Security Telecommunications and Information Systems Security Committee, as established byand consistent with NSD–42 and chaired by the Department of Defense, shall be designated as the ''Committee on National Security Systems.''

(c) Additional Responsibilities. The heads of executive branch departments and agencies are responsible and accountable for providing and maintaining adequate levels of security for information systems, including emergency preparedness communications systems, for programs under their control. Heads of such departments and agencies shall ensure the development and, within available appropriations, funding of programs that adequately address these mission systems, especially those critical systems that support the national security and other essential government programs. Additionally, security should enable, and not unnecessarily impede, department and agency business operations.

Sec. 3. The National Infrastructure Advisory Council. The National Infrastructure Advisory Council (NIAC), established on October 16, 2001, shall provide the President through the Secretary of Homeland Security with advice on the security of information systems for critical infrastructure supporting other sectors of the economy: banking and finance, transportation, energy, manufacturing, and emergency government services.
(a) Membership. The NIAC shall be composed of not more than 30 members appointed by the President. The members of the NIAC shall be selected from the private sector, academia, and State and local government. Members of the NIAC shall have expertise relevant to the functions of the NIAC and generally shall be selected from industry Chief Executive Officers (and equivalently ranked leaders of other organizations) with responsibilities for security of information infrastructure supporting the critical sectors of the economy, including banking and finance, transportation, energy, communications, and emergency government services. Members shall not be full-time officials or employees of the executive branch of the Federal Government. The President shall designate a Chair and Vice Chair from among the members of the NIAC.

(b) Functions of the NIAC. The NIAC will meet periodically to: (i) enhance the partnership of the public and private sectors in protecting information systems for critical infrastructures and provide reports on this issue to the Secretary of Homeland Security, as appropriate;
(ii) propose and develop ways to encourage private industry to perform periodic risk assessments of critical information and telecommunications systems;
(iii) monitor the development of private sector Information Sharing and Analysis Centers (ISACs) and provide recommendations to the President through the Secretary of Homeland Security on how these organizations can best foster improved cooperation among the ISACs, the Department of Homeland Security, and other Federal Government entities;
(iv) report to the President through the Secretary of Homeland Security, who shall ensure appropriate coordination with the Assistant to the President for Homeland Security, the Assistant to the President for Economic Policy, and the Assistant to the President for National Security Affairs under the terms of this order; and
(v) advise lead agencies with critical infrastructure responsibilities, sector coordinators, the Department of Homeland Security, and the ISACs.

(c) Administration of the NIAC.
(i) The NIAC may hold hearings, conduct inquiries, and establish subcommittees, as appropriate.

Executive Order 13231, October 16, 2001
Critical Infrastructure Protection in the Information Age
(ii) Upon request of the Chair, and to the extent permitted by law, the heads of the executive departments and agencies shall provide the NIAC with information and advice relating to its functions. (iii) Senior Federal Government officials may participate in the meetings of the NIAC, as appropriate. (iv) Members shall serve without compensation for their work on the NIAC. However, members may be reimbursed for travel expenses, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in Federal Government service (5 U.S.C. 5701–5707). (v) To the extent permitted by law and subject to the availability of appropriations, the Department of Homeland Security shall provide the NIAC with administrative services, staff, and other support services, and such funds as may be necessary for the performance of the NIAC's functions. (d) General Provisions. (i) Insofar as the Federal Advisory Committee Act, as amended (5 U.S.C. App.) (Act), may apply to the NIAC, the functions of the President under that Act, except that of reporting to the Congress, shall be performed by the Department of Homeland Security in accordance with the guidelines and procedures established by the Administrator of General Services. (ii) The NIAC shall terminate on October 15, 2003, unless extended by the President. (iii) Executive Order 13130 of July 14, 1999, was revoked on October 16, 2001. (iv) Nothing in this order shall supersede any requirement made by or under law. Sec. 4. Judicial Review. This order does not create any right or benefit, substantive or procedural, enforceable at law or in equity, against the United States, its depart ments, agencies, or other entities, its officers or employees, or any other person.''
Executive Order 13316, September 17, 2003
Section 1. Each advisory committee listed below is continued until September 30, 2005. (a) Committee for the Preservation of the White House; Executive Order 11145, as amended (Department of the Interior). (b) National Infrastructure Advisory Council; Section 3 of Executive Order 13231, as amended (Department of Homeland Security).

Executive Order 12958, as amended by Executive Order 13292 of March 25, 2003

Classified National Security Information

This document is included in its entirety on the Deskbook CD-ROM.

Purpose:
Prescribes a uniform system for classifying, safeguarding, and declassifying national security information.

UPDATES: None

Executive Order 13228, October 8, 2001

Establishing the Office of Homeland Security and the Homeland Security Council

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:
Section 1. Establishment. I hereby establish within the Executive Office of the President an Office of Homeland Security (the "Office") to be headed by the Assistant to the President for Homeland Security.

Sec. 2. Mission. The mission of the Office shall be to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks. The Office shall perform the functions necessary to carry out this mission, including the functions specified in section 3 of this order.

Sec. 3. Functions. The functions of the Office shall be to coordinate the executive branch's efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States.
(a) National Strategy. The Office shall work with executive departments and agencies, State and local governments, and private entities to ensure the adequacy of the national strategy for detecting, preparing for, preventing, protecting against, responding to, and recovering from terrorist threats or attacks within the United States and shall periodically review and coordinate revisions to that strategy as necessary.
(b) Detection. The Office shall identify priorities and coordinate efforts for collection and analysis of information within the United States regarding threats of terrorism against the United States and activities of terrorists or terrorist groups within the United States. The Office also shall identify, in coordination with the Assistant to the President for National Security Affairs, priorities for collection of intelligence outside the United States regarding threats of terrorism within the United States.
(i) In performing these functions, the Office shall work with Federal, State, and local agencies, as appropriate, to:
(A) facilitate collection from State and local governments and private entities of information pertaining to terrorist threats or activities within the United States;
(B) coordinate and prioritize the requirements for foreign intelligence relating to terrorism within the United States of executive departments and agencies responsible for homeland security and provide these requirements and priorities to the Director of Central Intelligence and other agencies responsible for collection of foreign intelligence;
(C) coordinate efforts to ensure that all executive departments and agencies that have intelligence collection responsibilities have sufficient technological capabilities and resources to collect intelligence and data relating to terrorist activities or possible terrorist acts within the United States, working with the Assistant to the President for National Security Affairs, as appropriate;
(D) coordinate development of monitoring protocols and equipment for use in detecting the release of biological, chemical, and radiological hazards; and
(E) ensure that, to the extent permitted by law, all appropriate and necessary intelligence and law enforcement information relating to homeland security is disseminated to and exchanged among appropriate executive departments and agencies responsible for homeland security and, where appropriate for reasons of homeland security, promote exchange of such information with and among State and local governments and private entities.
(ii) Executive departments and agencies shall, to the extent permitted by law, make available to the Office all information relating to terrorist threats and activities within the United States.
(c) Preparedness. The Office of Homeland Security shall coordinate national efforts to prepare for and mitigate the consequences of terrorist threats or attacks within the United States. In performing this function, the Office shall work with Federal, State, and local agencies, and private entities, as appropriate, to:
(i) review and assess the adequacy of the portions of all Federal emergency response plans that pertain to terrorist threats or attacks within the United States;

Executive Order 13228, October 8, 2001

(ii) coordinate domestic exercises and simulations designed to assess and practice systems that would be called upon to respond to a terrorist threat or attack within the United States and coordinate programs and activities for training Federal, State, and local employees who would be called upon to respond to such a threat or attack;
(iii) coordinate national efforts to ensure public health preparedness for a terrorist attack, including reviewing vaccination policies and reviewing the adequacy of and, if necessary, increasing vaccine and pharmaceutical stockpiles and hospital capacity;
(iv) coordinate Federal assistance to State and local authorities and nongovernmental organizations to prepare for and respond to terrorist threats or attacks within the United States;
(v) ensure that national preparedness programs and activities for terrorist threats or attacks are developed and are regularly evaluated under appropriate standards and that resources are allocated to improving and sustaining preparedness based on such evaluations; and
(vi) ensure the readiness and coordinated deployment of Federal response teams to respond to terrorist threats or attacks, working with the Assistant to the President for National Security Affairs, when appropriate.
(d) Prevention. The Office shall coordinate efforts to prevent terrorist attacks within the United States. In performing this function, the Office shall work with Federal, State, and local agencies, and private entities, as appropriate, to:
(i) facilitate the exchange of information among such agencies relating to immigration and visa matters and shipments of cargo; and, working with the Assistant to the President for National Security Affairs, ensure coordination among such agencies to prevent the entry of terrorists and terrorist materials and supplies into the United States and facilitate removal of such terrorists from the United States, when appropriate;
(ii) coordinate efforts to investigate terrorist threats and attacks within the United States; and
(iii) coordinate efforts to improve the security of United States borders, territorial waters, and airspace in order to prevent acts of terrorism within the United States, working with the Assistant to the President for National Security Affairs, when appropriate.
(e) Protection. The Office shall coordinate efforts to protect the United States and its critical infrastructure from the consequences of terrorist attacks. In performing this function, the Office shall work with Federal, State, and local agencies, and private entities, as appropriate, to:
(i) strengthen measures for protecting energy production, transmission, and distribution services and critical facilities; other utilities; telecommunications; facilities that produce, use, store, or dispose of nuclear material; and other critical infrastructure services and critical facilities within the United States from terrorist attack;
(ii) coordinate efforts to protect critical public and privately owned information systems within the United States from terrorist attack;
(iii) develop criteria for reviewing whether appropriate security measures are in place at major public and privately owned facilities within the United States;
(iv) coordinate domestic efforts to ensure that special events determined by appropriate senior officials to have national significance are protected from terrorist attack;
(v) coordinate efforts to protect transportation systems within the United States, including railways, highways, shipping, ports and waterways, and airports and civilian aircraft, from terrorist attack;
(vi) coordinate efforts to protect United States livestock, agriculture, and systems for the provision of water and food for human use and consumption from terrorist attack; and
(vii) coordinate efforts to prevent unauthorized access to, development of, and unlawful importation into the United States of, chemical, biological, radiological, nuclear, explosive, or other related materials that have the potential to be used in terrorist attacks.
(f) Response and Recovery. The Office shall coordinate efforts to respond to and promote recovery from terrorist threats or attacks within the United States. In performing this function, the Office shall work with Federal, State, and local agencies, and private entities, as appropriate, to:
(i) coordinate efforts to ensure rapid restoration of transportation systems, energy production, transmission, and distribution systems; telecommunications; other utilities; and other critical infrastructure facilities after disruption by a terrorist threat or attack;
(ii) coordinate efforts to ensure rapid restoration of public and private critical information systems after disruption by a terrorist threat or attack;
(iii) work with the National Economic Council to coordinate efforts to stabilize United States financial markets after a terrorist threat or attack and manage the immediate economic and financial consequences of the incident;
(iv) coordinate Federal plans and programs to provide medical, financial, and other assistance to victims of terrorist attacks and their families; and
(v) coordinate containment and removal of biological, chemical, radiological, explosive, or other hazardous materials in the event of a terrorist threat or attack involving such hazards and coordinate efforts to mitigate the effects of such an attack.
(g) Incident Management. The Assistant to the President for Homeland Security shall be the individual primarily responsible for coordinating the domestic response efforts of all departments and agencies in the event of an imminent terrorist threat and during and in the immediate aftermath of a terrorist attack within the United States and shall be the principal point of contact for and to the President with respect to coordination of such efforts. The Assistant to the President for Homeland Security shall coordinate with the Assistant to the President for National Security Affairs, as appropriate.

Executive Order 13228, October 8, 2001

(h) Continuity of Government. The Assistant to the President for Homeland Security, in coordination with the Assistant to the President for National Security Affairs, shall review plans and preparations for ensuring the continuity of the Federal Government in the event of a terrorist attack that threatens the safety and security of the United States Government or its leadership.

(i) Public Affairs. The Office, subject to the direction of the White House Office of Communications, shall coordinate the strategy of the executive branch for communicating with the public in the event of a terrorist threat or attack within the United States. The Office also shall coordinate the development of programs for educating the public about the nature of terrorist threats and appropriate precautions and responses.

(j) Cooperation with State and Local Governments and Private Entities. The Office shall encourage and invite the participation of State and local governments and private entities, as appropriate, in carrying out the Office's functions.

(k) Review of Legal Authorities and Development of Legislative Proposals. The Office shall coordinate a periodic review and assessment of the legal authorities available to executive departments and agencies to permit them to perform the functions described in this order. When the Office determines that such legal authorities are inadequate, the Office shall develop, in consultation with executive departments and agencies, proposals for presidential action and legislative proposals for submission to the Office of Management and Budget to enhance the ability of executive departments and agencies to perform those functions. The Office shall work with State and local governments in assessing the adequacy of their legal authorities to permit them to detect, prepare for, prevent, protect against, and recover from terrorist threats and attacks.

(l) Budget Review. The Assistant to the President for Homeland Security, in consultation with the Director of the Office of Management and Budget (the "Director") and the heads of executive departments and agencies, shall identify programs that contribute to the Administration's strategy for homeland security and, in the development of the President's annual budget submission, shall review and provide advice to the heads of departments and agencies for such programs. The Assistant to the President for Homeland Security shall provide advice to the Director on the level and use of funding in departments and agencies for homeland security-related activities and, prior to the Director's forwarding of the proposed annual budget submission to the President for transmittal to the Congress, shall certify to the Director the funding levels that the Assistant to the President for Homeland Security believes are necessary and appropriate for the homeland security-related activities of the executive branch.

Sec. 4. Administration.

(a) The Office of Homeland Security shall be directed by the Assistant to the President for Homeland Security.

(b) The Office of Administration within the Executive Office of the President shall provide the Office of Homeland Security with such personnel, funding, and administrative support, to the extent permitted by law and subject to the availability of appropriations, as directed by the Chief of Staff to carry out the provisions of this order.

(c) Heads of executive departments and agencies are authorized, to the extent permitted by law, to detail or assign personnel of such departments and agencies to the Office of Homeland Security upon request of the Assistant to the President for Homeland Security, subject to the approval of the Chief of Staff.

Sec. 5. Establishment of Homeland Security Council.

(a) I hereby establish a Homeland Security Council (the "Council"), which shall be responsible for advising and assisting the President with respect to all aspects of homeland security. The Council shall serve as the mechanism for ensuring coordination of homeland security-related activities of executive departments and agencies and effective development and implementation of homeland security policies.

(b) The Council shall have as its members the President, the Vice President, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Secretary of Health and Human Services, the Secretary of Transportation, the Director of the Federal Emergency Management Agency, the Director of the Federal Bureau of Investigation, the Director of Central Intelligence, the Assistant to the President for Homeland Security, and such other officers of the executive branch as the President may from time to time designate. The Chief of Staff, the Chief of Staff to the Vice President, the Assistant to the President for National Security Affairs, the Counsel to the President, and the Director of the Office of Management and Budget also are invited to attend any Council meeting. The Secretary of State, the Secretary of Agriculture, the Secretary of the Interior, the Secretary of Energy, the Secretary of Labor, the Secretary of Commerce, the Secretary of Veterans Affairs, the Administrator of the Environmental Protection Agency, the Assistant to the President for Economic Policy, and the Assistant to the President for Domestic Policy shall be invited to attend meetings pertaining to their responsibilities. The heads of other executive departments and agencies and other senior officials shall be invited to attend Council meetings when appropriate.

(c) The Council shall meet at the President's direction. When the President is absent from a meeting of the Council, at the President's direction the Vice President may preside. The Assistant to the President for Homeland Security shall be responsible, at the President's direction, for determining the agenda, ensuring that necessary papers are prepared, and recording Council actions and Presidential

Executive Order 13228, October 8, 2001

decisions.
Sec. 6. Original Classification Authority. I hereby delegate the authority to classify information originally as Top Secret, in accordance with Executive Order 12958 or any successor Executive Order, to the Assistant to the President for Homeland Security.
Sec. 7. Continuing Authorities. This order does not alter the existing authorities of United States Government departments and agencies. All executive departments and agencies are directed to assist the Council and the Assistant to the President for Homeland Security in carrying out the purposes of this order.
Sec. 8. General Provisions.
(a) This order does not create any right or benefit, substantive or procedural, enforceable at law or equity by a party against the United States, its departments, agencies or instrumentalities, its officers or employees, or any other person.
(b) References in this order to State and local governments shall be construed to include tribal governments and United States territories and other possessions.
(c) References to the "United States" shall be construed to include United States territories and possessions.
Sec. 9. Amendments to Executive Order 12656. Executive Order 12656 of November 18, 1988, as amended, is hereby further amended as follows:
(a) Section 101(a) is amended by adding at the end of the fourth sentence: ", except that the Homeland Security Council shall be responsible for administering such policy with respect to terrorist threats and attacks within the United States."
(b) Section 104(a) is amended by adding at the end: ", except that the Homeland Security Council is the principal forum for consideration of policy relating to terrorist threats and attacks within the United States."
(c) Section 104(b) is amended by inserting the words "and the Homeland Security Council" after the words "National Security Council."
(d) The first sentence of section 104(c) is amended by inserting the words "and the Homeland Security Council" after the words "National Security Council."
(e) The second sentence of section 104(c) is replaced with the following two sentences: "Pursuant to such procedures for the organization and management of the National Security Council and Homeland Security Council processes as the President may establish, the Director of the Federal Emergency Management Agency also shall assist in the implementation of and management of those processes as the President may establish. The Director of the Federal Emergency Management Agency also shall assist in the implementation of national security emergency preparedness policy by coordinating
with the other Federal departments and agencies and with State and local governments, and by providing periodic reports to the National Security Council and the Homeland Security Council on implementation of national security emergency preparedness policy."
(f) Section 201(7) is amended by inserting the words "and the Homeland Security Council" after the words "National Security Council."
(g) Section 206 is amended by inserting the words "and the Homeland Security Council" after the words "National Security Council."
(h) Section 208 is amended by inserting the words "or the Homeland Security Council" after the words "National Security Council."
THE WHITE HOUSE, October 8, 2001.

Source: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2001_register&docid=fr10oc01-144.pdf

UPDATE:

Executive Order 13284, Amendment of Executive Orders, and Other Actions, in Connection With the Establishment of the Department of Homeland Security, January 23, 2003

Sec. 3. Executive Order 13228 of October 8, 2001 (''Establishing the Office of Homeland Security and the Homeland Security Council''), is amended by inserting ''the Secretary of Homeland Security,'' after ''the Secretary of Transportation,'' in section 5(b). Further, during the period from January 24, 2003, until March 1, 2003, the Secretary of Homeland Security shall have the responsibility for coordinating the domestic response efforts otherwise assigned to the Assistant to the President for Homeland Security pursuant to section 3(g) of Executive Order 13228.

Executive Order 13286, Amendment of Executive Orders, and Other Actions, in Connection With the Transfer of Certain Functions to the Secretary of Homeland Security, February 28, 2003

Sec. 8. Executive Order 13228 of October 8, 2001 (''Establishing the Office of Homeland Security and the Homeland Security Council''), as amended, is further amended by:
(a) amending section 3(g) to read ''(g) Incident Management. Consistent with applicable law, including the statutory functions of the Secretary of Homeland Security, the Assistant to the President for Homeland Security shall be the official primarily responsible for advising and assisting the President in the coordination of domestic incident management activities of all departments and agencies in the event of a terrorist threat, and during and in the aftermath of terrorist attacks, major disasters, or other emergencies, within the United States. Generally, the Assistant to the President for Homeland Security shall serve as the principal point of contact for and to the President with respect to the coordination of such activities. The Assistant to the President for Homeland Security shall coordinate with the Assistant to the President for National Security Affairs, as appropriate.''; and
(b) inserting '', including the Department of Homeland Security'' after ''Government departments and agencies'' in section 7.

Homeland Security Presidential Directive-3, March 12, 2002

Homeland Security Advisory System

This document is included in its entirety on the Deskbook CD-ROM.

Purpose

The Nation requires a Homeland Security Advisory System to provide a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to Federal, State, and local authorities and to the American people. Such a system would provide warnings in the form of a set of graduated "Threat Conditions" that would increase as the risk of the threat increases. At each Threat Condition, Federal departments and agencies would implement a corresponding set of "Protective Measures" to further reduce vulnerability or increase response capability during a period of heightened alert.

This system is intended to create a common vocabulary, context, and structure for an ongoing national discussion about the nature of the threats that confront the homeland and the appropriate measures that should be taken in response. It seeks to inform and facilitate decisions appropriate to different levels of government and to private citizens at home and at work.

Homeland Security Advisory System

The Homeland Security Advisory System shall be binding on the executive branch and suggested, although voluntary, to other levels of government and the private sector. There are five Threat Conditions, each identified by a description and corresponding color. From lowest to highest, the levels and colors are:

Low = Green;
Guarded = Blue;
Elevated = Yellow;
High = Orange;
Severe = Red.

The higher the Threat Condition, the greater the risk of a terrorist attack. Risk includes both the probability of an attack occurring and its potential gravity. Threat Conditions shall be assigned by the Attorney General in consultation with the Assistant to the President for Homeland Security. Except in exigent circumstances, the Attorney General shall seek the views of the appropriate Homeland Security Principals or their subordinates, and other parties as appropriate, on the Threat Condition to be assigned. Threat Conditions may be assigned for the entire Nation, or they may be set for a particular geographic area or industrial sector. Assigned Threat Conditions shall be reviewed at regular intervals to determine whether adjustments are warranted.

For facilities, personnel, and operations inside the territorial United States, all Federal departments, agencies, and offices other than military facilities shall conform their existing threat advisory systems to this system and henceforth administer their systems consistent with the determination of the Attorney General with regard to the Threat Condition in effect.

The assignment of a Threat Condition shall prompt the implementation of an appropriate set of Protective Measures. Protective Measures are the specific steps an organization shall take to reduce its vulnerability or increase its ability to respond during a period of heightened alert. The authority to craft and implement Protective Measures rests with the Federal departments and agencies. It is recognized that departments and agencies may have several preplanned sets of responses to a particular Threat Condition to facilitate a rapid, appropriate, and tailored response. Department and agency heads are responsible for developing their own Protective Measures and other antiterrorism or self-protection and continuity plans, and resourcing, rehearsing, documenting, and maintaining these plans. Likewise, they retain the authority to respond, as necessary, to risks, threats, incidents, or events at facilities within the specific jurisdiction of their department or agency, and, as authorized by law, to direct agencies and industries to implement their own Protective Measures. They shall continue to be responsible for taking all appropriate proactive steps to reduce the vulnerability of their personnel and facilities to terrorist attack. Federal department and agency heads shall submit an annual written report to the President, through the Assistant to the President for Homeland Security, describing the steps they have taken to develop and implement appropriate Protective Measures for each Threat Condition. Governors, mayors, and the leaders of other organizations are encouraged to conduct a similar review of their organizations= Protective Measures.

The decision whether to publicly announce Threat Conditions shall be made on a case-by-case basis by the Attorney General in consultation with the Assistant to the President for Homeland Security. Every effort shall be made to share as much information regarding the threat as possible, consistent with the safety of the Nation. The Attorney General shall ensure, consistent with the safety of the Nation, that State and local government officials and law enforcement authorities are provided the most relevant and timely information. The Attorney General shall be responsible for identifying any other information developed in the threat assessment process that would be useful to State and local officials and others and conveying it to them as permitted consistent with the constraints of classification. The Attorney General shall establish a process and a system for conveying relevant information to Federal, State, and local government officials, law enforcement authorities, and the private sector expeditiously.

The Director of Central Intelligence and the Attorney General shall ensure that a continuous and timely flow of integrated threat assessments and reports is provided to the President, the Vice President, Assistant to the President and Chief of Staff, the Assistant to the President for Homeland Security, and the Assistant to the President for National Security Affairs. Whenever possible and practicable,

Homeland Security Presidential Directive-3, March 12, 2002

these integrated threat assessments and reports shall be reviewed and commented upon by the wider interagency community.
A decision on which Threat Condition to assign shall integrate a variety of considerations. This integration will rely on qualitative assessment, not quantitative calculation. Higher Threat Conditions indicate greater risk of a terrorist act, with risk including both probability and gravity. Despite best efforts, there can be no guarantee that, at any given Threat Condition, a terrorist attack will not occur. An initial and important factor is the quality of the threat information itself. The evaluation of this threat information shall include, but not be limited to, the following factors:

1. To what degree is the threat information credible?
2. To what degree is the threat information corroborated?
3. To what degree is the threat specific and/or imminent?
4. How grave are the potential consequences of the threat?
5.

Threat Conditions and Associated Protective Measures
The world has changed since September 11, 2001. We remain a Nation at risk to terrorist attacks and will remain at risk for the foreseeable future. At all Threat Conditions, we must remain vigilant, prepared, and ready to deter terrorist attacks. The following Threat Conditions each represent an increasing risk of terrorist attacks. Beneath each Threat Condition are some suggested Protective Measures, recognizing that the heads of Federal departments and agencies are responsible for developing and implementing appropriate agency-specific Protective Measures:
Low Condition (Green). This condition is declared when there is a low risk of terrorist attacks. Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures they develop and implement:
Refining and exercising as appropriate preplanned Protective Measures;
Ensuring personnel receive proper training on the Homeland Security Advisory System and specific preplanned department or agency Protective Measures; and
Institutionalizing a process to assure that all facilities and regulated sectors are regularly assessed for vulnerabilities to terrorist attacks, and all reasonable measures are taken to mitigate these vulnerabilities.
Guarded Condition (Blue). This condition is declared when there is a general risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Condition, Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement:
Checking communications with designated emergency response or command locations;
Reviewing and updating emergency response procedures; and
Providing the public with any information that would strengthen its ability to act appropriately.
Elevated Condition (Yellow). An Elevated Condition is declared when there is a significant risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Conditions, Federal departments and agencies should consider the following general measures in addition to the Protective Measures that they will develop and implement:
Increasing surveillance of critical locations;
Coordinating emergency plans as appropriate with nearby jurisdictions;
Assessing whether the precise characteristics of the threat require the further refinement of preplanned Protective Measures; and
Implementing, as appropriate, contingency and emergency response plans.
High Condition (Orange). A High Condition is declared when there is a high risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Conditions, Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement:
Coordinating necessary security efforts with Federal, State, and local law enforcement agencies or any National Guard or other appropriate armed forces organizations;
Taking additional precautions at public events and possibly considering alternative venues or even cancellation;
Preparing to execute contingency procedures, such as moving to an alternate site or dispersing their workforce; and
Restricting threatened facility access to essential personnel only.
Severe Condition (Red). A Severe Condition reflects a severe risk of terrorist attacks. Under most circumstances, the Protective Measures for a Severe Condition are not intended to be sustained for substantial periods of time. In addition to the Protective Measures in the previous Threat Conditions, Federal departments and agencies also should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement:

- Increasing or redirecting personnel to address critical emergency needs;
- Assigning emergency response personnel and pre-positioning and mobilizing specially trained teams or resources;
- Monitoring, redirecting, or constraining transportation systems; and
- Closing public and government facilities.

Comment and Review Periods

Homeland Security Presidential Directive-3, March 12, 2002
The Attorney General, in consultation and coordination with the Assistant to the President for Homeland Security, shall, for 45 days from the date of this directive, seek the views of government officials at all levels and of public interest groups and the private sector on the proposed Homeland Security Advisory System. One hundred thirty-five days from the date of this directive the Attorney General, after consultation and coordination with the Assistant to the President for Homeland Security, and having considered the views received during the comment period, shall recommend to the President in writing proposed refinements to the Homeland Security Advisory System.
Source: http://www.mipt.org/pdd-hspd3.asp
UPDATE
HSPD-5, Management of Domestic Incidents, February 28, 2003
Technical and Conforming Amendments to Homeland Security Presidential Directive-3 (HSPD-3) (24) The Homeland Security Act of 2002 assigned the responsibility for administering the Homeland Security Advisory System to the Secretary of Homeland Security. Accordingly, HSPD-3 of March 11, 2002 ("Homeland Security Advisory System") is amended as follows: (a) replacing the third sentence of the second paragraph entitled "Homeland Security Advisory System" with "Except in exigent circumstances, the Secretary of Homeland Security shall seek the views of the Attorney General, and any other federal agency heads the Secretary deems appropriate, including other members of the Homeland Security Council, on the Threat Condition to be assigned." (b) inserting "At the request of the Secretary of Homeland Security, the Department of Justice shall permit and facilitate the use of delivery systems administered or managed by the Department of Justice for the purposes of delivering threat information pursuant to the Homeland Security Advisory System." as a new paragraph after the fifth paragraph of the section entitled "Homeland Security Advisory System." (c) inserting ", the Secretary of Homeland Security" after "The Director of Central Intelligence" in the first sentence of the seventh paragraph of the section entitled "Homeland Security Advisory System". (d) striking "Attorney General" wherever it appears (except in the sentences referred to in subsections (a) and (c) above), and inserting "the Secretary of Homeland Security" in lieu thereof; and (e) striking the section entitled "Comment and Review Periods."

5 U.S.C. §552 (2002)

Freedom Of Information Act (FOIA)

This document is included in its entirety on the Deskbook CD-ROM.

(b) This section does not apply to matters that are -
(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and
(B) are in fact properly classified pursuant to such Executive order;
(2) related solely to the internal personnel rules and practices of an agency;
(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute
(A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or
(B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;
(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information
(A) could reasonably be expected to interfere with enforcement proceedings,
(B) would deprive a person of a right to a fair trial or an impartial adjudication,
(C) could reasonably be expected to constitute an unwarranted invasion of personal privacy,
(D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source,
(E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or
(F) could reasonably be expected to endanger the life or physical safety of any individual;
(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
(9) geological and geophysical information and data, including maps, concerning wells.
Any reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt under this subsection. The amount of information deleted shall be indicated on the released portion of the record, unless including that indication would harm an interest protected by the exemption in this subsection under which the deletion is made. If technically feasible, the amount of the information deleted shall be indicated at the place in the record where such deletion is made.
(c)
(1) Whenever a request is made which involves access to records described in subsection (b)(7)(A) and -
(A) the investigation or proceeding involves a possible violation of criminal law; and
(B) there is reason to believe that
(i) the subject of the investigation or proceeding is not aware of its pendency, and
(ii) disclosure of the existence of the records could reasonably be expected to interfere with enforcement proceedings, the agency may, during only such time as that circumstance continues, treat the records as not subject to the requirements of this section.
(2) Whenever informant records maintained by a criminal law enforcement agency under an informant's name or personal identifier are requested by a third party according to the informant's name or personal identifier, the agency may treat the records as not subject to the requirements of this section unless the informant's status as an informant has been officially confirmed.
(3) Whenever a request is made which involves access to records maintained by the Federal Bureau of Investigation pertaining to foreign intelligence or counterintelligence, or international terrorism, and the existence of the records is classified information as provided in subsection (b)(1), the Bureau may, as long as the existence of the records remains classified information, treat the records as not subject to the requirements of this section.

UPDATE

Pub. L. 107-306, Intelligence Authorization Act for Fiscal Year 2003, Nov. 27, 2002

Amended by sec. 312, 116 Stat. 2390.

Pub. L. 108-7, Consolidated Appropriations Resolution, 2003

New Note added by section 644.

18 U.S.C. §2517 (2002)
Authorization for disclosure and use of intercepted wire, oral, or electronic communications
Sec. 2517. (1) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived there from, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure. (2) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication or evidence derived there from may use such contents to the extent such use is appropriate to the proper performance of his official duties. (3) Any person who has received, by any means authorized by this chapter, any information concerning a wire, oral, or electronic communication, or evidence derived there from intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof. (4) No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character. (5) When an investigative or law enforcement officer, while engaged in intercepting wire, oral, or electronic communications in the manner authorized herein, intercepts wire, oral, or electronic communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived there from, may be disclosed or used as provided in subsections (1) and (2) of this section. Such contents and any evidence derived there from may be used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable. (6) Any investigative or law enforcement officer, or attorney for the Government, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived there from, may disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), or foreign intelligence information (as defined in subsection (19) of section 2510 of this title), to assist the official who is to receive that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information
UPDATE:
Pub. L. 107-296,The Homeland Security Act of 2002
Amended by Pub. L. 107-296, sec. 896 Note amended by Pub. L. 107-296, sec. 897(b)

18 U.S.C. §2518, 2002
Procedure for interception of wire, oral, or electronic communications
This document is included in its entirety on the Deskbook CD-ROM. Purpose: Outlines procedure for authorization of wire, oral, or electronic communications.
UPDATE: None

18 U.S.C. §2520 (2002)

Recovery of civil damages authorized

Sec. 2520.
(a) In General. -
Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.
(b) Relief. -
In an action under this section, appropriate relief includes -
(1) such preliminary and other equitable or declaratory relief as may be appropriate;
(2) damages under subsection (c) and punitive damages in appropriate cases; and
(3) a reasonable attorney's fee and other litigation costs reasonably incurred.
(c) Computation of Damages. -
(1) In an action under this section, if the conduct in violation of this chapter is the private viewing of a private satellite video communication that is not scrambled or encrypted or if the communication is a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the court shall assess damages as follows:
(A) If the person who engaged in that conduct has not previously been enjoined under section 2511(5) and has not been found liable in a prior civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $50 and not more than $500.
(B) If, on one prior occasion, the person who engaged in that conduct has been enjoined under section 2511(5) or has been found liable in a civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $100 and not more than $1000.
(2) In any other action under this section, the court may assess as damages whichever is the greater of -
(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or
(B) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.
(d) Defense. - A good faith reliance on -
(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;
(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or
(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;
is a complete defense against any civil or criminal action brought under this chapter or any other law.
(e) Limitation. -
A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.
(f) Administrative Discipline. -
If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.
(g) Improper Disclosure Is Violation. -
Any willful disclosure or use by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by section 2517 is a violation of this chapter for purposes of section 2520(a).

UPDATE:

Pub. L. 107-296, The Homeland Security Act of 2002

Amended by Pub. L. 107-296, sec. 225(e)

18 U.S.C. §2702 (2002)
Voluntary disclosure of customer communications or records
Sec. 2702. (a) Prohibitions. - Except as provided in subsection (b) - (1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and (2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service - (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and (3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity. (b) Exceptions for disclosure of communications. - A provider described in subsection (a) may divulge the contents of a communication - (1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient; (2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title; (3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service; (4) to a person employed or authorized or whose facilities are used to forward such communication to its destination; (5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; or (6) to a law enforcement agency - (A)if the contents - (i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime; (B) if required by section 227 of the Crime Control Act of 1990; or (C) if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay. (c) Exceptions for Disclosure of Customer Records. - A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2)) - (1) as otherwise authorized in section 2703; (2) with the lawful consent of the customer or subscriber; (3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; (4) to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information; or (5) to any person other than a governmental entity
UPDATES:
Pub. L. 107-296, Homeland Security Act of 2002
Amended by Pub. L. 107-296, sec. 225(d)(1), 116 Stat. 2157.
Pub. L. 108-21, Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act of 2003
Amended by Pub. L. 108-21, sec. 508(b), 117 Stat. 684.

28 U.S.C. §1346 (2002)

United States as defendant

Sec. 1346. United States as defendant

(a) The district courts shall have original jurisdiction, concurrent with the United States Court of Federal Claims, of:

(1) Any civil action against the United States for the recovery of any internal-revenue tax alleged to have been erroneously or illegally assessed or collected, or any penalty claimed to have been collected without authority or any sum alleged to have been excessive or in any manner wrongfully collected under the internal-revenue laws;

(2) Any other civil action or claim against the United States, not exceeding $10,000 in amount, founded either upon the Constitution, or any Act of Congress, or any regulation of an executive department, or upon any express or implied contract with the United States, or for liquidated or unliquidated damages in cases not sounding in tort, except that the district courts shall not have jurisdiction of any civil action or claim against the United States founded upon any express or implied contract with the United States or for liquidated or unliquidated damages in cases not sounding in tort which are subject to sections 8(g)(1) and 10(a)(1) of the Contract Disputes Act of 1978. For the purpose of this paragraph, an express or implied contract with the Army and Air Force Exchange Service, Navy Exchanges, Marine Corps Exchanges, Coast Guard Exchanges, or Exchange Councils of the National Aeronautics and Space Administration shall be considered an express or implied contract with the United States.

(b)(1) Subject to the provisions of chapter 171 of this title, the district courts, together with the United States District Court for the District of the Canal Zone and the District Court of the Virgin Islands, shall have exclusive jurisdiction of civil actions on claims against the United States, for money damages, accruing on and after January 1, 1945, for injury or loss of property, or personal injury or death caused by the negligent or wrongful act or omission of any employee of the Government while acting within the scope of his office or employment, under circumstances where the United States, if a private person, would be liable to the claimant in accordance with the law of the place where the act or omission occurred.

(2) No person convicted of a felony who is incarcerated while awaiting sentencing or while serving a sentence may bring a civil action against the United States or an agency, officer, or employee of the Government, for mental or emotional injury suffered while in custody without a prior showing of physical injury.

(c) The jurisdiction conferred by this section includes jurisdiction of any set-off, counterclaim, or other claim or demand whatever on the part of the United States against any plaintiff commencing an action under this section.

(d) The district courts shall not have jurisdiction under this section of any civil action or claim for a pension.

(e) The district courts shall have original jurisdiction of any civil action against the United States provided in section 6226, 6228(a), 7426, or 7428 (in the case of the United States district court for the District of Columbia) or section 7429 of the Internal Revenue Code of 1986.

(f) The district courts shall have exclusive original jurisdiction of civil actions under section 2409a to quiet title to an estate or interest in real property in which an interest is claimed by the United States.

(g) Subject to the provisions of chapter 179, the district courts of the United States shall have exclusive jurisdiction over any civil action commenced under section 453(2) of title 3, by a covered employee under chapter 5 of such title.

Source: http://uscode.house.gov/usc.htm

UPDATE: None

28 U.S.C. §2680 (2002)

Exceptions

Sec. 2680.

The provisions of this chapter and section 1346(b) of this title shall not apply to -

(a) Any claim based upon an act or omission of an employee of the Government, exercising due care, in the execution of a statute or regulation, whether or not such statute or regulation be valid, or based upon the exercise or performance or the failure to exercise or perform a discretionary function or duty on the part of a federal agency or an employee of the Government, whether or not the discretion involved be abused.

(b) Any claim arising out of the loss, miscarriage, or negligent transmission of letters or postal matter.

(c) Any claim arising in respect of the assessment or collection of any tax or customs duty, or the detention of any goods, merchandise, or other property by any officer of customs or excise or any other law enforcement officer, except that the provisions of this chapter and section 1346(b) of this title apply to any claim based on injury or loss of goods, merchandise, or other property, while in the possession of any officer of customs or excise or any other law enforcement officer, if -

(1) the property was seized for the purpose of forfeiture under any provision of Federal law providing for the forfeiture of property other than as a sentence imposed upon conviction of a criminal offense;

(2) the interest of the claimant was not forfeited;

(3) the interest of the claimant was not remitted or mitigated (if the property was subject to forfeiture); and

(4) the claimant was not convicted of a crime for which the interest of the claimant in the property was subject to forfeiture under a Federal criminal forfeiture law.

(d) Any claim for which a remedy is provided by sections 741-752, 781-790 of Title 46, relating to claims or suits in admiralty against the United States.

(e) Any claim arising out of an act or omission of any employee of the Government in administering the provisions of sections 1-31 of Title 50, Appendix.

(f) Any claim for damages caused by the imposition or establishment of a quarantine by the United States.

(g) Repealed. Sept. 26, 1950, ch. 1049, Sec. 13 (5), 64 Stat. 1043.)

(h) Any claim arising out of assault, battery, false imprisonment, false arrest, malicious prosecution, abuse of process, libel, slander, misrepresentation, deceit, or interference with contract rights: Provided, That, with regard to acts or omissions of investigative or law enforcement officers of the United States Government, the provisions of this chapter and section 1346(b) of this title shall apply to any claim arising, on or after the date of the enactment of this proviso, out of assault, battery, false imprisonment, false arrest, abuse of process, or malicious prosecution. For the purpose of this subsection, "investigative or law enforcement officer" means any officer of the United States who is empowered by law to execute searches, to seize evidence, or to make arrests for violations of Federal law.

(i) Any claim for damages caused by the fiscal operations of the Treasury or by the regulation of the monetary system.

(j) Any claim arising out of the combatant activities of the military or naval forces, or the Coast Guard, during time of war.

(k) Any claim arising in a foreign country.

(l) Any claim arising from the activities of the Tennessee Valley Authority.

(m) Any claim arising from the activities of the Panama Canal Company.

(n) Any claim arising from the activities of a Federal land bank, a Federal intermediate credit bank, or a bank for cooperatives

UPDATE: None

42 U.S.C. §2011 *et seq.* (2002)

Atomic Energy Act of 1954, as amended.

This document is included in its entirety on the Deskbook CD-ROM.

Sec. 2013. - Purpose of chapter
It is the purpose of this chapter to effectuate the policies set forth above by providing for -
(a) program of conducting, assisting, and fostering research and development in order to encourage maximum scientific and industrial progress;
(b) a program for the dissemination of unclassified scientific and technical information and for the control, dissemination, and declassification of Restricted Data, subject to appropriate safeguards, so as to encourage scientific and industrial progress;
(c) a program for Government control of the possession, use, and production of atomic energy and special nuclear material, whether owned by the Government or others, so directed as to make the maximum contribution to the common defense and security and the national welfare, and to provide continued assurance of the Government's ability to enter into and enforce agreements with nations or groups of nations for the control of special nuclear materials and atomic weapons;
(d) a program to encourage widespread participation in the development and utilization of atomic energy for peaceful purposes to the maximum extent consistent with the common defense and security and with the health and safety of the public;
(e) a program of international cooperation to promote the common defense and security and to make available to cooperating nations the benefits of peaceful applications of atomic energy as widely as expanding technology and considerations of the common defense and security will permit; and
(f) a program of administration which will be consistent with the foregoing policies and programs, with international arrangements, and with agreements for cooperation, which will enable the Congress to be currently informed so as to take further legislative action as may be appropriate
§2014 (y)
The term "Restricted Data" means all data concerning
(1) design, manufacture, or utilization of atomic weapons;
(2) the production of special nuclear material; or
(3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to section 2162 of this title.

Sec. 2161. - Policy of Commission
It shall be the policy of the Commission to control the dissemination and declassification of Restricted Data in such a manner as to assure the common defense and security. Consistent with such policy, the Commission shall be guided by the following principles:
(a) Until effective and enforceable international safeguards against the use of atomic energy for destructive purposes have been established by an international arrangement, there shall be no exchange of Restricted Data with other nations except as authorized by section 2164 of this title; and
(b) The dissemination of scientific and technical information relating to atomic energy should be permitted and encouraged so as to provide that free interchange of ideas and criticism which is essential to scientific and industrial progress and public understanding and to enlarge the fund of technical information

Sec. 2162. - Classification and declassification of Restricted Data
(a) Periodic determination
The Commission shall from time to time determine the data, within the definition of Restricted Data, which can be published without undue risk to the common defense and security and shall thereupon cause such data to be declassified and removed from the category of Restricted Data.
(b) Continuous review
The Commission shall maintain a continuous review of Restricted Data and of any Classification Guides issued for the guidance of those in the atomic energy program with respect to the areas of Restricted Data which have been declassified in order to determine which information may be declassified and removed from the category of Restricted Data without undue risk to the common defense and security.
(c) Joint determination on atomic weapons; Presidential determination on disagreement
In the case of Restricted Data which the Commission and the Department of Defense jointly determine to relate primarily to the military utilization of atomic weapons, the determination that such data may be published without constituting an unreasonable risk to the common defense and security shall be made by the Commission and the Department of Defense jointly, and if the Commission and the Department of Defense do not agree, the determination shall be made by the President.
(d) Removal from Restricted Data category

42 U.S.C. §2011 *et seq.* (2002)

The Commission shall remove from the Restricted Data category such data as the Commission and the Department of Defense jointly determine relates primarily to the military utilization of atomic weapons and which the Commission and Department of Defense jointly determine can be adequately safeguarded as defense information: Provided, however, That no such data so removed from the Restricted Data category shall be transmitted or otherwise made available to any nation or regional defense organization, while such data remains defense information, except pursuant to an agreement for cooperation entered into in accordance with subsection (b) or (d) of section 2164 of this title.

(e) Joint determination on atomic energy programs

The Commission shall remove from the Restricted Data category such information concerning the atomic energy programs of other nations as the Commission and the Director of Central Intelligence jointly determine to be necessary to carry out the provisions of section 403(d) of title 50 and can be adequately safeguarded as defense information.

Sec. 2163. - Access to Restricted Data

The Commission may authorize any of its employees, or employees of any contractor, prospective contractor, licensee or prospective licensee of the Commission or any other person authorized access to Restricted Data by the Commission under section 2165(b) and (c) of this title to permit any employee of an agency of the Department of Defense or of its contractors, or any member of the Armed Forces to have access to Restricted Data required in the performance of his duties and so certified by the head of the appropriate agency of the Department of Defense or his designee: Provided, however, That the head of the appropriate agency of the Department of Defense or his designee has determined, in accordance with the established personnel security procedures and standards of such agency, that permitting the member or employee to have access to such Restricted Data will not endanger the common defense and security: And provided further, That the Secretary of Defense finds that the established personnel and other security procedures and standards of such agency are adequate and in reasonable conformity to the standards established by the Commission under section 2165 of this title

Sec. 2165. - Security restrictions

(a) On contractors and licensees

No arrangement shall be made under section 2051 of this title, no contract shall be made or continued in effect under section 2061 of this title, and no license shall be issued under section 2133 or 2134 of this title, unless the person with whom such arrangement is made, the contractor or prospective contractor, or the prospective licensee agrees in writing not to permit any individual to have access to Restricted Data until the Director of the Office of Personnel Management shall have made an investigation and report to the Commission on the character, associations, and loyalty of such individual, and the Commission shall have determined that permitting such person to have access to Restricted Data will not endanger the common defense and security.

(b) Employment of personnel; access to Restricted Data

Except as authorized by the Commission or the General Manager upon a determination by the Commission or General Manager that such action is clearly consistent with the national interest, no individual shall be employed by the Commission nor shall the Commission permit any individual to have access to Restricted Data until the Director of the Office of Personnel Management shall have made an investigation and report to the Commission on the character, associations, and loyalty of such individual, and the Commission shall have determined that permitting such person to have access to Restricted Data will not endanger the common defense and security.

(c) Acceptance of investigation and clearance granted by other Government agencies

Government agencies - In lieu of the investigation and report to be made by the Director of the Office of Personnel Management pursuant to subsection (b) of this section, the Commission may accept an investigation and report on the character, associations, and loyalty of an individual made by another Government agency which conducts personnel security investigations, provided that a security clearance has been granted to such individual by another Government agency based on such investigation and report.

(d) Investigations by FBI

In the event an investigation made pursuant to subsections (a) and (b) of this section develops any data reflecting that the individual who is the subject of the investigation is of questionable loyalty, the Director of the Office of Personnel Management shall refer the matter to the Federal Bureau of Investigation for the conduct of a full field investigation, the results of which shall be furnished to the Director of the Office of Personnel Management for his information and appropriate action.

(e) Presidential investigation

(1) If the President deems it to be in the national interest he may from time to time determine that investigations of any group or class which are required by subsections (a), (b), and (c) of this section be made by the Federal Bureau of Investigation.

(2) In the case of an individual employed in a program known as a Special Access Program or a Personnel Security and Assurance Program, any investigation required by subsections (a), (b), and (c) of this section shall be made by the Federal Bureau of Investigation.

(f) Certification of specific positions for investigation by FBI

Notwithstanding the provisions of subsections (a), (b), and (c) of this section, a majority of the members of the Commission shall certify those specific positions which are of a high degree of importance or sensitivity, and upon such certification, the investigation and reports required by such provisions shall be made by the Federal Bureau of Investigation.

(g) Investigation standards

42 U.S.C. §2011 *et seq.* (2002)

The Commission shall establish standards and specifications in writing as to the scope and extent of investigations, the reports of which will be utilized by the Commission in making the determination, pursuant to subsections (a), (b), and (c) of this section, that permitting a person access to restricted data will not endanger the common defense and security. Such standards and specifications shall be based on the location and class or kind of work to be done, and shall, among other considerations, take into account the degree of importance to the common defense and security of the restricted data to which access will be permitted.

(h) War time clearance

Whenever the Congress declares that a state of war exists, or in the event of a national disaster due to enemy attack, the Commission is authorized during the state of war or period of national disaster due to enemy attack to employ individuals and to permit individuals access to Restricted Data pending the investigation report, and determination required by subsection (b) of this section, to the extent that and so long as the Commission finds that such action is required to prevent impairment of its activities in furtherance of the common defense and security

Sec. 2166. - Applicability of other laws

(a) Sections 2161 to 2165 of this title shall not exclude the applicable provisions of any other laws, except that no Government agency shall take any action under such other laws inconsistent with the provisions of those sections.

(b) The Commission shall have no power to control or restrict the dissemination of information other than as granted by this or any other law

Sec. 2168. - Dissemination of unclassified information

(a) Dissemination prohibited; rules and regulations; determinations of Secretary prerequisite to issuance of prohibiting regulations or orders; criteria

(1) In addition to any other authority or requirement regarding protection from dissemination of information, and subject to section 552(b)(3) of title 5, the Secretary of Energy (hereinafter in this section referred to as the "Secretary"), with respect to atomic energy defense programs, shall prescribe such regulations, after notice and opportunity for public comment thereon, or issue such orders as may be necessary to prohibit the unauthorized dissemination of unclassified information pertaining to -

(A) the design of production facilities or utilization facilities;

(B) security measures (including security plans, procedures, and equipment) for the physical protection of:

(i) production or utilization facilities,

(ii) nuclear material contained in such facilities, or

(iii) nuclear material in transit; or

(C) the design, manufacture, or utilization of any atomic weapon or component if the design, manufacture, or utilization of such weapon or component was contained in any information declassified or removed from the Restricted Data category by the Secretary (or the head of the predecessor agency of the Department of Energy) pursuant to section 2162 of this title.

(2) The Secretary may prescribe regulations or issue orders under paragraph (1) to prohibit the dissemination of any information described in such paragraph only if and to the extent that the Secretary determines that the unauthorized dissemination of such information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of

(A) illegal production of nuclear weapons, or

(B) theft, diversion, or sabotage of nuclear materials, equipment, or facilities.

(3) In making a determination under paragraph (2), the Secretary may consider what the likelihood of an illegal production, theft, diversion, or sabotage referred to in such paragraph would be if the information proposed to be prohibited from dissemination under this section were at no time available for dissemination.

(4) The Secretary shall exercise his authority under this subsection to prohibit the dissemination of any information described in paragraph (1) of this subsection -

(A) so as to apply the minimum restrictions needed to protect the health and safety of the public or the common defense and security; and

(B) upon a determination that the unauthorized dissemination of such information could reasonably be expected to result in a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of

(i) illegal production of nuclear weapons, or

(ii) theft, diversion, or sabotage of nuclear materials, equipment, or facilities.

(5) Nothing in this section shall be construed to authorize the Secretary to authorize the withholding of information from the appropriate committees of the Congress.

(b) Civil penalties

(1) Any person who violates any regulation or order of the Secretary issued under this section with respect to the unauthorized dissemination of information shall be subject to a civil penalty, to be imposed by the Secretary, of not to exceed $100,000 for each such

42 U.S.C. §2011 *et seq.* (2002)
violation. The Secretary may compromise, mitigate, or remit any penalty imposed under this subsection. (2) The provisions of subsections (b) and (c) of section 2282 of this title, shall be applicable with respect to the imposition of civil penalties by the Secretary under this section in the same manner that such provisions are applicable to the imposition of civil penalties by the Commission under subsection (a) of such section. (c) Criminal penalties For the purposes of section 2273 of this title, any regulation prescribed or order issued by the Secretary under this section shall also be deemed to be prescribed or issued under section 2201(b) of this title. (d) Judicial review Any determination by the Secretary concerning the applicability of this section shall be subject to judicial review pursuant to section 552(a)(4)(B) of title 5. (e) Quarterly reports for interested persons; contents The Secretary shall prepare on a quarterly basis a report to be made available upon the request of any interested person, detailing the Secretary's application during that period of each regulation or order prescribed or issued under this section. In particular, such report shall - (1) identify any information protected from disclosure pursuant to such regulation or order; (2) specifically state the Secretary's justification for determining that unauthorized dissemination of the information protected from disclosure under such regulation or order could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of illegal production of nuclear weapons, or theft, diversion, or sabotage of nuclear materials, equipment, or facilities, as specified under subsection (a) of this section; and (3) provide justification that the Secretary has applied such regulation or order so as to protect from disclosure only the minimum amount of information necessary to protect the health and safety of the public or the common defense and security
UPDATE: None to these sections

42 U.S.C. §5121 *et seq.* (2002)

The Stafford Act

This document is included in its entirety on the Deskbook CD-ROM.

Sec. 5132. - Disaster warnings
(a) Readiness of Federal agencies to issue warnings to State and local officials
The President shall insure that all appropriate Federal agencies are prepared to issue warnings of disasters to State and local officials.
(b) Technical assistance to State and local governments for effective warnings
The President shall direct appropriate Federal agencies to provide technical assistance to State and local governments to insure that timely and effective disaster warning is provided.
(c) Warnings to governmental authorities and public endangered by disaster
The President is authorized to utilize or to make available to Federal, State, and local agencies the facilities of the civil defense communications system established and maintained pursuant to section 5196(c) of this title or any other Federal communications system for the purpose of providing warning to governmental authorities and the civilian population in areas endangered by disasters.
(d) Agreements with commercial communications systems for use of facilities
The President is authorized to enter into agreements with the officers or agents of any private or commercial communications systems who volunteer the use of their systems on a reimbursable or nonreimbursable basis for the purpose of providing warning to governmental authorities and the civilian population endangered by disasters

Sec. 5185. Emergency Communications
The President is authorized during, or in anticipation of, an emergency or major disaster to establish temporary communications systems and to make such communications available to State and local government officials and other persons as he deems appropriate

Sec. 5196d. - Use of funds to prepare for and respond to hazards
Funds made available to the States under this subchapter may be used by the States for the purposes of preparing for hazards and providing emergency assistance in response to hazards. Regulations prescribed to carry out this section shall authorize the use of emergency preparedness personnel, materials, and facilities supported in whole or in part through contributions under this subchapter for emergency preparedness activities and measures related to hazards

UPDATE: None

47 U.S.C. §308 (2002)

Requirements for license

(a) Writing; exceptions
The Commission may grant construction permits and station licenses, or modifications or renewals thereof, only upon written application therefore received by it: Provided, That (1) in cases of emergency found by the Commission involving danger to life or property or due to damage to equipment, or (2) during a national emergency proclaimed by the President or declared by the Congress and during the continuance of any war in which the United States is engaged and when such action is necessary for the national defense or security or otherwise in furtherance of the war effort, or (3) in cases of emergency where the Commission finds, in the non-broadcast services, that it would not be feasible to secure renewal applications from existing licensees or otherwise to follow normal licensing procedure, the Commission may grant construction permits and station licenses, or modifications or renewals thereof, during the emergency so found by the Commission or during the continuance of any such national emergency or war, in such manner and upon such terms and conditions as the Commission shall by regulation prescribe, and without the filing of a formal application, but no authorization so granted shall continue in effect beyond the period of the emergency or war requiring it:

Provided further, That the Commission may issue by cable, telegraph, or radio a permit for the operation of a station on a vessel of the United States at sea, effective in lieu of a license until said vessel shall return to a port of the continental United States.

(b) Conditions
All applications for station licenses, or modifications or renewals thereof, shall set forth such facts as the Commission by regulation may prescribe as to the citizenship, character, and financial, technical, and other qualifications of the applicant to operate the station; the ownership and location of the proposed station and of the stations, if any, with which it is proposed to communicate; the frequencies and the power desired to be used; the hours of the day or other periods of time during which it is proposed to operate the station; the purposes for which the station is to be used; and such other information as it may require. The Commission, at any time after the filing of such original application and during the term of any such license, may require from an applicant or licensee further written statements of fact to enable it to determine whether such original application should be granted or denied or such license revoked. Such application and/or such statement of fact shall be signed by the applicant and/or licensee in any manner or form, including by electronic means, as the Commission may prescribe by regulation.
(c) Commercial communication
The Commission in granting any license for a station intended or used for commercial communication between the United States or any Territory or possession, continental or insular, subject to the jurisdiction of the United States, and any foreign country, may impose any terms, conditions, or restrictions authorized to be imposed with respect to submarine-cable licenses by section 35 of this title.
(d) Summary of complaints
Each applicant for the renewal of a commercial or noncommercial television license shall attach as an exhibit to the application a summary of written comments and suggestions received from the public and maintained by the licensee (in accordance with Commission regulations) that comment on the applicant's programming, if any, and that are characterized by the comment or as constituting violent programming.

UPDATE: None

47 U.S.C. §606 (2002)

Telegraphs, Telephones, and Radiotelegraphs

Section 606. War powers of President

(a) Priority communications

During the continuance of a war in which the United States is engaged, the President is authorized, if he finds it necessary for the national defense and security, to direct that such communications as in his judgment may be essential to the national defense and security shall have preference or priority with any carrier subject to this chapter. He may give these directions at and for such times as he may determine, and may modify, change, suspend, or annul them and for any such purpose he is authorized to issue orders directly, or through such person or persons as he designates for the purpose, or through the Commission. Any carrier complying with any such order or direction for preference or priority herein authorized shall be exempt from any and all provisions in existing law imposing civil or criminal penalties, obligations, or liabilities upon carriers by reason of giving preference or priority in compliance with such order or direction.

(b) Obstruction of interstate or foreign communications

It shall be unlawful for any person during any war in which the United States is engaged to knowingly or willfully, by physical force or intimidation by threats of physical force, obstruct or retard or aid in obstructing or retarding interstate or foreign communication by radio or wire. The President is authorized, whenever in his judgment the public interest requires, to employ the armed forces of the United States to prevent any such obstruction or retardation of communication: Provided, That nothing in this section shall be construed to repeal, modify, or affect either section 17 of title 15 or section 52 of title 29.

(c) Suspension or amendment of rules and regulations applicable to certain emission stations or devices

Upon proclamation by the President that there exists war or a threat of war, or a state of public peril or disaster or other national emergency, or in order to preserve the neutrality of the United States, the President, if he deems it necessary in the interest of national security or defense, may suspend or amend, for such time as he may see fit, the rules and regulations applicable to any or all stations or devices capable of emitting electromagnetic radiations within the jurisdiction of the United States as prescribed by the Commission, and may cause the closing of any station for radio communication, or any device capable of emitting electromagnetic radiations between 10 kilocycles and 100,000 megacycles, which is suitable for use as a navigational aid beyond five miles, and the removal therefrom of its apparatus and equipment, or he may authorize the use or control of any such station or device and/or its apparatus and equipment, by any department of the Government under such regulations as he may prescribe upon just compensation to the owners. The authority granted to the President, under this subsection, to cause the closing of any station or device and the removal therefrom of its apparatus and equipment, or to authorize the use or control of any station or device and/or its apparatus and equipment, may be exercised in the Canal Zone.

(d) Suspension or amendment of rules and regulations applicable to wire communications; closing of facilities; Government use of facilities

Upon proclamation by the President that there exists a state or threat of war involving the United States, the President, if he deems it necessary in the interest of the national security and defense, may, during a period ending not later than six months after the termination of such state or threat of war and not later than such earlier date as the Congress by concurrent resolution may designate, (1) suspend or amend the rules and regulations applicable to any or all facilities or stations for wire communication within the jurisdiction of the United States as prescribed by the Commission, (2) cause the closing of any facility or station for wire communication and the removal therefrom of its apparatus and equipment, or (3) authorize the use or control of any such facility or station and its apparatus and equipment by any department of the Government under such regulations as he may prescribe, upon just compensation to the owners.

(e) Compensation

The President shall ascertain the just compensation for such use or control and certify the amount ascertained to Congress for appropriation and payment to the person entitled thereto. If the amount so certified is unsatisfactory to the person entitled thereto, such person shall be paid only 75 per centum of the amount and shall be entitled to sue the United States to recover such further sum as added to such payment of 75 per centum will make such amount as will be just compensation for the use and control. Such suit shall be brought in the manner provided by section 1346 or section 1491 of title 28.

(f) Affect on State laws and powers

Nothing in subsection (c) or (d) of this section shall be construed to amend, repeal, impair, or affect existing laws or powers of the States in relation to taxation or the lawful police regulations of the several States, except wherein such laws, powers, or regulations may affect the transmission of Government communications, or the issue of stocks and bonds by any communication system or systems.

47 U.S.C. §606 (2002)

(g) Limitations upon Presidential power

Nothing in subsection (c) or (d) of this section shall be construed to authorize the President to make any amendment to the rules and regulations of the Commission which the Commission would not be authorized by law to make; and nothing in subsection (d) of this section shall be construed to authorize the President to take any action the force and effect of which shall continue beyond the date after which taking of such action would not have been authorized.

(h) Penalties

Any person who willfully does or causes or suffers to be done any act prohibited pursuant to the exercise of the President's authority under this section, or who willfully fails to do any act which he is required to do pursuant to the exercise of the President's authority under this section, or who willfully causes or suffers such failure, shall, upon conviction thereof, be punished for such offense by a fine of not more than $1,000 or by imprisonment for not more than one year, or both, and, if a firm, partnership, association, or corporation, by fine of not more than $5,000, except that any person who commits such an offense with intent to injure the United States, or with intent to secure an advantage to any foreign nation, shall, upon conviction thereof, be punished by a fine of not more than $20,000 or by imprisonment for not more than 20 years, or both.

UPDATE: None

50 U.S.C. §401 et seq. (2002)

The National Security Act

This document is included in its entirety on the Deskbook CD-ROM.

Sec. 401. Congressional declaration of purpose
In enacting this legislation, it is the intent of Congress to provide a comprehensive program for the future security of the United States; to provide for the establishment of integrated policies and procedures for the departments, agencies, and functions of the Government relating to the national security; to provide a Department of Defense, including the three military Departments of the Army, the Navy (including naval aviation and the United States Marine Corps), and the Air Force under the direction, authority, and control of the Secretary of Defense; to provide that each military department shall be separately organized under its own Secretary and shall function under the direction, authority, and control of the Secretary of Defense; to provide for their unified direction under civilian control of the Secretary of Defense but not to merge these departments or services; to provide for the establishment of unified or specified combatant commands, and a clear and direct line of command to such commands; to eliminate unnecessary duplication in the Department of Defense, and particularly in the field of research and engineering by vesting its overall direction and control in the Secretary of Defense; to provide more effective, efficient, and economical administration in the Department of Defense; to provide for the unified strategic direction of the combatant forces, for their operation under unified command, and for their integration into an efficient team of land, naval, and air forces but not to establish a single Chief of Staff over the armed forces nor an overall armed forces general staff.

UPDATE

Pub. L. 107-306 Intelligence Authorization Act for Fiscal Year 2003, 2002

New note added by secs. 109, 352, 402, 801, 901, and 1001-1011
Note amended by secs. 401, 841, and 811
Amended by secs. 321, 324, 342, 353, 811, 821, 822, 841, and 903
New section added or section amended generally by secs. 311, 313, 331, 341, 342, 343, 502, 811, 823, 827, 902, and 904

Pub. L. 107-248, Department of Defense Appropriations Act for FY2003

New note added by secs. 8058(b) and 8042

Pub. L. 107-296, The Homeland Security Act of 2002

Amended by sec. 897(a)

Pub. L. 108-87 Department of Defense Appropriations Act for FY 2004

New note added by secs. 8042 and 8057(b)

50 U.S.C. 1801 et seq., 2002

Foreign Intelligence Surveillance Act (FISA)

This document is included in its entirety on the Deskbook CD-ROM.

Sec. 1825. - Use of information

(a) Compliance with minimization procedures; lawful purposes

Information acquired from a physical search conducted pursuant to this subchapter concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this subchapter. No information acquired from a physical search pursuant to this subchapter may be used or disclosed by Federal officers or employees except for lawful purposes.

(b) Notice of search and identification of property seized, altered, or reproduced

Where a physical search authorized and conducted pursuant to section 1824 of this title involves the residence of a United States person, and, at any time after the search the Attorney General determines there is no national security interest in continuing to maintain the secrecy of the search, the Attorney General shall provide notice to the United States person whose residence was searched of the fact of the search conducted pursuant to this chapter and shall identify any property of such person seized, altered, or reproduced during such search.

(c) Statement for disclosure

No information acquired pursuant to this subchapter shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

(d) Notification by United States

Whenever the United States intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from a physical search pursuant to the authority of this subchapter, the United States shall, prior to the trial, hearing, or the other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the United States intends to so disclose or so use such information.

(e) Notification by States or political subdivisions

Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof against an aggrieved person any information obtained or derived from a physical search pursuant to the authority of this subchapter, the State or political subdivision thereof shall notify the aggrieved person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information.

(f) Motion to suppress

(1) Any person against whom evidence obtained or derived from a physical search to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from such search on the grounds that -

(A) the information was unlawfully acquired; or

(B) the physical search was not made in conformity with an order of authorization or approval.

(2) Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

(g) In camera and ex parte review by district court

Whenever a court or other authority is notified pursuant to subsection (d) or (e) of this section, or whenever a motion is made pursuant to subsection (f) of this section, or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to a physical search authorized by this subchapter or to discover, obtain, or suppress evidence or information obtained or derived from a physical search authorized by this subchapter, the United States district court or, where the motion

50 U.S.C. 1801 et seq., 2002

is made before another authority, the United States district court in the same district as the authority shall, notwithstanding any other provision of law, if the Attorney General files an affidavit under oath that disclosure or any adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the physical search as may be necessary to determine whether the physical search of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the physical search, or may require the Attorney General to provide to the aggrieved person a summary of such materials, only where such disclosure is necessary to make an accurate determination of the legality of the physical search.

(h) Suppression of evidence; denial of motion
If the United States district court pursuant to subsection (g) of this section determines that the physical search was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from the physical search of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the physical search was lawfully authorized or conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(i) Finality of orders
Orders granting motions or requests under subsection (h) of this section, decisions under this section that a physical search was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to the physical search shall be final orders and binding upon all courts of the United States and the several States except a United States Court of Appeals or the Supreme Court.

(j) Notification of emergency execution of physical search; contents; postponement, suspension, or elimination
(1) If an emergency execution of a physical search is authorized under section 1824(d) [1] of this title and a subsequent order approving the search is not obtained, the judge shall cause to be served on any United States person named in the application and on such other United States persons subject to the search as the judge may determine in his discretion it is in the interests of justice to serve, notice of -
(A) the fact of the application;
(B) the period of the search; and
(C) the fact that during the period information was or was not obtained.
(2) On an ex parte showing of good cause to the judge, the serving of the notice required by this subsection may be postponed or suspended for a period not to exceed 90 days. Thereafter, on a further ex parte showing of good cause, the court shall forego ordering the serving of the notice required under this subsection.

(k) Coordination with law enforcement on national security matters
(1) Federal officers who conduct physical searches to acquire foreign intelligence information under this subchapter may consult with Federal law enforcement officers to coordinate efforts to investigate or protect against -
(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
(B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.
(2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 1823(a)(7) of this title or the entry of an order under section 1824 of this title

Sec. 1861. - Access to certain business records for foreign intelligence and international terrorism investigations
(a) Application for order; conduct of investigation generally
(1) The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.
(2) An investigation conducted under this section shall -
(A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and
(B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.
(b) Recipient and contents of application
Each application under this section -

50 U.S.C. 1801 et seq., 2002
(1) shall be made to - (A) a judge of the court established by section 1803(a) of this title; or (B) a United States Magistrate Judge under chapter 43 of title 28, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and (2) shall specify that the records concerned are sought for an authorized investigation conducted in accordance with subsection (a)(2) of this section to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities. (c) Ex parte judicial order of approval (1) Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application meets the requirements of this section. (2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in subsection (a) of this section. (d) Nondisclosure No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section. (e) Liability for good faith disclosure; waiver A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production. Such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context
UPDATE
Pub. L. 107-56, USA PATRIOT Act of 2002
Amended by §§206-208, 214, 215.
Pub. L. 107-273, 21st Century Department of Justice Appropriations Authorization Act, 2002
Amended by Pub. L. 107-273, sec. 4005(c). New note added by Pub. L. 107-273, sec. 4005(c).
Pub. L. 107-296, Homeland Security Act of 2002
Amended by Pub. L. 107-296, sec. 898. Amended by Pub. L. 107-296, sec. 899. .

USCS Federal Rules of Criminal Procedure 6, 2002

The Grand Jury

Rule 6. The Grand Jury

(e) Recording and Disclosing the Proceedings.

(1) Recording the Proceedings. Except while the grand jury is deliberating or voting, all proceedings must be recorded by a court reporter or by a suitable recording device. But the validity of a prosecution is not affected by the unintentional failure to make a recording. Unless the court orders otherwise, an attorney for the government will retain control of the recording, the reporter's notes, and any transcript prepared from those notes.

(2) Secrecy.

(A) No obligation of secrecy may be imposed on any person except in accordance with Rule 6(e)(2)(B).

(B) Unless these rules provide otherwise, the following persons must not disclose a matter occurring before the grand jury:

(i) a grand juror;

(ii) an interpreter;

(iii) a court reporter;

(iv) an operator of a recording device;

(v) a person who transcribes recorded testimony;

(vi) an attorney for the government; or

(vii) a person to whom disclosure is made under Rule 6(e)(3)(A)(ii) or (iii);

(3) Exceptions.

(A) Disclosure of a grand-jury matter--other than the grand jury's deliberations or any grand juror's vote--may be made to:

(i) an attorney for the government for use in performing that attorney's duty;

(ii) any government personnel--including those of a state or state subdivision or of an Indian tribe--that an attorney for the government considers necessary to assist in performing that attorney's duty to enforce federal criminal law; or

(iii) a person authorized by 18 U.S.C. § 3322.

(B) A person to whom information is disclosed under Rule 6(e)(3)(A)(ii) may use that information only to assist an attorney for the government in performing that attorney's duty to enforce federal criminal law. An attorney for the government must promptly provide the court that impaneled the grand jury with the names of all persons to whom a disclosure has been made, and must certify that the attorney has advised those persons of their obligation of secrecy under this rule.

(C) An attorney for the government may disclose any grand-jury matter to another federal grand jury.

(D) An attorney for the government may disclose any grand-jury matter involving foreign intelligence, counterintelligence (as defined in 50 U.S.C. § 401a), or foreign intelligence information (as defined in Rule 6(e)(3)(D)(iii)) to any federal law enforcement, intelligence, protective, immigration, national defense, or national security official to assist the official receiving the information in the performance of that official's duties.

(i) Any federal official who receives information under Rule 6(e)(3)(D) may use the information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.

(ii) Within a reasonable time after disclosure is made under Rule 6(e)(3)(D), an attorney for the government must file, under seal, a notice with the court in the district where the grand jury convened stating that such information was disclosed and the departments, agencies, or entities to which the disclosure was made.

(iii) As used in Rule 6(e)(3)(D), the term "foreign intelligence information" means:

(a) information, whether or not it concerns a United States person, that relates to the ability of the United States to protect against--

. actual or potential attack or other grave hostile acts of a foreign power or its agent;

. sabotage or international terrorism by a foreign power or its agent; or

. clandestine intelligence activities by an intelligence service or network of a foreign power or by its agent; or

(b) information, whether or not it concerns a United States person, with respect to a foreign power or foreign territory that relates to--

. the national defense or the security of the United States; or

. the conduct of the foreign affairs of the United States.

(E) The court may authorize disclosure--at a time, in a manner, and subject to any other conditions that it directs--of a grand-jury matter:

(i) preliminarily to or in connection with a judicial proceeding;

(ii) at the request of a defendant who shows that a ground may exist to dismiss the indictment because of a matter that occurred before the grand jury;

(iii) at the request of the government if it shows that the matter may disclose a violation of state or Indian tribal criminal law, as long

USCS Federal Rules of Criminal Procedure 6, 2002

as the disclosure is to an appropriate state, state subdivision, or Indian tribal official for the purpose of enforcing that law; or

(iv) at the request of the government if it shows that the matter may disclose a violation of military criminal law under the Uniform Code of Military Justice, as long as the disclosure is to an appropriate military official for the purpose of enforcing that law.

(F) A petition to disclose a grand-jury matter under Rule 6(e)(3)(E)(i) must be filed in the district where the grand jury convened. Unless the hearing is ex parte--as it may be when the government is the petitioner--the petitioner must serve the petition on, and the court must afford a reasonable opportunity to appear and be heard to:

(i) an attorney for the government;

(ii) the parties to the judicial proceeding; and

(iii) any other person whom the court may designate.

(G) If the petition to disclose arises out of a judicial proceeding in another district, the petitioned court must transfer the petition to the other court unless the petitioned court can reasonably determine whether disclosure is proper. If the petitioned court decides to transfer, it must send to the transferee court the material sought to be disclosed, if feasible, and a written evaluation of the need for continued grand jury secrecy. The transferee court must afford those persons identified in Rule 6(e)(3)(F) a reasonable opportunity to appear and be heard.

(4) Sealed Indictment. The magistrate judge to whom an indictment is returned may direct that the indictment be kept secret until the defendant is in custody or has been released pending trial. The clerk must then seal the indictment, and no person may disclose the indictment's existence except as necessary to issue or execute a warrant or summons.

(5) Closed Hearing. Subject to any right to an open hearing in a contempt proceeding, the court must close any hearing to the extent necessary to prevent disclosure of a matter occurring before a grand jury.

(6) Sealed Records. Records, orders, and subpoenas relating to grand-jury proceedings must be kept under seal to the extent and as long as necessary to prevent the unauthorized disclosure of a matter occurring before a grand jury.

(7) Contempt. A knowing violation of Rule 6 may be punished as a contempt of court.

UPDATE

Pub. L. 107-296, Homeland Security Act of 2002

Amended by sec.895.

47 CFR Part 201.2 (2002)

Executive Policy

This document is included in its entirety on the Deskbook CD-ROM.

TITLE 47—TELECOMMUNICATION
CHAPTER II--OFFICE OF SCIENCE AND TECHNOLOGY POLICY AND NATIONAL SECURITY COUNCIL
PART 201--EXECUTIVE POLICY--Table of Contents

Sec. 201.2 Definitions.
The following definitions apply herein:

(a) Communications common carrier, specialized carrier, or carrier means any individual, partnership, association, joint stock company, trust, or corporation subject to Federal or State regulation engaged in providing telecommunications facilities or services, for use by the public, for hire.

(b) Government means Federal, State, county, municipal, and other local government authority. Specific qualification will be provided whenever reference to a particular level of government is intended.

(c) Joint Telecommunications Resources Board (JTRB) means that organization established by the Director, Office of Science and Technology Policy, pursuant to Executive Order 12472 to assist the Director, OSTP, in exercising the non-wartime emergency telecommunications functions assigned by Executive Order 12472.

(d) The National Communications System (NCS) means that organization established by Executive Order 12472 consisting of the telecommunications assets of the entities represented on the NCS Committee of Principals and an administrative structure consisting of the Executive Agent, the NCS Committee of Principals and the Manager. The NCS Committee of Principals consists of representatives from those Federal departments, agencies or entities, designated by the President, which lease or own telecommunications facilities or services of significance to national security and emergency preparedness, and, to the extent permitted by law, other Executive entities which bear policy, regulatory or enforcement responsibilities of importance to national security and emergency preparedness telecommunications capabilities. The NCS is a confederative arrangement in which member Federal agencies participate with their owned and leased telecommunications assets to provide necessary communications services for the Federal Government, under all conditions, including nuclear war.

(e) National Coordinating Center (NCC) refers to the joint industry-government telecommunications entity established by the NCS pursuant to Executive Order 12472 to assist in the initiation, coordination, restoration and reconstitution of national security and emergency preparedness telecommunications services or facilities under all conditions of crisis or emergency.

(f) National priorities means those essential actions and activities in which the government and the private sector must become engaged in the interests of national survival and recovery.

(g) National security and emergency preparedness (NS/EP) telecommunications services, or NS/EP services, means those telecommunication services which are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) which causes or could cause injury or harm to the population, damage to or loss of property, or degrades or threatens the NS/EP posture of the United States.

(h) NS/EP treatment refers to the provisioning of a telecommunications service before others based on the provisioning priority level assigned by the Executive Office of the President.

(i) National Telecommunications Management Structure (NTMS) means a survivable and enduring management structure which will support the exercise of the war power functions of the President under section 706 of the Communications Act of 1934 (47 U.S.C. 606), as amended.

(j) Private sector means those sectors of non-government entities that are users of telecommunications services.

(k) Telecommunications means any transmission, emission, or reception of signs, signals, writing, images, graphics, and sounds or intelligence of any nature by wire, radio, optical, or other electromagnetic systems.

(l) Telecommunications resources include telecommunications personnel, equipment, material, facilities, systems, and services, public and private, wheresoever located within the jurisdiction of the United States.

(m) Wartime emergency means a crisis or event which permits the exercise of the war power functions of the President under section 706 of the Communications Act of 1934 (47 U.S.C. 606), as amended.

UPDATE: None

Atty Gen. Ashcroft Memorandum, Oct. 12, 2001

Memorandum for Heads of all Federal Departments and Agencies

This document is included in its entirety on the Deskbook CD-ROM.

From: John Ashcroft, Attorney General
Subject: The Freedom of Information Act

As you know, the Department of Justice and this Administration are committed to full compliance with the Freedom of Information Act (FOIA), 5 U.S.C. § 552 (2000). It is only through a well-informed citizenry that the leaders of our nation remain accountable to the governed and the American people can be assured that neither fraud nor government waste is concealed.

The Department of Justice and this Administration are equally committed to protecting other fundamental values that are held by our society. Among them are safeguarding our national security, enhancing the effectiveness of our law enforcement agencies, protecting sensitive business information and, not least, preserving personal privacy.

Our citizens have a strong interest as well in a government that is fully functional and efficient. Congress and the courts have long recognized that certain legal privileges ensure candid and complete agency deliberations without fear that they will be made public. Other privileges ensure that lawyers' deliberations and communications are kept private. No leader can operate effectively without confidential advice and counsel. Exemption 5 of the FOIA, 5 U.S.C. § 552(b)(5), incorporates these privileges and the sound policies underlying them.

I encourage your agency to carefully consider the protection of all such values and interests when making disclosure determinations under the FOIA. Any discretionary decision by your agency to disclose information protected under the FOIA should be made only after full and deliberate consideration of the institutional, commercial, and personal privacy interests that could be implicated by disclosure of the information.

In making these decisions, you should consult with the Department of Justice's Office of Information and Privacy when significant FOIA issues arise, as well as with our Civil Division on FOIA litigation matters. When you carefully consider FOIA requests and decide to withhold records, in whole or in part, you can be assured that the Department of Justice will defend your decisions unless they lack a sound legal basis or present an unwarranted risk of adverse impact on the ability of other agencies to protect other important records.

This memorandum supersedes the Department of Justice's FOIA Memorandum of October 4, 1993, and it likewise creates no substantive or procedural right enforceable at law.

UPDATE: None

Pub. L. 107-56, 2001

Uniting and Strengthening America By Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001

This document is included in its entirety on the Deskbook CD-ROM.

SEC. 203. AUTHORITY TO SHARE CRIMINAL INVESTIGATIVE INFORMATION.

(a) Authority To Share Grand Jury Information.--

(1) In general.--Rule 6(e)(3)(C) of the Federal Rules of Criminal Procedure is amended to read as follows:

``(C)(i) Disclosure otherwise prohibited by this rule of matters occurring before the grand jury may also be made--

``(I) when so directed by a court preliminarily to or in connection with a judicial proceeding;

``(II) when permitted by a court at the request of the defendant, upon a showing that grounds may exist for a motion to dismiss the indictment because of matters occurring before the grand jury;

``(III) when the disclosure is made by an attorney for the government to another Federal grand jury;

``(IV) when permitted by a court at the request of an attorney for the government, upon a showing that such matters may disclose a violation of State criminal law, to an appropriate official of a State or subdivision of a State for the purpose of enforcing such law; or

``(V) when the matters involve foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), or foreign intelligence information

(as defined in clause (iv) of this subparagraph), to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties.

``(ii) If the court orders disclosure of matters occurring before the grand jury, the disclosure shall be made in such manner, at such time, and under such conditions as the court may direct.

``(iii) Any Federal official to whom information is disclosed pursuant to clause (i)(V) of this subparagraph may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information. Within a reasonable time after such disclosure, an attorney for the government shall file under seal a notice with the court stating the fact that such information was disclosed and the departments, agencies, or entities to which the disclosure was made.

``(iv) In clause (i)(V) of this subparagraph, the term `foreign intelligence information' means--

``(I) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against--

``(aa) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

``(bb) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

``(cc) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of foreign power; or

``(II) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to--

``(aa) the national defense or the security of the United States; or

``(bb) the conduct of the foreign affairs of the United States.".

(2) Conforming amendment.--Rule 6(e)(3)(D) of the Federal Rules of Criminal Procedure is amended by striking ``(e)(3)(C)(i)" and inserting ``(e)(3)(C)(i)(I)".

(b) Authority To Share Electronic, Wire, and Oral Interception Information.--

(1) Law enforcement.--Section 2517 of title 18, United States Code, is amended by inserting at the end the following:

``(6) Any investigative or law enforcement officer, or attorney for the Government, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), or foreign intelligence information (as defined in subsection (19) of section 2510 of this title), to assist the official who is to receive that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.".

(2) Definition.--Section 2510 of title 18, United States Code, is amended by--

(A) in paragraph (17), by striking ``and" after the semicolon;

(B) in paragraph (18), by striking the period and inserting ``; and"; and

(C) by inserting at the end the following:

Pub. L. 107-56, 2001

``(19) `foreign intelligence information' means--
``(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against--
``(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
``(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
``(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
``(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to--
``(i) the national defense or the security of the United States; or
``(ii) the conduct of the foreign affairs of the United States.".

(c) Procedures.--The Attorney General shall establish procedures for the disclosure of information pursuant to section 2517(6) and Rule 6(e)(3)(C)(i)(V) of the Federal Rules of Criminal Procedure
that identifies a United States person, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801)).

(d) Foreign Intelligence Information.--
(1) In general.--Notwithstanding any other provision of law, it shall be lawful for foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)) or foreign intelligence information obtained as part of a criminal investigation to be disclosed to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.
(2) Definition.--In this subsection, the term ``foreign intelligence information'' means--
(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against--
(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to--
(i) the national defense or the security of the United States; or
(ii) the conduct of the foreign affairs of the United States.

SEC. 212. EMERGENCY DISCLOSURE OF ELECTRONIC COMMUNICATIONS TO PROTECT LIFE AND LIMB.
(a) Disclosure of Contents.--
(1) In general.--Section 2702 of title 18, United States Code, is amended--
(A) by striking the section heading and inserting he following:

``Sec. 2702. Voluntary disclosure of customer communications or records'';
(B) in subsection (a)--
(i) in paragraph (2)(A), by striking ``and'' at the end;
(ii) in paragraph (2)(B), by striking the period and inserting ``; and''; and
(iii) by inserting after paragraph (2) the following:
``(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.'';
(C) in subsection (b), by striking ``Exceptions.--A person or entity'' and inserting ``Exceptions for disclosure of communications.-- A provider described in subsection (a)'';
(D) in subsection (b)(6)--
(i) in subparagraph (A)(ii), by striking ``or'';
(ii) in subparagraph (B), by striking the period and inserting ``; or''; and
(iii) by adding after subparagraph (B) the following:

Pub. L. 107-56, 2001

``(C) if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay."; and (E) by inserting after subsection (b) the following:

``(c) Exceptions for Disclosure of Customer Records.--A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))—

``(1) as otherwise authorized in section 2703;

``(2) with the lawful consent of the customer or subscriber;

``(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

``(4) to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information; or

``(5) to any person other than a governmental entity.".

(2) Technical and conforming amendment.--The table of sections for chapter 121 of title 18, United States Code, is amended by striking the item relating to section 2702 and inserting the following:

``2702. Voluntary disclosure of customer communications or records.".

(b) Requirements for Government Access.--

(1) In general.--Section 2703 of title 18, United States Code, is amended--

(A) by striking the section heading and inserting the following:

``Sec. 2703. Required disclosure of customer communications or records";

(B) in subsection (c) by redesignating paragraph (2) as paragraph (3);

(C) in subsection (c)(1)--

(i) by striking ``(A) Except as provided in subparagraph (B), a provider of electronic communication service or remote computing service may" and inserting ``A governmental entity may require a provider of electronic communication service or remote computing service to";

(ii) by striking ``covered by subsection (a) or (b) of this section) to any person other than a governmental entity.

``(B) A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to a governmental entity" and inserting ``)";

(iii) by redesignating subparagraph (C) as paragraph (2);

(iv) by redesignating clauses (i), (ii),(iii), and (iv) as subparagraphs (A), (B), (C), and (D), respectively;

(v) in subparagraph (D) (as redesignated) by striking the period and inserting ``; or"; and

(vi) by inserting after subparagraph (D) (as redesignated) the following:

``(E) seeks information under paragraph (2).";and

(D) in paragraph (2) (as redesignated) by striking ``subparagraph (B)" and insert ``paragraph (1)".

(2) Technical and conforming amendment.--The table of sections for chapter 121 of title 18, United States Code, is amended by striking the item relating to section 2703 and inserting the following:

``2703. Required disclosure of customer communications or records.".

SEC. 223. CIVIL LIABILITY FOR CERTAIN UNAUTHORIZED DISCLOSURES.

(a) Section 2520 of title 18, United States Code, is amended--

(1) in subsection (a), after ``entity", by inserting ``, other than the United States,";

(2) by adding at the end the following:

``(f) Administrative Discipline.--If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide

Pub. L. 107-56, 2001

the Inspector General with the reasons for such determination."; and

(3) by adding a new subsection (g), as follows:

``(g) Improper Disclosure Is Violation.--Any willful disclosure or use by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by section 2517 is a violation of this chapter for purposes of section 2520(a).".

(b) Section 2707 of title 18, United States Code, is amended--

(1) in subsection (a), after ``entity", by inserting ``, other than the United States,";

(2) by striking subsection (d) and inserting the following:

``(d) Administrative Discipline.--If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination."; and

(3) by adding a new subsection (g), as follows:

``(g) Improper Disclosure.--Any willful disclosure of a `record', as that term is defined in section 552a(a) of title 5, United States Code, obtained by an investigative or law enforcement officer, or a governmental entity, pursuant to section 2703 of this title, or from a device installed pursuant to section 3123 or 3125 of this title, that is not a disclosure made in the proper performance of the official functions of the officer or governmental entity making the disclosure, is a violation of this chapter. This provision shall not apply to information previously lawfully disclosed (prior to the commencement of any civil or administrative proceeding under this chapter) to the public by a Federal, State, or local governmental entity or by the plaintiff in a civil action under this chapter.".

(c)(1) Chapter 121 of title 18, United States Code, is amended by adding at the end the following:

``Sec. 2712. Civil actions against the United States

``(a) In General.--Any person who is aggrieved by any willful violation of this chapter or of chapter 119 of this title or of sections 106(a), 305(a), or 405(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) may commence an action in United States District Court against the United States to recover money damages. In any such action, if a person who is aggrieved successfully establishes such a violation of this chapter or of chapter 119 of this title or of the above specific provisions of title 50, the Court may assess as damages--

``(1) actual damages, but not less than $10,000, whichever amount is greater; and

``(2) litigation costs, reasonably incurred.

``(b) Procedures.--(1) Any action against the United States under this section may be commenced only after a claim is presented to the appropriate department or agency under the procedures of the Federal Tort Claims Act, as set forth in title 28, United States Code.

``(2) Any action against the United States under this section shall be forever barred unless it is presented in writing to the appropriate Federal agency within 2 years after such claim accrues or unless action is begun within 6 months after the date of mailing, by certified or registered mail, of notice of final denial of the claim by the agency to which it was presented. The claim shall accrue on the date upon which the claimant first has a reasonable opportunity to discover the violation.

``(3) Any action under this section shall be tried to the court without a jury.

``(4) Notwithstanding any other provision of law, the procedures set forth in section 106(f), 305(g), or 405(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) shall be the exclusive means by which materials governed by those sections may be reviewed.

``(5) An amount equal to any award against the United States under this section shall be reimbursed by the department or agency concerned to the fund described in section 1304 of title 31, United States Code, out of any appropriation, fund, or other account (excluding any part of such appropriation, fund, or account that is available for the enforcement of any Federal law) that is available for the operating expenses of the department or agency concerned.

``(c) Administrative Discipline.--If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary

Pub. L. 107-56, 2001

action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

``(d) Exclusive Remedy.--Any action against the United States under this subsection shall be the exclusive remedy against the United States for any claims within the purview of this section.

``(e) Stay of Proceedings.--(1) Upon the motion of the United States, the court shall stay any action commenced under this section if the court determines that civil discovery will adversely affect the ability of the Government to conduct a related investigation or the prosecution of a related criminal case. Such a stay shall toll the limitations periods of paragraph (2) of subsection (b).

``(2) In this subsection, the terms `related criminal case' and `related investigation' mean an actual prosecution or investigation in progress at the time at which the request for the stay or any subsequent motion to lift the stay is made. In determining whether an investigation or a criminal case is related to an action commenced under this section, the court shall consider the degree of similarity between the parties, witnesses, facts, and circumstances involved in the 2 proceedings, without requiring that any one or more factors be identical.

``(3) In requesting a stay under paragraph (1), the Government may, in appropriate cases, submit evidence ex parte in order to avoid disclosing any matter that may adversely affect a related investigation or a related criminal case. If the Government makes such an ex parte submission, the plaintiff shall be given an opportunity to make a submission to the court, not ex parte, and the court may, in its discretion, request further information from either party.".

(2) The table of sections at the beginning of chapter 121 is amended to read as follows:

``2712. Civil action against the United States.''

UPDATE: None

Pub. L. 107-188, 2002

Public Health Security and Bioterrorism Preparedness and Response Act of 2002

This document is included in its entirety on the Deskbook CD-ROM.

SEC. 104. ADVISORY COMMITTEES AND COMMUNICATIONS; STUDY REGARDING COMMUNICATIONS ABILITIES OF PUBLIC HEALTH AGENCIES.
(a) IN GENERAL- Section 319F of the Public Health Service Act (42 U.S.C. 247d-6) is amended--
(1) by striking subsections (b) and (i);
(2) by redesignating subsections (c) through (h) as subsections (e) through (j), respectively; and
(3) by inserting after subsection (a) the following subsections:
`(b) ADVICE TO THE FEDERAL GOVERNMENT-
`(1) REQUIRED ADVISORY COMMITTEES- In coordination with the working group under subsection (a), the Secretary shall establish advisory committees in accordance with paragraphs (2) and (3) to provide expert recommendations to assist such working groups in carrying out their respective responsibilities under subsections (a) and (b).
`(2) NATIONAL ADVISORY COMMITTEE ON CHILDREN AND TERRORISM-
`(A) IN GENERAL- For purposes of paragraph (1), the Secretary shall establish an advisory committee to be known as the National Advisory Committee on Children and Terrorism (referred to in this paragraph as the `Advisory Committee').
`(B) DUTIES- The Advisory Committee shall provide recommendations regarding--
`(i) the preparedness of the health care (including mental health care) system to respond to bioterrorism as it relates to children;
`(ii) needed changes to the health care and emergency medical service systems and emergency medical services protocols to meet the special needs of children; and
`(iii) changes, if necessary, to the national stockpile under section 121 of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 to meet the emergency health security of children.
`(C) COMPOSITION- The Advisory Committee shall be composed of such Federal officials as may be appropriate to address the special needs of the diverse population groups of children, and child health experts on infectious disease, environmental health, toxicology, and other relevant professional disciplines.
`(D) TERMINATION- The Advisory Committee terminates one year after the date of the enactment of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002.
`(3) EMERGENCY PUBLIC INFORMATION AND COMMUNICATIONS ADVISORY COMMITTEE-
`(A) IN GENERAL- For purposes of paragraph (1), the Secretary shall establish an advisory committee to be known as the Emergency Public Information and Communications Advisory Committee (referred to in this paragraph as the `EPIC Advisory Committee').
`(B) DUTIES- The EPIC Advisory Committee shall make recommendations to the Secretary and the working group under subsection (a) and report on appropriate ways to communicate public health information regarding bioterrorism and other public health emergencies to the public.
`(C) COMPOSITION- The EPIC Advisory Committee shall be composed of individuals representing a diverse group of experts in public health, medicine, communications, behavioral psychology, and other areas determined appropriate by the Secretary.
`(D) DISSEMINATION- The Secretary shall review the recommendations of the EPIC Advisory Committee and ensure that appropriate information is disseminated to the public.
`(E) TERMINATION- The EPIC Advisory Committee terminates one year after the date of the enactment of Public Health Security and Bioterrorism Preparedness and Response Act of 2002.
`(c) STRATEGY FOR COMMUNICATION OF INFORMATION REGARDING BIOTERRORISM AND OTHER PUBLIC HEALTH EMERGENCIES- In coordination with working group under subsection (a), the Secretary shall develop a strategy for effectively communicating information regarding bioterrorism and other public health emergencies, and shall develop means by which to communicate such information. The Secretary may carry out the preceding sentence directly or through grants, contracts, or cooperative agreements.
`(d) RECOMMENDATION OF CONGRESS REGARDING OFFICIAL FEDERAL INTERNET SITE ON BIOTERRORISM- It is the recommendation of Congress that there should be established an official Federal Internet site on bioterrorism, either directly or through provision of a grant to an entity that has expertise in bioterrorism and the development of websites, that should include information relevant to diverse populations (including messages directed at the general public and such relevant groups as medical personnel, public safety workers, and agricultural workers) and links to appropriate State and local government sites.'.
(b) STUDY REGARDING COMMUNICATIONS ABILITIES OF PUBLIC HEALTH AGENCIES- The Secretary of Health and Human Services, in consultation with the Federal Communications Commission, the National Telecommunications and Information Administration, and other appropriate Federal agencies, shall conduct a study to determine whether local public health entities have the ability to maintain communications in the event of a bioterrorist attack or other public health emergency. The study shall examine whether redundancies are required in the telecommunications system, particularly with respect to mobile communications, for public health

Pub. L. 107-188, 2002
Public Health Security and Bioterrorism Preparedness and Response Act of 2002
entities to maintain systems operability and connectivity during such emergencies. The study shall also include recommendations to industry and public health entities about how to implement such redundancies if necessary.
UPDATE: None

Pub. L. 107-296, 2002

Homeland Security Act of 2002

This document is included in its entirety on the Deskbook CD-ROM.

SEC. 102. SECRETARY; FUNCTIONS.

(a) SECRETARY.—

(1) IN GENERAL.—There is a Secretary of Homeland Security, appointed by the President, by and with the advice and consent of the Senate.

(2) HEAD OF DEPARTMENT.—The Secretary is the head of the Department and shall have direction, authority, and control over it.

(3) FUNCTIONS VESTED IN SECRETARY.—All functions of all officers, employees, and organizational units of the Department are vested in the Secretary.

(b) FUNCTIONS.—The Secretary—

(1) except as otherwise provided by this Act, may delegate any of the Secretary's functions to any officer, employee, or organizational unit of the Department;

(2) shall have the authority to make contracts, grants, and cooperative agreements, and to enter into agreements with other executive agencies, as may be necessary and proper to carry out the Secretary's responsibilities under this Act or otherwise provided by law; and

(3) shall take reasonable steps to ensure that information systems and databases of the Department are compatible with each other and with appropriate databases of other Departments.

(c) COORDINATION WITH NON-FEDERAL ENTITIES.—With respect to homeland security, the Secretary shall coordinate through the Office of State and Local Coordination (established under section 801) (including the provision of training and equipment) with State and local government personnel, agencies, and authorities, with the private sector, and with other entities, including by—

(1) coordinating with State and local government personnel, agencies, and authorities, and with the private sector, to ensure adequate planning, equipment, training, and exercise activities;

(2) coordinating and, as appropriate, consolidating, the Federal Government's communications and systems of communications relating to homeland security with State and local government personnel, agencies, and authorities, the private sector, other entities, and the public; and

(3) distributing or, as appropriate, coordinating the distribution of, warnings and information to State and local government personnel, agencies, and authorities and to the public.

(d) MEETINGS OF NATIONAL SECURITY COUNCIL.—The Secretary may, subject to the direction of the President, attend and participate in meetings of the National Security Council.

(e) ISSUANCE OF REGULATIONS.—The issuance of regulations by the Secretary shall be governed by the provisions of chapter 5 of title 5, United States Code, except as specifically provided in this Act, in laws granting regulatory authorities that are transferred by this Act, and in laws enacted after the date of enactment of this Act.

(f) SPECIAL ASSISTANT TO THE SECRETARY.—The Secretary shall appoint a Special Assistant to the Secretary who shall be responsible for—

(1) creating and fostering strategic communications with the private sector to enhance the primary mission of the Department to protect the American homeland;

(2) advising the Secretary on the impact of the Department's policies, regulations, processes, and actions on the private sector;

(3) interfacing with other relevant Federal agencies with homeland security missions to assess the impact of these agencies' actions on the private sector;

(4) creating and managing private sector advisory councils composed of representatives of industries and associations designated by the Secretary to—

(A) advise the Secretary on private sector products, applications, and solutions as they relate to homeland security challenges; and

(B) advise the Secretary on homeland security policies, regulations, processes, and actions that affect the participating industries and associations;

(5) working with Federal laboratories, federally funded research and development centers, other federally funded organizations, academia, and the private sector to develop innovative approaches to address homeland security challenges to produce and deploy the best available technologies for homeland security missions;

(6) promoting existing public-private partnerships and developing new public-private partnerships to provide for collaboration and mutual support to address homeland security challenges; and

(7) assisting in the development and promotion of private sector best practices to secure critical infrastructure.

(g) STANDARDS POLICY.—All standards activities of the Department shall be conducted in accordance with section 12(d) of the National Technology Transfer Advancement Act of 1995 (15 U.S.C. 272 note) and Office of Management and Budget Circular A–119.

SEC. 214. PROTECTION OF VOLUNTARILY SHARED CRITICAL INFRASTRUCTURE INFORMATION.

Pub. L. 107-296, 2002

(a) PROTECTION.—
(1) IN GENERAL.—Notwithstanding any other provision of law, critical infrastructure information (including the identity of the submitting person or entity) that is voluntarily submitted to a covered Federal agency for use by that agency regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by
an express statement specified in paragraph (2)—(A) shall be exempt from disclosure under section 552
of title 5, United States Code (commonly referred to as the Freedom of Information Act);
(B) shall not be subject to any agency rules or judicial doctrine regarding ex parte communications with a decision making official;
(C) shall not, without the written consent of the person or entity submitting such information, be used directly by such agency, any other Federal, State, or local authority, or any third party, in any civil action arising under Federal or State law if such information is submitted in good faith;
(D) shall not, without the written consent of the person or entity submitting such information, be used or disclosed by any officer or employee of the United States for purposes other than the purposes of this subtitle, except—
(i) in furtherance of an investigation or the prosecution of a criminal act; or
(ii) when disclosure of the information would be—
(I) to either House of Congress, or to the extent of matter within its jurisdiction, any committee
or subcommittee thereof, any joint committee thereof or subcommittee of any such joint committee; or
(II) to the Comptroller General, or any authorized representative of the Comptroller General, in
the course of the performance of the duties of the General Accounting Office.
(E) shall not, if provided to a State or local government or government agency—
(i) be made available pursuant to any State or local law requiring disclosure of information or records;
(ii) otherwise be disclosed or distributed to any party by said State or local government or government
agency without the written consent of the person or entity submitting such information; or
(iii) be used other than for the purpose of protecting critical infrastructure or protected systems, or
in furtherance of an investigation or the prosecution of a criminal act; and
(F) does not constitute a waiver of any applicable privilege or protection provided under law, such as trade secret protection.
(2) EXPRESS STATEMENT.—For purposes of paragraph (1), the term "express statement", with respect to information or records, means—
(A) in the case of written information or records, a written marking on the information or records substantially similar to the following: "This information is voluntarily submitted to the Federal Government in expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Information Act of 2002."; or
(B) in the case of oral information, a similar written statement submitted within a reasonable period following the oral communication.
(b) LIMITATION.—No communication of critical infrastructure information to a covered Federal agency made pursuant to this subtitle shall be considered to be an action subject to the requirements of the Federal Advisory Committee Act (5 U.S.C. App. 2).
(c) INDEPENDENTLY OBTAINED INFORMATION.—Nothing in this section shall be construed to limit or otherwise affect the ability of a State, local, or Federal Government entity, agency, or authority,
or any third party, under applicable law, to obtain critical infrastructure information in a manner not covered by subsection (a), including any information lawfully and properly disclosed generally or broadly to the public and to use such information in any manner permitted by law.
(d) TREATMENT OF VOLUNTARY SUBMITTAL OF INFORMATION.— The voluntary submittal to the Government of information or records that are protected from disclosure by this subtitle shall not be construed to constitute compliance with any requirement to submit such information to a Federal agency under any other
provision of law.
(e) PROCEDURES.—
(1) IN GENERAL.—The Secretary of the Department of Homeland Security shall, in consultation with appropriate representatives of the National Security Council and the Office of Science and Technology Policy, establish uniform procedures for the receipt, care, and storage by Federal agencies of critical
infrastructure information that is voluntarily submitted to the Government. The procedures shall be established not later than 90 days after the date of the enactment of this subtitle.
(2) ELEMENTS.—The procedures established under paragraph
(1) shall include mechanisms regarding—
(A) the acknowledgement of receipt by Federal agencies of critical infrastructure information that is voluntarily submitted to the Government;
(B) the maintenance of the identification of such information as voluntarily submitted to the Government
for purposes of and subject to the provisions of this subtitle;

Pub. L. 107-296, 2002

(C) the care and storage of such information; and
(D) the protection and maintenance of the confidentiality of such information so as to permit the sharing of such information within the Federal Government and with State and local governments, and the issuance of notices and warnings related to the protection of critical infrastructure and protected systems, in such manner as to protect from public disclosure the identity of the submitting person or entity, or information that is proprietary, business sensitive, relates specifically to the submitting person or entity, and is otherwise not appropriately in the public domain.
(f) PENALTIES.—Whoever, being an officer or employee of the United States or of any department or agency thereof, knowingly publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law, any critical infrastructure information protected from disclosure by this subtitle coming to him in the course of this employment or official duties or by reason of any examination or investigation made by, or return, report, or record made to or filed with, such department or agency or officer or employee thereof, shall be fined under title 18 of the United States Code, imprisoned not more than 1 year, or both, and shall be removed from office or employment.
(g) AUTHORITY TO ISSUE WARNINGS.—The Federal Government may provide advisories, alerts, and warnings to relevant companies, targeted sectors, other governmental entities, or the general public regarding potential threats to critical infrastructure as appropriate. In issuing a warning, the Federal Government shall take appropriate actions to protect from disclosure—
(1) the source of any voluntarily submitted critical infrastructure information that forms the basis for the warning; or
(2) information that is proprietary, business sensitive, relates specifically to the submitting person or entity, or is otherwise not appropriately in the public domain.
(h) AUTHORITY TO DELEGATE.—The President may delegate authority to a critical infrastructure protection program, designated under section 213, to enter into a voluntary agreement to promote critical infrastructure security, including with any Information Sharing and Analysis Organization, or a plan of action as otherwise defined in section 708 of the Defense Production Act of 1950 (50 U.S.C. App. 2158).

SEC. 892. FACILITATING HOMELAND SECURITY INFORMATION SHARING PROCEDURES.
(a) PROCEDURES FOR DETERMINING EXTENT OF SHARING OF HOMELAND SECURITY INFORMATION.—
(1) The President shall prescribe and implement procedures under which relevant Federal agencies—
(A) share relevant and appropriate homeland security information with other Federal agencies, including the Department, and appropriate State and local personnel;
(B) identify and safeguard homeland security information that is sensitive but unclassified; and
(C) to the extent such information is in classified form, determine whether, how, and to what extent to remove classified information, as appropriate, and with which such personnel it may be shared after such information is removed.
(2) The President shall ensure that such procedures apply to all agencies of the Federal Government.
(3) Such procedures shall not change the substantive requirements for the classification and safeguarding of classified information.
(4) Such procedures shall not change the requirements and authorities to protect sources and methods.
(b) PROCEDURES FOR SHARING OF HOMELAND SECURITY INFORMATION.—
(1) Under procedures prescribed by the President, all appropriate agencies, including the intelligence community, shall, through information sharing systems, share homeland security information with Federal agencies and appropriate State and local personnel to the extent such information may be shared, as determined in accordance with subsection (a), together with assessments of the credibility of such information.
(2) Each information sharing system through which information is shared under paragraph (1) shall—
(A) have the capability to transmit unclassified or classified information, though the procedures and recipients for each capability may differ;
(B) have the capability to restrict delivery of information to specified subgroups by geographic location, type of organization, position of a recipient within an organization, or a recipient's need to know such information;
(C) be configured to allow the efficient and effective sharing of information; and
(D) be accessible to appropriate State and local personnel.
(3) The procedures prescribed under paragraph (1) shall establish conditions on the use of information shared under paragraph (1)—
(A) to limit the redissemination of such information to ensure that such information is not used for an unauthorized purpose;
(B) to ensure the security and confidentiality of such information;
(C) to protect the constitutional and statutory rights of any individuals who are subjects of such information; and
(D) to provide data integrity through the timely removal and destruction of obsolete or erroneous names and information.
(4) The procedures prescribed under paragraph (1) shall ensure, to the greatest extent practicable, that the information sharing system through which information is shared under such paragraph include existing information sharing systems, including, but not limited to, the

Pub. L. 107-296, 2002

National Law Enforcement Telecommunications System, the Regional Information Sharing System, and the Terrorist Threat Warning System of the Federal Bureau of Investigation.
(5) Each appropriate Federal agency, as determined by the President, shall have access to each information sharing system through which information is shared under paragraph
(1), and shall therefore have access to all information, as appropriate, shared under such paragraph.
(6) The procedures prescribed under paragraph (1) shall ensure that appropriate State and local personnel are authorized to use such information sharing systems—
(A) to access information shared with such personnel; and
(B) to share, with others who have access to such information sharing systems, the homeland security
information of their own jurisdictions, which shall be marked appropriately as pertaining to potential terrorist activity.
(7) Under procedures prescribed jointly by the Director of Central Intelligence and the Attorney General, each appropriate Federal agency, as determined by the President, shall review and assess the information shared under paragraph (6) and integrate such information with existing intelligence.
(c) SHARING OF CLASSIFIED INFORMATION AND SENSITIVE BUT UNCLASSIFIED INFORMATION WITH STATE AND LOCAL PERSONNEL.—
(1) The President shall prescribe procedures under which Federal agencies may, to the extent the President considers necessary, share with appropriate State and local personnel homeland security information that remains classified or otherwise protected after the determinations prescribed under the procedures set forth in subsection (a).
(2) It is the sense of Congress that such procedures may include 1 or more of the following means:
(A) Carrying out security clearance investigations with respect to appropriate State and local personnel.
(B) With respect to information that is sensitive but unclassified, entering into nondisclosure agreements with appropriate State and local personnel.
(C) Increased use of information-sharing partnerships that include appropriate State and local personnel, such as the Joint Terrorism Task Forces of the Federal Bureau of Investigation, the Anti-Terrorism Task Forces of the Department of Justice, and regional Terrorism Early Warning Groups.
(d) RESPONSIBLE OFFICIALS.—For each affected Federal agency, the head of such agency shall designate an official to administer this Act with respect to such agency.
(e) FEDERAL CONTROL OF INFORMATION.—Under procedures prescribed under this section, information obtained by a State or local government from a Federal agency under this section shall remain under the control of the Federal agency, and a State or local law authorizing or requiring such a government to disclose information shall not apply to such information.
(f) DEFINITIONS.—As used in this section:
(1) The term "homeland security information" means any information possessed by a Federal, State, or local agency that—
(A) relates to the threat of terrorist activity;
(B) relates to the ability to prevent, interdict, or disrupt terrorist activity;
(C) would improve the identification or investigation of a suspected terrorist or terrorist organization; or
(D) would improve the response to a terrorist act.
(2) The term "intelligence community" has the meaning given such term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).
(3) The term "State and local personnel" means any of the following persons involved in prevention, preparation, or response for terrorist attack:
(A) State Governors, mayors, and other locally elected officials.
(B) State and local law enforcement personnel and firefighters.
(C) Public health and medical professionals.
(D) Regional, State, and local emergency management agency personnel, including State adjutant generals.
(E) Other appropriate emergency response agency personnel.
(F) Employees of private-sector entities that affect critical infrastructure, cyber, economic, or public health security, as designated by the Federal Government in procedures developed pursuant to this section.
(4) The term "State" includes the District of Columbia and any commonwealth, territory, or possession of the United States.
(g) CONSTRUCTION.—Nothing in this Act shall be construed as authorizing any department, bureau, agency, officer, or employee of the Federal Government to request, receive, or transmit to any other Government entity or personnel, or transmit to any State or local entity or personnel otherwise authorized by this Act to
receive homeland security information, any information collected by the Federal Government solely for statistical purposes in violation of any other provision of law relating to the confidentiality of such information.

UPDATE: None

441 U.S. 211

Douglas Oil Co of CA et al v. Petrol Stops Northwest et al

This document is included in its entirety on the Deskbook CD-ROM.

Excerpt at 218:
According to petitioners, this approach to disclosure under Fed. Rule Crim. Proc. 6 (e) is contrary to prior decisions of this Court indicating that "a civil litigant must demonstrate a compelling necessity for specified grand jury materials before disclosure is proper." Brief for Petitioners 16. n8

n8 As an initial matter, respondents argue that petitioners lack standing to object to the disclosure order, as the only interest in grand jury secrecy remaining in this case is a public one. Accord, *United States v. American Oil Co., 456 F.2d 1043 (CA3 1972)* (*per curiam*). Contra, *Illinois v. Sarbaugh, 552 F.2d 768* (CA7), cert. denied *sub nom. J. L. Simmons Co.* v. *Illinois, 434 U.S. 889 (1977).* There can be no question that there is standing under Art. III for petitioners to object to the disclosure order, as release of the transcripts to their civil adversaries could result in a substantial injury to them. See *Warth v. Seldin, 422 U.S. 490, 499 (1975).* Moreover, the interest petitioners assert is one legally protected under the Court's rulings concerning grand jury secrecy. One of the several interests promoted by grand jury secrecy is the protection of the innocent accused from disclosure of the accusations made against him before the grand jury. See n. 10, *infra*. Although petitioners in the present case were indicted and pleaded *nolo contendere*, under our decisions they nonetheless are legally entitled to protection, as there may have been accusations made for which no indictment was returned.

UPDATE: None

DoDD 5240.1, April 25, 1988

DoD Intelligence Activities

This document is included in its entirety on the Deskbook CD-ROM.

A. REISSUANCE AND PURPOSE
This Directive:

1. Reissues reference (a); implements references (b) through (d); updates policies; and shall be the only authority used as guidance by DoD intelligence components to collect, retain, or disseminate information concerning U.S. persons.
2. Continues in effect procedures previously approved by the U.S. Attorney General for use by DoD intelligence components under Presidential Directive NSC-9 (reference (e)).
3. Authorizes the publication of DoD 5240.1-R (reference (f)), consistent with DoD 5025.1-M (reference (g)) add this Directive.

B. APPLICABILITY AND SCOPE
This Directive:

1. Applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Organization of the Joint Chiefs of Staff (OJCS), the Unified and Specified Commands, and the Defense Agencies (hereafter referred to collectively as "DoD Components").
2. Applies to all intelligence activities of DoD Components.
3. Does not apply to authorized law enforcement activities carried out by DoD intelligence components having a law enforcement mission.

C. DEFINITIONS

1. Intelligence activities. The collection, production, and dissemination of foreign intelligence and counterintelligence by DoD intelligence components authorized under reference (b).
2. Foreign intelligence. Information relating to the capabilities, intentions, and activities of foreign-powers, organizations, or persons, but not including counter-intelligence except for information on international terrorist-activities.
3. Counterintelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or international terrorist activities, but not including personnel, physical, document, or communications security programs.
4. DoD intelligence components. All DoD Components conducting intelligence activities, including the following:
a. The National Security Agency Central Security Service (NSACSS).
b. The Defense Intelligence Agency (DIA).
c. The offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs.
d. The Office of the Deputy Chief of Staff for Intelligence (ODCSINT), U.S. Army.
e. The Office of Naval Intelligence (ONI).
f. The Office of the Assistant Chief of Staff, Intelligence (OAGSI), U.S. Air Force.
g. Intelligence Division, U.S. Marine Corps.
h. The Army Intelligence and Security Command (USAINSCOM).
i. The Naval Intelligence Command (NIC).
j. The Naval Security Group Command (NSGC).
k. The Air Force Intelligence Agency (AFIA).
l. The Electronic Security Command (ESC), U.S. Air Force.
m. The counterintelligence elements of the Naval Security and Investigative Command (NSIC).
n. The counterintelligence elements of the Air Force Office of Special Investigations (AFOSI).
o. The 650th Military Intelligence Group, Supreme Headquarters Allied Powers Europe (SHAPE).
p. Other intelligence and counterintelligence organizations, staffs, and offices, or elements thereof, when used for foreign intelligence or counter-intelligence purposes. The heads of such organizations, staffs, and offices, or elements thereof, shall, however, not be considered as heads of DoD intelligence components for purposes of this Directive.
5. Special activities. Activities conducted in support of national foreign policy objectives abroad, which are planned and executed so that the role of the U.S. Government is not apparent or acknowledged publicly, and functions in support of such activities, but which are not intended to influence U.S. political processes, public opinion, policies, or media, and do not include diplomatic activities or the collection and production of intelligence or related support functions.

DoDD 5240.1, April 25, 1988

6. United States person. A citizen of the United States; an alien known by the intelligence agency concerned to be a permanent resident alien; an unincorporated association organized in the United States or substantially composed of U.S. citizens or permanent resident aliens; or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

D. POLICY

1. All DoD intelligence activities shall be carried out in strict conformity with the U.S. Constitution, applicable law, E.O. 12333 (reference (b)), the policies and procedures authorized herein, and by other relevant DoD Directives, with special emphasis given to the protection of the constitutional rights and privacy of U.S. persons.
2. Reference (b) requires that the Department of Defense promulgate procedures to govern the collection, retention, and dissemination of information about U.S persons, and to govern the use of certain information-gathering techniques. These procedures, approved by the Attorney General of the United States, are contained in DoD 5240.1-R (reference (f)). No DoD intelligence component shall request any person or entity to undertake unauthorized activities.
a. Authority to employ the collection techniques prescribed by DoD 5240.1-R (reference (f)) shall be limited to that necessary to perform functions assigned to the DoD intelligence component concerned. Use of such techniques to collect information about U.S. persons shall be limited to the least intrusive means feasible.
b. DoD intelligence component employees shall report all intelligence activities that may violate a law, an Executive order, a Presidential Directive, or applicable DoD policy to the Inspector General or General Counsel responsible for the DoD intelligence component concerned, or to the Assistant to the Secretary of Defense (Intelligence Oversight) (ATSD(IO)).
3. DoD Components shall not conduct, or provide support for the conduct of, special activities except in times of war declared by the Congress or during a period covered by a report from the President to the Congress under the War Powers Resolution (50 U.S.C. 1541-1548, reference (h)), unless such actions have been approved by the President and directed by the Secretary of Defense.
4. Under no circumstances shall any DoD employee engage in, or conspire to engage in, assassination.

E. RESPONSIBILITIES

1. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD(C3I)) shall provide overall policy guidance for the conduct of DoD intelligence activities.
2. The Deputy Under Secretary of Defense (Policy) (DUSD(P)) shall provide overall policy guidance for the conduct of DoD counterintelligence activities.
3. The General Counsel, Department of Defense (GC, DoD), shall:
a. Serve as the central focal point for contact with, and reporting to, the Attorney General regarding the legal matters arising under this Directive.
b. Interpret this Directive and DoD 5240.1-R (reference (f)), as may be required.
4. The Assistant to the Secretary of Defense (Intelligence Oversight) (ATSD(IO)) shall serve as the central focal point for all contacts with the President's Intelligence Oversight Board (E.O. 12334, reference (c)) and shall perform the responsibilities assigned in DoD Directive 5148.11 (reference (i)).
5. The Heads of DoD Components shall ensure that their intelligence components implement this Directive and reference (f), as appropriate.

(e) Presidential Directive NSC-9, March 30, 1977
(f) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," December 11, 1982, authorized by this Directive
(g) DoD 5025.1-N, "Directives System Procedures," April 1981, authorized by DoD Directive 5025.1, October 16, 1980
(h) Title SO, United States Code, Sections 1541-1548, "The War Powers Resolution" (87 Stat. 555), P.L. 93-148
(i) DoD Directive 5148.11, "Assistant to the Secretary of Defense (Intelligence Oversight)," December 1, 1982

UPDATE: None

DoD Regulation 5240.1-R, December, 1982

Procedures governing the activities of DoD intelligence components that affect United States persons, December 1982

This document is included in its entirety on the Deskbook CD-ROM.

Procedure 1

A. 3. The procedures do not apply to law enforcement activities, including civil disturbance activities that may be undertaken by DoD intelligence components. When an investigation or inquiry undertaken pursuant to these procedures establishes reasonable belief that a crime has been committed, the DoD intelligence component concerned shall refer the matter to the appropriate law enforcement agency in accordance with procedures 12 and 15 or, if the DoD intelligence component is otherwise authorized to conduct law enforcement activities, shall continue such investigation under appropriate law enforcements procedures.

B. Criteria for Dissemination

Except as provided in section C., below, information about United States persons that identifies those persons may be disseminated without the consent of those persons only under the following conditions:

2. the recipient is reasonably believed to have a need to receive such information for the performance of a lawful governmental function, and is one of the following:

b. a law enforcement entity of federal, state, or local government and the information may indicate involvement in activities which may violate laws which the recipient is responsible to enforce…

UPDATE: None

DoDD 5200.27, January 7, 1980

Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense

Refs: (a) DoD Directive 5200.27, subject as above, December 8, 1975 (hereby canceled)
(b) DoD Directive 5240.1, "Activities of DoD Intelligence Components that Affect U.S. Persons," November 30, 1979

A. REISSUANCE AND PURPOSE

This Directive reissues reference (a) to establish for the Defense Investigative Program general policy, limitations, procedures, and operational guidance pertaining to the collecting, processing, storing, and disseminating of information concerning persons and organizations not affiliated with the Department of Defense.

B. APPLICABILITY AND SCOPE

1. Except as provided by subsection B.3., below, this Directive is applicable to the Office of the Secretary of Defense, Military Departments, Office of the Joint Chiefs of Staff, Unified and Specified Commands, and the Defense Agencies (hereafter referred to as "DoD Components").
2. The provisions of this Directive encompass the acquisition of information concerning the activities of:
a. Persons and organizations, not affiliated with the Department of Defense, within the 50 States, the District of Columbia, the Commonwealth of Puerto. Rico, and U.S. territories and possessions; and
b. Non-DoD-affiliated U.S. citizens anywhere in the world.
3. This Directive is not applicable to DoD intelligence components as defined by DoD Directive 5240.1 (reference (b)).
4. Authority to act for the Secretary of Defense in matters in this Directive which require specific approval are delineated in enclosure I.

C. POLICY
1. Department of Defense policy prohibits collecting, reporting, processing, or storing information on individuals or organizations not affiliated with the Department of Defense, except in those limited circumstances where such information is essential to the accomplishment of the Department of Defense missions outlined below.
2. Information-gathering activities shall be subject to overall civilian control, a high level of general supervision and frequent inspections at the field level.
3. Where collection activities are authorized to meet an essential requirement for information, maximum reliance shall be placed upon domestic civilian investigative agencies, Federal, State and local.
4. In applying the criteria for the acquisition and retention of information established pursuant to this Directive, due consideration shall be given to the need to protect DoD functions and property in the different circumstances existing in geographic areas outside the United States. Relevant factors include:
a. The level of disruptive activity against U.S. forces;
b. The competence of host country investigative agencies;
c. The degree to which U.S. military and host country agencies exchange investigative information;
d. The absence of other U.S. investigative capabilities; and
e. The unique and vulnerable position of U.S. forces abroad.

D. AUTHORIZED ACTIVITIES

DoD Components are authorized to gather information essential to the accomplishment of the following defense missions:
1. Protection of DoD Functions and Property. Information may be acquired about activities threatening defense military and civilian personnel and defense activities and installations, including vessels, aircraft, communications equipment, and supplies. Only the following types of activities justify acquisition of information under the authority of this subsection:
a. Subversion of loyalty, discipline, or morale of DoD military or civilian personnel by actively encouraging violation of law, disobedience of lawful order or regulation, or disruption of military activities.
b. Theft of arms, ammunition, or equipment, or destruction or sabotage of facilities, equipment, or records belonging to DoD units or installations.
c. Acts jeopardizing the security of DoD elements or operations or compromising classified defense information by unauthorized disclosure or by espionage.
d. Unauthorized demonstrations on active or reserve DoD installations.
e. Direct threats to DoD military or civilian personnel in connection with their official duties or to other persons who have been authorized protection by DoD resources.

DoDD 5200.27, January 7, 1980

f. Activities endangering facilities which have classified defense contracts or which have been officially designated as key defense facilities.
g. Crimes for which DoD has responsibility for investigating or prosecuting.
2. Personnel Security. Investigations may be conducted in relation to the following categories of persons:
a. Members of the Armed Forces, including retired personnel, members of the Reserve Components, and applicants for commission or enlistment.
b. DoD civilian personnel and applicants for such status.
c. Persons having need for access to official information requiring protection in the interest of national defense under the Department of Defense Industrial Security Program or being considered for participation in other authorized Department of Defense programs.
3. Operations Related to Civil Disturbance. The Attorney General is the chief civilian officer in charge of coordinating all Federal Government activities relating to civil disturbances. Upon specific prior authorization of the Secretary of Defense or his designee, information may be acquired which is essential to meet operational requirements flowing from the mission assigned to the Department of Defense to assist civil authorities in dealing with civil disturbances. Such authorization will only be granted when there is a distinct threat of a civil disturbance exceeding the law enforcement capabilities of State and local authorities.

E. PROHIBITED ACTIVITIES
1. The acquisition of information on individuals or organizations not affiliated with the Department of Defense will be restricted to that which is essential to the accomplishment of assigned Department of Defense missions under this Directive.
2. No information shall be acquired about a person or organization solely because of lawful advocacy of measures in opposition to Government policy.
3. There shall be no physical or electronic surveillance of Federal, State, or local officials or of candidates for such offices.
4. There shall be no electronic surveillance of any individual or organization except as authorized by law.
5. There shall be no covert or otherwise deceptive surveillance or penetration of civilian organizations unless specifically authorized by the Secretary of Defense, or his designee.
6. No DoD personnel will be assigned to attend public or private meetings, demonstrations, or other similar activities for the purpose of acquiring information, the collection of which is authorized by this Directive without specific prior approval by the Secretary of Defense, or his designee. An exception to this policy may be made by the local commander concerned, or higher authority, when, in his judgment, the threat is direct and immediate and time precludes obtaining prior approval. In each such case a report will be made immediately to the Secretary of Defense, or his designee.
7. No computerized data banks shall be maintained relating to individuals or organizations not affiliated with the Department of Defense, unless authorized by the Secretary of Defense, or his designee.

F. OPERATIONAL GUIDANCE
1. Nothing in this Directive shall be construed to prohibit the prompt reporting to law enforcement agencies of any information indicating the existence of a threat to life or property, or the violation of law, nor to prohibit keeping a record of such a report.
2. Nothing in this Directive shall be construed to restrict the direct acquisition by overt means of the following information:
a. Listings of Federal, State, and local officials who have official responsibilities related to the control of civil disturbances. Such listings may be maintained currently.
b. Physical data on vital public or private installations, facilities, highways, and utilities, as appropriate, to carry out a mission assigned by this Directive.
3. Access to information obtained under the provisions of this Directive shall be restricted to governmental agencies which require such information in the execution of their duties.
4. Information within the purview of this Directive, regardless of when acquired, shall be destroyed within 90 days unless its retention is required by law or unless its retention is specifically authorized under criteria established by the Secretary of Defense, or his designee.
5. This Directive does not abrogate any provision of the Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation, April 5, 1979, nor preclude the collection of information required by Federal statute or Executive Order.

G. EFFECTIVE DATE AND IMPLEMENTATION
This Directive is effective immediately. Forward two copies of implementing regulations to the Deputy Under Secretary of Defense (Policy Review) within 120 days.
W. Graham Claytor, Jr. Deputy Secretary of Defense

Enclosure - 1 Delegation of Authority

DoDD 5200.27, January 7, 1980
DELEGATION OF AUTHORITY A. The Secretary of the Army is designated to authorize those activities delineated in subsection D.3., basic Directive. This authority may not be further delegated to other than the Under Secretary of the Army. B. The Deputy Under Secretary of Defense (Policy Review) (DUSD(PR)) is designated to authorize those activities delineated in subsection E.5., basic Directive, within the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, and U.S. territories and possessions. This authority may not be delegated. The investigating DoD Component, prior to requesting approval for authorizations under this provision, shall coordinate prospective activities with the Federal Bureau of Investigation. C. The DUSD(PR) and the Secretaries of the Military Departments are designated to authorize those activities (delineated in subsection E.5., basic Directive) abroad when membership of the civilian organization is reasonably expected to include a significant number of non-DoD-affiliated U.S. citizens. This authority may not be further delegated to other than the Under Secretaries of the Military Departments. When the Military Department Secretary or Under Secretary exercises this delegation of authority, the DUSD(PR) shall be advised promptly. NOTE: "Abroad" means "outside the United States, its territories and possessions." D. The Secretaries of the Military Departments are designated to authorize in their Departments those activities delineated in subsection E.6., basic Directive, within the 50 states, the District of Columbia, the Common wealth of Puerto Rico, and U.S. territories and possessions. This authority may not be further delegated to other than the Under Secretaries of the Military Departments. E. The Secretaries of the Military Departments are designated to authorize in their Departments those activities (delineated in subsection E.6., basic Directive) abroad" when a significant number of non-DoD-affiliated U.S. citizens are expected to be present. This authority may be further delegated, in writing, as circumstances warrant, to an authorized designee. The DUSD(PR) will be notified immediately of such further delegations of authority. When the Secretary or Under Secretary of a Military Department or his designee exercises this delegated authority, the DUSD(PR) shall be advised promptly. F. The DUSD(PR) is designated to authorize those activities delineated in subsections E.7. and F.4., basic Directive. These authorities may not be further delegated.
Source: http://www.dtic.mil
UPDATE: None