THE FEDERAL LEGAL LANDSCAPE

A "LEGAL FOUNDATIONS" STUDY

Report 2 of 12

Report to the
President's Commission
on Critical Infrastructure Protection
1997

This report was submitted to the President's Commission on Critical Infrastructure Protection, and informed its deliberations and recommendations. This report represents the opinions and conclusions solely of its developers.

Contents

Page

Acknowledgments 1

Preface 2

Introduction 4

Part One: The Critical Infrastructures 5

- Overview 5
- Information & Communications Infrastructure 6
- Physical Distribution Infrastructure 9
- Banking & Finance Infrastructure 10
- Energy Infrastructure 11
- Vital Human Services Infrastructure 14
- Cross-Infrastructure Issues 16

Part Two: Summary of Agency Authorities 17

- Central Intelligence Agency 17
- Federal Bureau of Investigation 18
- Department of Energy 20
- Department of Transportation 23
- Federal Emergency Management Agency 26
- Department of Commerce 28

Department of the Treasury 31

Department of Justice 33

National Security Agency 34

U.S. Customs Service 35

Bureau of Alcohol, Tobacco & Firearms 37

U.S. Secret Service 37

Department of Education 39

General Services Administration 39

Federal Communications Commission 42

U.S. Postal Service 47

Department of the Interior 48

Department of State 54

U.S. Information Agency 55

Nuclear Regulatory Commission 56

Federal Energy Regulatory Commission 57

Department of Agriculture 60

Securities and Exchange Commission 61

Board of Governors of the Federal Reserve 61

Federal Deposit Insurance Corporation 63

International Trade Commission 64

Conclusion 66

Table of Authorities 67

Appendix – Federal Agency Contacts_____79

Acknowledgments

The *Legal Foundations* series of reports of the President's Commission on Critical Infrastructure Protection (PCCIP) resulted from the concerted efforts and hard work of several individuals. The Commission gratefully acknowledges Commissioner Stevan D. Mitchell and Assistant General Counsel Elizabeth A. Banker for their leadership and important contributions in developing the *Legal Foundations* series of reports. Their research, writing and analytical contributions were essential to the success of the effort.

The Commission also acknowledges Lee M. Zeichner, Esq. of LegalNet Works Incorporated and his staff, for conceptualizing and maintaining the legal issues database and for providing tireless research support. Finally, the Commission acknowledges the contributions of Senior Consultant Paul Byron Pattak for his deft editing of this compilation.

Preface

Executive Order 13010 established the President's Commission on Critical Infrastructure Protection (PCCIP) and tasked it with assessing the vulnerabilities of, and threats to, eight named critical infrastructures and developing a national strategy for protecting those infrastructures from physical and cyber threats. The Executive Order also required that the PCCIP consider the legal and policy issues raised by efforts to protect the critical infrastructures and propose statutory and regulatory changes necessary to effect any subsequent PCCIP recommendations.

To respond to the legal challenges posed by efforts to protect critical infrastructures, the PCCIP undertook a variety of activities to formulate options and to facilitate eventual implementation of PCCIP recommendations by the Federal government and the private sector. The PCCIP recognized that the process of infrastructure assurance would require cultural and legal change over time. Thus, these activities were undertaken with the expectation that many would continue past the life of the PCCIP itself.

The *Legal Foundations* series of reports attempts to identify and describe many of the legal issues associated with the process of infrastructure assurance. The reports were used by the PCCIP to inform its deliberations. The series consists of 12 reports:

1. *Legal Foundations: Studies and Conclusions*
2. *The Federal Legal Landscape*
3. *The Regulatory Landscape*
4. *Legal Authorities Database*
5. *Infrastructure Protection Solutions Catalog*
6. *Major Federal Legislation*
7. *Adequacy of Criminal Law and Procedure (Cyber)*
8. *Adequacy of Criminal Law and Procedure (Physical)*
9. *Privacy and the Employer-Employee Relationship*
10. *Legal Impediments to Information Sharing*
11. *Federal Government Model Performance*
12. *Approaches to Cyber Intrusion Response*

and two special studies:

- *Information Sharing Models*
- *Private Intrusion Response*

Legal Foundations: Studies and Conclusions is the overall summary report. It describes the other reports, the methodologies used by the researchers to prepare them, and summarizes the possible approaches and conclusions that were presented to the PCCIP for its consideration. The series has been sequenced to allow interested readers to study in detail a specific area of interest. However, to fully appreciate the scope of the topics studied and their potential interaction, a review of the entire series is recommended.

Introduction

This report represents the first effort of its kind to characterize the legal and regulatory structures of the critical infrastructures as they pertain to infrastructure assurance. As a first step, surveys were sent to the ten agencies represented on the Commission: the Departments of Commerce, Defense, Energy, Justice, Transportation, and the Treasury, The Central Intelligence Agency, the Federal Bureau of Investigation, the Federal Emergency Management Agency, and the National Security Agency.[1] The surveys asked agency counsel to identify the legal authorities and mechanisms associated with their agency that related to infrastructure assurance. The survey also asked that existing or planned programs related to infrastructure assurance and other agencies with a stake in the activities be identified. After the initial agency submissions were received, it was apparent that the federal government's authorities with respect to infrastructure assurance were spread across a vast number of agencies and departments. Assistance was then requested from another twenty-five federal organizations.

The first part of this report provides a high-level overview of the legal landscape of each of the critical infrastructures. Though this effort does incorporate some additional sources, [2] it relies primarily on the submissions received, thus focusing on the federal government's legal and regulatory authorities. The report then presents the results of the two-stage agency survey process. It proceeds agency-by-agency and, in some cases, office-by-office and describes each of the relevant body's authority and jurisdiction and its current mechanisms and programs relating to infrastructure assurance. It also attempts to identify authorities or mechanisms and, in some instances, to merely spot infrastructure assurance-related issues. The efforts to characterize the legal landscape of infrastructure assurance has lead to the identification of many legal and policy issues and will help drive the implementation process for the Commission's recommendations.

---

[1] Exec. Order 13010 (July 15, 1996); 61 Fed. Reg. 37347, 37348 (July 17, 1996).

[2] The PCCIP Legal Authorities Database includes a broader range of materials including relevant authorities at federal, state, and international levels as well as materials from the private sector.

Part One

The Critical Infrastructures

Overview

A number of difficulties arise in any effort to characterize the legal landscape of infrastructure assurance. The first and most fundamental challenge arises with regard to identifying and collecting infrastructure assurance-related authorities. Typically an attorney confronted with a research project will be able to recognize the issue and identify relevant bodies of law. Research then may consist merely of typing a word or phrase into the search engine of a legal database, or even the Internet. However, for infrastructure assurance there is no existing body of law– no keyword under which to search. The task thus requires an upfront recognition of the types of issues which may impact, positively or negatively, the fulfillment of certain infrastructure assurance objectives.

With eight infrastructures named in the Executive Order and the disparate subparts contained within each of those critical infrastructures, the next challenge is in many ways one of sheer volume. Massive amounts of law have been promulgated and implemented under the auspices of the critical infrastructures. None of these laws were specifically directed at "infrastructure assurance," but many impact directly on infrastructure assurance concerns. Physical security, information security, reliability and safety of services, emergency authorities, law enforcement, intelligence and defense activities are just a few of the legal considerations which should be taken into account in compiling the legal landscape.

In other areas, the law and thus the structure and assurance level of the infrastructures are in flux. Recent deregulation and restructuring efforts in such industries as telecommunications and electric power may impact these infrastructures' abilities to address infrastructure assurance concerns. It is difficult, though, to analyze the impacts of such changes on infrastructure

assurance and the legal landscape until the authorities and mechanisms have been more fully implemented.

This preliminary effort should make clearer the areas where federal involvement is historically and legally precedented and those areas which are better left to the states, associations, and individual owners and operators. It may be necessary to examine these roles, particularly as they evolve in this area of increased competition, deregulation and restructuring, in the future. The current legal landscape of infrastructure assurance appears to provide a rich body of resources tapped and untapped for meeting infrastructure assurance objectives.

Information and Communications Infrastructure

To the extent any of the critical infrastructures are owned by the federal government, full authority exists to protect them from potential threats and vulnerabilities. If the infrastructure is privately owned, a federal role is generally premised on the infrastructures involvement in interstate commerce.

This is true in the area of telecommunications. For example on the government side, the GSA administers the federal telephone system under the FTS 2000 program.[3] NCS ensures the availability of telecommunications service during emergencies through GETS. NSA is charged with the security of the government telecommunications services.[4] Programs are in place for other means of communications as well as, such as NTIA's role in spectrum allocation and use of satellites for the government[5] and BLM's emergency radio capabilities.[6] Other federal government agencies also play more narrow and defined roles, such as the U.S. Secret Service's role in investigating access device fraud.[7]

[3] *See infra* p. 37.

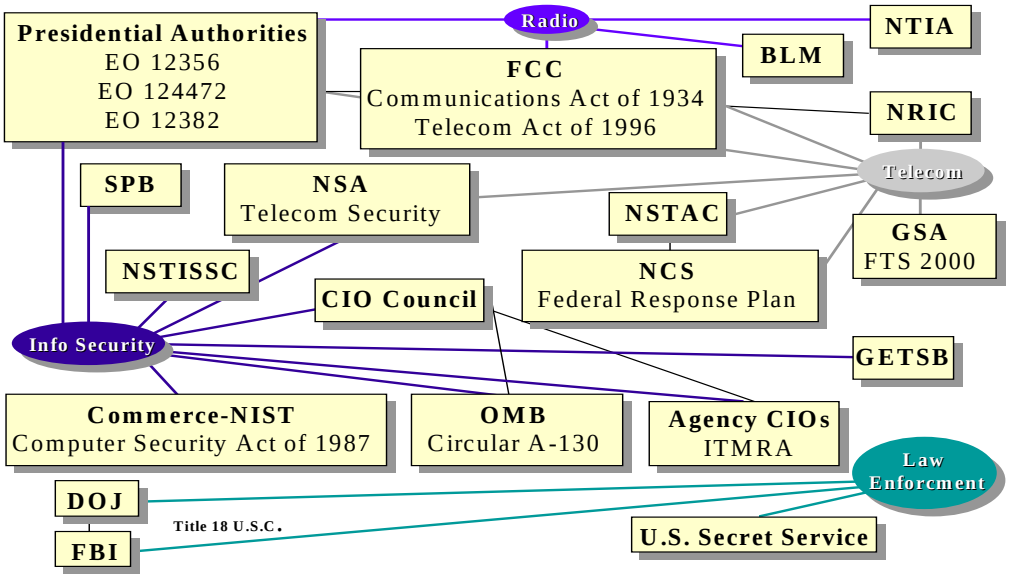
[4] *See* discussion of NSA authorities *infra* pp. 31-32.

[5] *See infra* p. 25.

[6] *See infra* p. 45.

[7] *See infra* p. 35.

The Federal Legal Landscape: *Information & Communications*



Jurisdiction over privately-owned communications media is given to the FCC based on the interstate commerce implications of such communications. The exact nature of the FCC's jurisdiction does vary depending on the communications media in question.[8] However, the FCC's general mandate is to ensure that safe and reliable communications services are widely available. To accomplish this mission, the FCC has regulatory authority to issue licenses, make appropriate regulations, issue fines and other penalties. The FCC uses many of these authorities to ensure the safety and reliability of communications, however there may be room for a greater focus on infrastructure assurance objectives. In addition, state Public Utility Commissions (PUCs) generally regulate facility and equipment siting and rate setting. While the focus of both the FCC, at the federal level, and the PUCs, at the state level, have traditionally been on providing universal service, these bodies are now moving their focus toward access and continuity of service. For example, the FCC chartered Network Reliability and Interoperability Council currently has reporting requirements in place for outages, but is considering whether the thresholds for reporting should be changed in light of industry restructuring and security and reliability concerns. Also, the impact that some of the provisions of the Telecommunications Act of 1996, such as new obligations for interconnection, unbundling of services, and resale of infrastructure access on existing providers of local exchange services, will have on infrastructure objectives is not yet clear and may depend on the manner of FCC implementation, a process that is still

[8] *See* discussion of FCC authorities *infra* pp. 38-43.

underway. In the meantime, new technologies are being introduced in the communications arena everyday.

For protection of information systems specifically, much the same pattern is found. Government systems have a wide and diverse group of federal entities charged with some aspect of their protection and proper functioning. NIST has the primary responsibility for setting standards for information security,[9] but other entities such as NSA, SPB, CSSPAB, CIO Council, and GITSB, provide inputs and play a role in federal information security endeavors. Individual agencies, through their CIOs, also bear considerable responsibility for their own systems. Some agencies have risen to the challenge more readily than others. FCC, for example, has its own computer emergency response capability and conducts "red teaming" activities.[10]

In contrast, there is no federal government focal point for privately-owned critical infrastructure information security. NIST and NSA may provide technical expertise, but any regulatory requirements are derived from the overall regulatory scheme of the oversight agency. FERC, for example, requires interstate transmitters of energy to link to the OASIS system and has put in place requirements for the security of that system.[11] Few agencies have mandated such requirements, though they most likely have the statutory authority to do so in order to protect the safe and proper operation of the critical infrastructures they regulate.

Whether government or private communications systems, two needs are critical to infrastructure assurance objectives—law enforcement and education and awareness. The Secret Service,[12] to a limited extent, and the Department of Justice[13] both have jurisdiction over crimes in the communications infrastructure. Education efforts for proper use of computers and computer ethics may be funded for the private sector through Department of Education programs.[14] OPM and individual agencies are generally responsible for training government employees on such topics.

---

[9] *See infra* p. 27.

[10] *See* discussion of FCC Computer Security Program *infra* pp. 42-43.

[11] For further discussion of OASIS system and FERC regulations *see infra* p. 55.

[12] *See infra* p. 34.

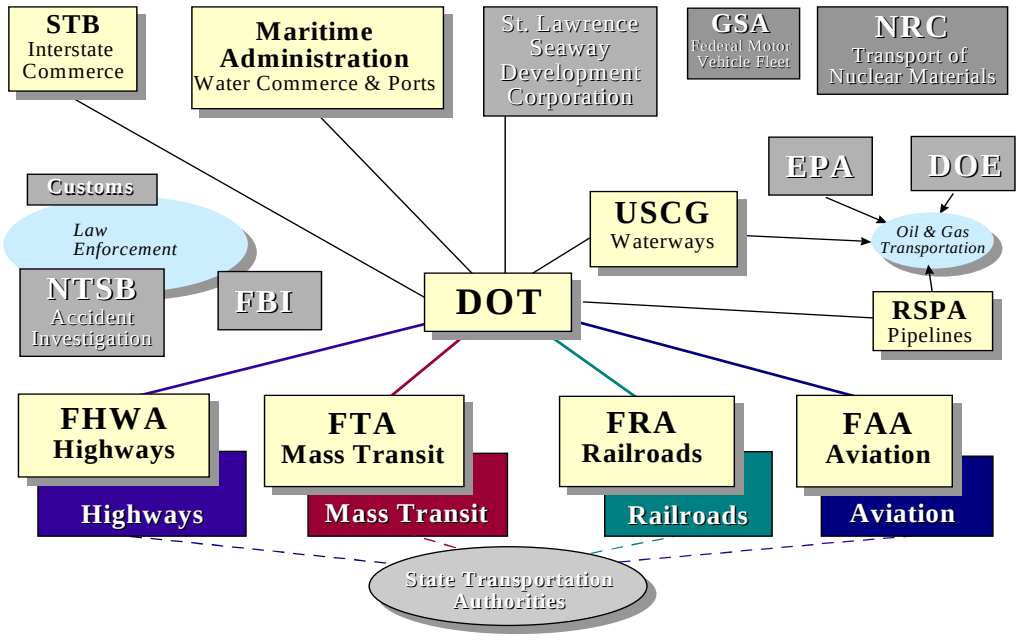
[13] *See* FBI summary *infra* pp. 15-16.

[14] *See infra* pp. 35-36.

Physical Distribution

The transportation infrastructure's legal landscape is particularly difficult to characterize because of the unique nature of each of the various modes of transportation involved. Rather than a centralized and cohesive structure, the legal landscape is fragmented. The Department of Transportation is itself broken into a number of individual agencies to address each of the modes of transport.[15] These include the Federal Railroad Administration, the Federal Aviation Administration, the Federal Highway Administration, the Federal Transit Administration, the Surface Transportation Board, the U.S. Coast Guard, and the Maritime Administration. More specialized federal bodies also exist to address specific elements of the transportation infrastructure, such as the St. Lawerence Seaway. This mode-specific approach to governance is echoed in the state structures which regulate transportation.

The Federal Legal Landscape: *Physical Distribution*



The nature of these agencies' authorities over the modes of transportation they concern also differ tremendously. While air transportation is more heavily regulated by the FAA, the Federal Highway Administration and Federal Transit Authority play a more influential role through grant programs and studies aimed

[15] *See infra* pp. 19-22 for further discussion of DOT authorities.

at safety. This may be due to the *intra*state nature of many of these modes of transportation, necessitating a more state-centric approach to oversight. States and local governments bear tremendous responsibility for the transportation infrastructure, much of it being owned by those government entities. Highways and roads, bridges, even airports are usually owned and maintained by municipal or state authorities. However, to the extent transportation involves a specific federally-regulated material, such as nuclear materials, a strong federal role will be defined for the agency primarily responsible for such items—in this case the Nuclear Regulatory Commission.[16]

An effective legal strategy for infrastructure assurance may need to be tailored to each individual mode of transport. Authorities to conduct inspections, require training, and security measures may exist at the federal or state level for any of the elements of the transportation infrastructure. There may also be room for improvement in their current implementation. For example, there are no security regulations for rail passenger terminals similar to those for airports.[17] In addition, the impact of information technology and automation will have to be carefully studied to determine the proper use of legal authority for infrastructure assurance objectives. Electronic systems already control air traffic and rail traffic, and are quickly moving into urban traffic control centers.[18]

Banking and Finance

Despite the complex web of financial institutions and other entities involved in the banking and finance infrastructure, federal regulation and control of the infrastructure is fairly tightly centered and maintained. The Federal Reserve[19] and FDIC[20] regulate many aspects of the operations of the banks they oversee. These organizations have already had to respond to important infrastructure-related concerns through their regulatory structure with the increasing popularity of electronic commerce. The Federal Financial Institutions Examinations Council is working to standardize the practices among the federal regulators regarding electronic fund transfers.[21]

---

16 *See infra* pp. 55-52.

17 *See* Argonne National Laboratory, *Overview of the Impacts of Regulatory Agency Practices on Critical Infrastructure Protection*, Prepared for PCCIP § 7 (July 15, 1997).

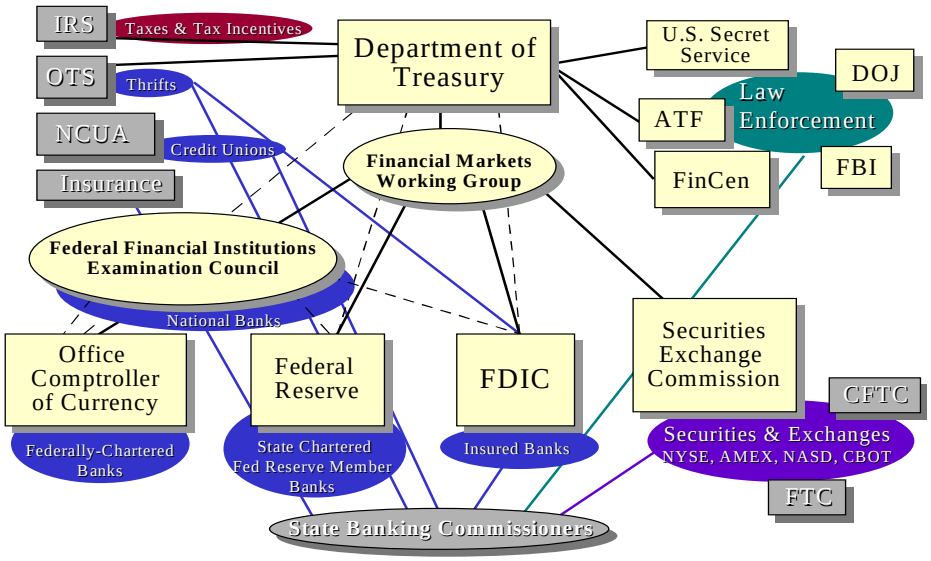
18 *Id.*

19 *See infra* pp. 57-58.

20 *See infra* pp. 58-59.

21 *See infra* p. 59.

The Federal Legal Landscape: *Banking and Finance*



The SEC also has the necessary authority to respond to incidents disrupting the trading of securities, though it has not yet been forced to invoke such authority.[22] The Department of Treasury has attempted to play an integrating role for its many constituents--OCC, FDIC, IRS—through such efforts as the Financial Markets Working Group which is designed to share information and to find solutions to various problems in the banking and finance area.[23] This group has lately begun to focus on infrastructure assurance-related topics such as disruptions. The Secret Service has jurisdiction over crimes involving currency and other financial instruments.[24] The FBI and Department of Justice also have jurisdiction over federal crimes in the banking and finance infrastructure.[25]

Energy

As was demonstrated in the telecommunications arena, federal authority differs considerably from government to privately owned systems. DOE has the statutory authority to require government energy facilities to meet any

[22] *See infra* pp. 56-57 for discussion of SEC authorities.

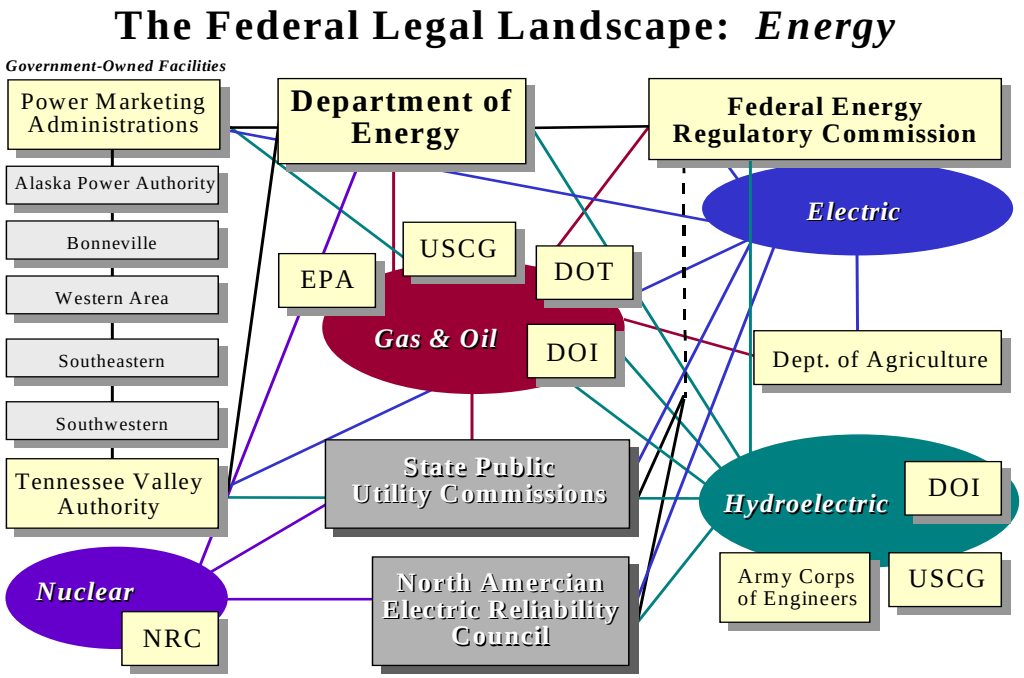
[23] *See infra* p. 28.

[24] *See infra* pp. 34-35 for discussion of Secret Service jurisdiction.

[25] *See infra* pp. 15-16.

requirements necessary to meet infrastructure assurance objectives.[26] While these currently involve some physical security requirements, it is not otherwise clear to what extent such objectives are currently taken into account.

Both DOE and FERC have significant authority over interstate energy facilities even if privately owned.[27] State PUCs have jurisdiction over retail sale of electricity. This includes the authority to issue permits and set standards for construction. This authority differs depending on the energy source. In fact, nuclear energy is regulated at the federal level by the NRC almost exclusively.[28]



Generally, federal energy regulators have licensing authority, ability to impose reporting requirements and to conduct investigations, and to make regulations for operation of energy facilities. The DPA provides powers to assist in reconstitution following an emergency.[29] And specific powers such as ordering interconnection or expanded service and tariff review could be used for

---

[26] Government-owned energy facilities are discussed *infra* pp. 16-17.

[27] *See infra* pp. 16-19 (discussion of DOE authorities) and pp. 53-56 (discussion of FERC authorities).

[28] *See* discussion of NRC authorities *infra* pp. 51-52.

[29] *See, e.g.*, discussion *infra* p. 17.

infrastructure assurance objectives.[30] While sufficient authority is in place, the federal government has not yet required substantial physical, or for that matter cyber, security measures for non-nuclear energy facilities.

Pipelines pose more complex legal questions than do other types of energy-related infrastructures. FERC has authority over the interstate transportation and sale of gas and oil.[31] The Department of Transportation is responsible for the safety and construction standards for pipelines, including those which transport oil and gas.[32] The EPA also has a role in the transport and storage of oil and gas. Before infrastructure assurance objectives related to pipelines are implemented, the roles of these agencies should be clarified.

There is sufficient authority at the federal level to enhance infrastructure assurance within the energy infrastructure. However, as the industry continues its move toward competition in electric generation, careful consideration must be given to using those authorities to ensure that infrastructure assurance objectives are met. In addition to DOE, FERC and NRC, unique roles are also played by the Department of Agriculture in development of universal service in rural areas,[33] BLM in the protection of utilities on public lands and leasing of lands for production of oil and gas,[34] state public utility commissions, and associations such as the North American Electric Reliability Council (NERC). NERC, a voluntary association of utilities formed in 1968, is becoming an increasingly important presence in the energy industry.[35] NERC just recently voted for its reliability standards to be obligatory for its members. The roles of the state PUCs will also be important to follow as the infrastructure undergoes this change. Due to this fragmentation of the jurisdiction over the energy infrastructure, all of these legal and regulatory entities should be taken into account when evaluating the legal landscape.

---

[30] The potential uses for such regulatory authorities are discussed within the FERC summary. *See infra* pp. 53-56.

[31] *See infra* p. 55.

[32] *See infra* p. 19.

[33] *See* discussion of Department of Agriculture programs *infra* p. 56.

[34] *See infra* p. 47.

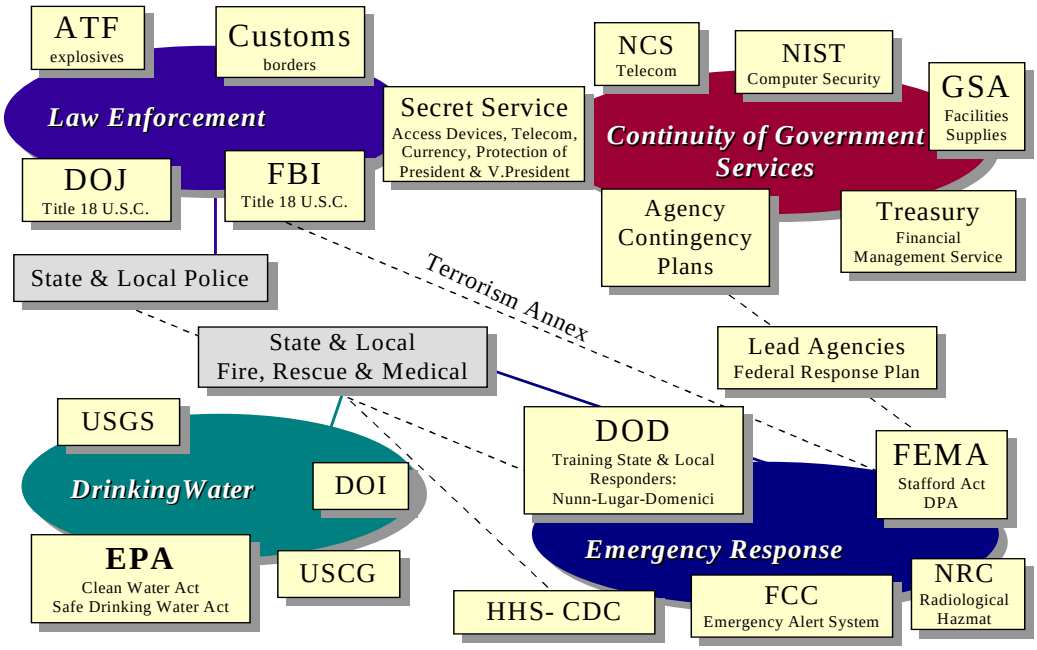
[35] NERC is discussed extensively in Argonne National Labs' Regulatory Landscape Report to the President's Commission on Critical Infrastructure protection. *See supra* note 16 § 4.

Vital Human Services

(Including Emergency Services and Continuity of Government Services)

Vital Human Services refers to a wide range of activities at federal, state and local levels that are both crucial for everyday life and needed in the event of an emergency. The responsibilities for provision of services related to police, fire, and medical care belong principally to local and state governments. Under unique circumstances, such as a major disaster that strains state response capabilities, the Federal government has the authority to respond under the Stafford Act.[36] Emergency functions are administered by FEMA, but involve many of the federal agencies under a management structure set out in the Federal Response Plan. Other avenues, such as the Nunn-Lugar-Domenici Weapons of Mass Destruction legislation of 1996, provide training or access to equipment for first responders.

The Federal Legal Landscape*: Vital Human Services*



The government has planned for continuity of its own communications capabilities through GSA, NCS and other avenues for the provision of telecommunications service during an emergency.[37] The Federal Response Plan

[36] *See infra* pp. 23-24.

[37] *See infra* p. 37.

and other documents divide responsibilities during emergencies among the federal agencies. It is not currently clear whether the federal government has adequately taken into account interdependencies among the critical infrastructures in its own planning for emergencies.

Individual agencies, in addition to GSA, have taken measures in the wake of the Oklahoma City bombing to increase physical security of their facilities and to prepare for emergencies. Some agencies have prepared evacuation plans and plans for reconstitution after an incident.[38] Disparities between agencies are similar to those in the area of information security, where some are well prepared to handle a contingency and others have not taken the need for security precautions and advanced planning as seriously. As provision of government services moves increasingly "on-line," agencies that provide such services will undoubtedly feel pressure to ensure the integrity and reliability of those services from potential cyber-related disruptions. However, no government entity has clear and authoritative enforcement authority over the implementation of such requirements.

If a critical infrastructure incident reaches a level where it impacts national interests, several federal mechanisms and authorities are applicable. Cross-infrastructure services such as law enforcement and intelligence are important parts of averting national security level incidents pertaining to infrastructures. The FBI[39] and CIA[40] have adequate authority to include the critical infrastructures within the ambit of their normal investigatory and intelligence related functions. In fact, the FBI has taken several steps to improve its awareness and ability to respond to critical infrastructure incidents such as the Key Asset Program and the CITAC which houses the Infrastructure Protection Task Force.[41] The Department of State, Customs, Federal Emergency Management Agency, Secret Service, the prosecutors of the Department of Justice, and others may also be involved in an infrastructure-related incident.

The federal government plays only a limited role in protection of the drinking water supply. Local Governments and state PUCs are the primary authority for protection of the drinking water supply. However, the EPA has a strong role related to keeping drinking water safe and clean.[42] The EPA sets standards adopted and followed by most local water infrastructure operators. These standards generally address issues such as vulnerability to industrial or natural

---

[38] *See, e.g.,* summary of U.S. Postal Service authorities and mechanisms *infra* p. 44.

[39] *See* discussion of FBI authorities *infra* pp. 15-16.

[40] *See* discussion of CIA authorities *infra* pp. 14-15.

[41] *See infra* pp. 15-16 for further discussion of these FBI programs.

[42] *See supra* note 16 at 97 (discussion of EPA role in drinking water infrastructure).

conditions, but do not address intentional sabotage of drinking water quality. Monitoring of water quality will likely continue to expand under the existing legal regime. The U.S. Geological Survey also runs a National Water Quality Assessment program.[43] The Bureau of Reclamation also is involved in water operations though usually only at the onset of development of a processing operation.[44]

Cross-Infrastructure Issues

Many of the legal authorities collected during the survey process do not fit neatly into one of the critical infrastructures, rather they cut across all of the infrastructures in special ways. Law enforcement and intelligence functions are two such examples which are well documented within the agency submissions.[45] However, there are other examples that pervade the way all of the federal agencies surveyed are carrying out their missions, but were not included within the agency submissions. Recent "Reinventing Government" initiatives, such as the Government Performance and Results Act,[46] the Information Technology Management Reform Act,[47] and other authorities that seek to include risk management techniques in the regulatory structure, set out a new way of conducting government business.[48] These acts set the tone for future legal and regulatory efforts related to infrastructure assurance.

---

[43] *See infra* p. 46.

[44] *See infra* pp. 48-49.

[45] *See, e.g., infra* pp. 14-15 (CIA); pp. 15-16 (FBI); pp. 33-34 (U.S. Secret Service); pp. 31-32 (Customs Service); pp. 32-33 (ATF).

[46] Pub. Law No. 103-62 (1993).

[47] Pub. Law No. 104-106 (1996).

[48] *See, e.g.,* Pub. Law No. 104-304 (1996) (Accountable Pipelines Safety and Partnership Act of 1996); *see also supra* note 16 at 54-55.

Part Two

Summary of Agency Authorities

Central Intelligence Agency

The CIA has the authority to undertake intelligence and counterintelligence gathering and dissemination activities involving any of the critical infrastructures to the extent that there is foreign intelligence involving those infrastructures.[49] If the investigation or gathering of such intelligence and counterintelligence is to take place within the United States, the CIA efforts must be coordinated with the Federal Bureau of Investigation.[50] The CIA does not have police, subpoena, law enforcement or internal security powers.[51] However, a recent amendment to the National Security Act allows the Intelligence Community to collect information abroad about non-U.S. persons in order to support a U.S. law enforcement or counterintelligence investigation upon request of a U.S. law enforcement agency.[52]

---

[49] The National Security Act of 1947, 50 U.S.C. §§ 401 *et seq*., and the Central Intelligence Agency Act of 1949, 50 U.S.C. §§ 403a *et seq*., define the CIA's authority with regard to collection of intelligence data. Executive Order 12333 (1981), however, contains the specific scope of the intelligence activities in which the CIA may engage and limits those activities to the gathering of "foreign intelligence" and "counterintelligence." "Foreign intelligence" is specifically defined in the Executive Order as "information relating to the capabilities, intentions and activities of foreign powers, organizations or persons, but not including counterintelligence except for information on international terrorist activities." Exec. Order 12333 § 3.4(d). The Executive Order also defines counterintelligence as "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 person, or international terrorist activities, but not including personnel, physical, document or communications security programs." Exec. Order 12333 § 3.4(a).

[50] Exec. Order 12333 § 1.8(a) & (c). *See also infra* pp. 15-16 (Federal Bureau of Investigation Summary). Similarly, the FBI, which is tasked with collecting counterintelligence primarily within the United States, must coordinate counterintelligence gathering outside the U.S. with the CIA. Exec. Order 12333 § 1.14(a) & (b).

[51] 50 U.S.C. § 403-3(d)(1).

[52] 50 U.S.C. § 403 (1996).

Actual mechanisms in place relating to the various infrastructures are limited to the protection and reconstitution of CIA's own telecommunications, power, emergency services, and critical government operations. The CIA may engage in covert actions to "influence political, economic, or military conditions abroad" with the approval of the President.[53] The Director of the Central Intelligence (DCI) plays a pivotal role in intelligence community, sitting on the Committee on Transnational Threats,[54] approving assignment of funds under the National Foreign Intelligence Program,[55] and coordinating relationships with foreign governments.[56] In addition, the DCI reports to Congress on potential threats to the national information infrastructure from foreign powers and, semi-annually reports to Congress on foreign nations' acquisition of technology relating to weapons of mass destruction and advanced conventional munitions.[57]

Federal Bureau of Investigation

The Federal Bureau of Investigation (FBI) has been delegated the authority to investigate all crimes against the United States.[58] In fulfilling its statutory mandate, the Bureau is tasked with acting as the lead agency in all crimes for which it has concurrent or primary jurisdiction and which involve terrorist activities.[59] In addition, FBI is to take charge of investigations involving espionage, sabotage, subversive activities and related matters. The only substantial limits on the scope of the FBI's investigatory authority over violations of federal law come from specific grants of investigatory power to other investigative agencies.[60] Among such provisions is Executive Order 12333 which requires that the FBI conduct counterintelligence outside the United States in

---

[53] 50 U.S.C. § 413b(a) & (e).

[54] 50 U.S.C. § 402(I)(1) (1996).

[55] 50 U.S.C. § 403-3(c).

[56] 50 U.S.C. § 403-4(e).

[57] H.R. 3259 §§ 310 & 711.

[58] 28 U.S.C. § 533 vests the Attorney General with the power to appoint officials to "detect and prosecute crimes against the United States." The Attorney General has delegated the investigatory authority to the FBI. 28 C.F.R. Part 0.85(a).

[59] 28 C.F.R. Part 0.85 defines "terrorist activities" as "unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."

[60] *See* 28 C.F.R. part 0.85(a).

coordination with the CIA.[61] The FBI suggests that 28 U.S.C. § 533 is sufficiently broad that it may be extended beyond federal crimes in that it contains a provision to deal with "unanticipated exigent circumstances."[62] In combination, the various federal statutes addressing protection of infrastructures[63] and the authorization to conduct counterintelligence activities, which specifically include protection of certain infrastructures,[64] provide a broad basis for FBI involvement in infrastructure assurance.

The broad nature of the FBI's authority is evident from the variety of mechanisms currently in place within the Bureau aimed at infrastructure assurance. The Strategic Intelligence Operations Center allows the FBI to monitor incidents and coordinate responses on a national and potentially world-wide level. The FBI has developed plans to deal with unconventional crisis situations including a Nuclear Terrorism Response Plan, a Chemical/Biological Incident Contingency Plan, the Critical Incident Response Group, and the Hostage Rescue Team. The Computer Intrusion and Infrastructure Threat Analysis Center was established to handle computer/communications related infrastructure assurance issues, but its role has been expanded to develop the expertise necessary to deal with any infrastructure threat. In addition to these programs, the FBI has developed an Infrastructure Vulnerability/Key Asset Program as a counter terrorism mechanism. Unfortunately, this program has not reached its full potential and currently has an out-of-date database on the key assets and an insufficient warning system to alert the general public.[65]

---

[61] Exec. Order 12333 § 1.14(b).

[62] *See* FBI Authorities for Critical Infrastructure Incident Response 1, fn. 1 (October 11, 1996).

[63] Examples of such statutes include: 18 U.S.C. § 1030(a)(5)(A) (computer fraud and related activities); 18 U.S.C. § 2511 (interception of communications); 18 U.S.C. §§ 793-94 (espionage); 18 U.S.C. § 641 (theft of government property); 18 U.S.C. § 2153 (sabotage).

[64] The National Security Threat List (1995) includes foreign power sponsored or coordinated intelligence activities directed at denial of communications services, unauthorized monitoring of communications systems, unauthorized disclosure of information on a communications system, etc.

[65] *See* FBI Authorities for Critical Infrastructure Incident Response at 6-7.

Department of Energy

Electrical Power Systems

The Department of Energy (DOE) has statutory authority to implement measures for protection of transmission and related facilities, the minimization of consequences of attack, and reconstitution following attack for DOE-owned facilities.[66] This authority is vested in five different Power Marketing Administrations (PWAs)-- Alaska Power Authority, Bonneville Power Administration Southeastern Power Administration and Western Area Power Administration, Southwestern Power Administration which developed the mechanisms for using their infrastructure assurance authority on an individual basis. In addition, the Defense Production Act of 1950[67] may be useful in the case of an energy emergency. It allows the President to require performance of contracts on a priority basis and to allocate materials and resources as "necessary or appropriate to promote the national defense."[68] 50 U.S.C. app. § 2071(c) authorizes the President to make the prioritization of contracts or allocation of resources in order to maximize domestic energy supplies. Features of the DPA, such as Voluntary Agreement Authority and the DPA loan and grant fund, could also be used for infrastructure assurance.

While DOE has no specific authority for infrastructure assurance over non-Federal facilities, there are two statutes which potentially could be used for such purposes. The Public Utilities Regulatory Policies Act (PURPA) gives DOE authority to gather information and make recommendations to industry regarding electric energy transmission system reliability.[69] Executive Order 10485 allows conditions to be attached, "as the public interest may require," to permits for electrical power transmission across the U.S. border.[70] Statutory vehicles available for the reconstitution of electrical power systems include the

---

[66] This authority is held by various Power Marketing Administrations (PWAs) and is contained in their respective enabling acts. *See* 16 U.S.C. § 832 *et seq*; 16 U.S.C. § 838; 16 U.S.C. § 837-837h; 16 U.S.C. § 839; 43 U.S.C. § 620 *et seq.*; 16 U.S.C. § 837g-1; 16 U.S.C. § 825s.

[67] 50 U.S.C. app. § 2061 *et seq.*

[68] 50 U.S.C. app. § 2071(a).

[69] 16 U.S.C. § 824-2(b).

[70] Exec. Order 10485 § 1(a)(3).

Defense Production Act of 1950 and the Federal Power Act.[71] The latter authorizes DOE to order temporary interconnections, generation and transmission of electric energy in emergency situations.

DOE also has authority with respect to nuclear energy facilities. The Atomic Energy Act of 1954 (AEA)[72] provides the general authority for maintenance and protection of nuclear facilities owned by the United States and under DOE control. The AEA allows the DOE to promulgate regulations and orders to: protect real and personal property, restrict data, guard against loss or diversion of special nuclear material, and govern design, location, and operations related to such facilities. Included among these powers is a limited arrest authority and authorization to allow certain employees to carry firearms. The AEA also authorizes the President to use the powers of any government agency as necessary to protect against unlawful dissemination of restricted data, and to safeguard DOE facilities, equipment, materials and other property. DOE nuclear facilities are also protected under the AEA from unauthorized photography, mapping or drawings. The President's powers in emergency situations under the Defense Production Act extend to nuclear facilities, both under DOE control and private, and may be used to reestablish vital capabilities. DOE has no further authority over non-federal nuclear facilities to require infrastructure assurance measures, but the Nuclear Regulatory Commission does have such authority.

Other government entities with a stake in electrical power systems protection include: The Federal Energy Regulatory Commission, the Tennessee Valley Authority, the Department of the Interior, and the U.S. Army Corps of Engineers.

Gas and Oil Storage and Transportation

With respect to DOE-owned facilities, the Energy Policy and Conservation Act[73] and the Department of Energy Organization Act[74] authorize the Secretary of Energy to establish, operate, and protect the physical security of the Strategic Petroleum Reserve (SPR) oil storage and transportation systems in Louisiana and Texas. The authority to protect the SPR includes the power to take action to deter trespass at those facilities.[75] The Secretary of Energy also has authority to

---

[71] 16 U.S.C. § 791a *et seq.*

[72] 42 U.S.C. § 2011 *et seq.*

[73] 42 U.S.C. §§ 6231-6241.

[74] 42 U.S.C. §§ 7270a-7270b.

[75] The statute conferring authority to make regulations prohibiting trespass, 50 U.S.C. § 7270b(a), and the regulations that actually prohibit trespass, 10 C.F.R. § 1048.5, define trespass slightly differently. The Secretary of Energy is given the broad power to issue

operate and protect the Naval Petroleum and Oil Shale Reserve's oil and gas production systems in California, Utah and Wyoming.[76] With respect to reestablishing vital capabilities related to gas and oil storage and transportation, the Defense Production Act of 1950 may be used in much the same way as with electrical power systems.

DOE has no specific authority to require infrastructure assurance measures of non-federal facilities. However, the Natural Gas Act, under which DOE has the power to grant permits for import and export of natural gas, may have potential uses for infrastructure assurance measures in that it allows the Federal Energy Regulatory Commission (FERC)[77] to grant the permits subject to conditions and modifications that it deems necessary or appropriate.[78] Significant statutory authority is in place for the reestablishing of vital capabilities of the gas and oil energy infrastructure. The Defense Production Act of 1950, as with electrical systems, gives the President authority to create priorities for contract performance and allocation of resources under appropriate conditions. The Act also facilitates cooperation between gas and oil service companies in the case of emergency by providing a limited antitrust defense for industry participants voluntarily helping the U.S. with emergency preparedness.[79] The same Act also provides the President with the authority to train and employ persons from the private sector to facilitate planning for and responding to emergencies.[80] In the case of an existing or imminent "severe natural gas shortage, endangering the supply of natural gas," the President is authorized to approve purchases of natural gas and to allocate supplies of natural gas in interstate commerce.[81] Under identical circumstances, the President is also authorized to prohibit the burning of natural gas by electrical power plants or major fuel-burning installations.[82] The Powerplant and Industrial Fuel Use Act[83] allows the President control over the allocation and burning of coal during "a severe energy supply interruption."

---

regulations relating to "the entry upon or carrying, transporting, or otherwise introducing or causing to be introduced any dangerous weapon, explosive, or other dangerous instrument or material likely to produce substantial injury or damage to persons or property." The actual regulation prohibiting trespass addresses "willful unauthorized entry" and "willful unauthorized introduction of weapons or dangerous materials."

[76] 41 U.S.C. § 251 *et seq*.

[77] *See infra* p. 53-56 discussing FERC's authorities.

[78] 15 U.S.C. § 717b(a).

[79] 50 U.S.C. app. § 2158.

[80] 50 U.S.C. app. § 2160.

[81] 15 U.S.C. §§ 3362-3363.

[82] 15 U.S.C. § 717z & 16 U.S.C. § 2601 *et seq*.

[83] 42 U.S.C. § 8301 *et seq*.

Department of Transportation

The Office of Intelligence and Security (OIS) operates under the Secretary of Transportation and is charged with assessing intelligence information relating to long-term transportation security, developing policies and strategies for dealing with threats to transportation security, coordinating countermeasures with appropriate Federal departments, and serving as the primary liaison with the intelligence and law enforcement community. The primary law enforcement agency under the Department of Transportation is the Coast Guard, which has jurisdiction over enforcement of criminal laws over the high seas and waters of the United States.

Telecommunications

The Coast Guard and the Federal Highway Administration have internal and/or department-wide computer security measures in place. The Saint Lawrence Seaway Development Corporation (SLSDC) has established an Operations and Contingency Plan concerning security and disaster/backup recovery. The FAA also has an internal security program for its computer systems as required the Computer Security Act of 1987.[84]

Gas and Oil Storage and Transportation

The Secretary of Transportation has the statutory authority to prescribe minimum safety standards for transportation of gas and hazardous liquids and for operation of pipeline facilities generally.[85] The Research and Special Programs Administration (RSPA) is charged with regulating pipelines and has implemented numerous regulations to that end. RSPA has in place requirements for design and installation of pipe components, operation and maintenance procedures addressing continuing surveillance and emergency response, line patrolling, training, firefighting equipment and security, and damage prevention programs.[86] Similar statutory authority and regulatory requirements exist for

[84] Pub. Law No. 100-235.

[85] 49 U.S.C. § 60102.

[86] *See, e.g.*, 49 C.F.R. Part 192, subpart D; 49 C.F.R. §§ 195.116, 195.254, & 195.258 (design and installation of components); 49 C.F.R. § 192.613; 49 C.F.R. § 192.615; 49 C.F.R. § 195.402 (c)-(d) (surveillance and emergency response); 49 C.F.R. §§ 192.705 & 192.721 (line patrol); 49 C.F.R. § 195.403 (training); 49 C.F.R. §§ 195.430 & 195.436 (firefighting and security); 49 C.F.R. §§ 192.614 & 195.442 (damage prevention).

liquefied natural gas pipeline facilities as well.[87] The Office of Pipeline Safety (OPS) is charged with enforcing pipeline safety measures.[88] Among the enforcement measures available to OPS are civil penalties, compliance orders, and hazardous facility orders. In addition, 49 U.S.C. § 60123 makes it a crime to knowingly and willfully damage or destroy or attempt to damage or destroy, an interstate transmission or hazardous liquid pipeline facility. OPS coordinates its transportation safety responsibilities with the Department of Energy. Currently, OPS is working to develop a contingency plan to address security and terrorism issues within the DOT, as well as participating in interagency security information meetings.

The Coast Guard also has authority over the transportation of oil and gas (as well as other hazardous liquids) to the extent they are transported over the high seas.[89] Safety regulations include additional requirements for vessels that transport oil or hazardous material in bulk as cargo or cargo residue, including double hull requirements. The Coast Guard has also implemented regulations and requirements regarding the transportation of oil as part of an environmental initiative and oil pollution response.

SLSDC also has an emergency response plan in place for events such as oil spills that affect the St. Lawrence Seaway.

Transportation

The Coast Guard's role in the protection of the transportation infrastructure relates primarily to boating. The Coast Guard Commandant has authority over boating safety and may set and require compliance with manufacturing requirements and standards. Both civil penalties and criminal sanctions are available as enforcement mechanisms. The Coast Guard may engage in surveillance and boarding activities to monitor compliance.

The Federal Highway Administration (FHWA) has a three-part role in transportation infrastructure assurance. FHWA provides federal financial assistance to States for construction and improvement of highways; it administers the highway bridge inspection and rehabilitation program; and the emergency relief program to assist in the repair or reconstruction of Federal-aid highways and certain federal roads. As part of the Emergency Relief Program, FHWA may provide funding for emergency relief after serious damage is caused

[87] *See* 49 U.S.C. § 60103; 49 C.F.R. Part 193.

[88] 49 C.F.R. Part 190.

[89] *See, e.g.*, 33 U.S.C. § 1225, 1231; 46 U.SC. § 3306; 46 U.S.C. § 3703; 49 U.S.C. app. §§ 1801-19.

to highways, roads, and trails that has occurred as the result of a natural disaster or catastrophic failure from any external cause.[90]

The National Highway Traffic Safety Administration (NHTSA) is charged with setting and enforcing safety standards for motor vehicles and making grants to states to help organize highway safety programs in order to reduce deaths, injuries and economic losses resulting from motor vehicle crashes.

While the Federal Transit Administration (FTA) does not currently have any measures in place specifically addressing infrastructure assurance, the statutory grants of authority to the Secretary of Transportation relating to the FTA mission[91] are broad enough to encompass infrastructure assurance measures. 49 U.S.C. § 5321 provides the general authority for the Secretary of Transportation to make grants for crime prevention and security. Grants are also authorized for mass transportation security projects such as increased lighting at transit stations, camera surveillance, and emergency phones.[92] The Violent Crime Control and Law Enforcement Act of 1994 makes available up to ten million dollars in grants for these same purposes. [93]

SLSDC has an emergency response plan in place to deal with damage to tunnels under the canals or vessel accidents in the Seaway.

The Maritime Administration (MARAD) conducts a preparedness program for industrial mobilization of all materials related to shipping via voluntary agreements with vessel and equipment owners. During national security emergencies, MARAD is charged under the Defense Production Act with controlling ports. In addition, MARAD maintains the National Defense Reserve Fleet which, when called to duty, operates under the Navy and is an essential part of the national defense waterborne supply network. MARAD is also responsible for development and maintenance of the Merchant Marine at levels sufficient to carry the nation's waterborne commerce as well as foreign commerce, and to act as a military auxiliary during a national emergency. MARAD chairs the Secretary of Transportation's *Ad Hoc* Working Group on Maritime Security Awareness and produces the Maritime Security Report on a quarterly basis. Together with Secretary of Defense, MARAD works to promote and develop ports and transportation facilities in connection with water commerce and to alleviate port congestion.

---

[90] 23 U.S.C. § 125; 23 C.F.R. Part 668.

[91] The FTA provides financial and planning assistance for the design, building, and operation of rail, bus and paratransit systems.

[92] *See* 49 U.S.C. § 5307(d)(1)(J)(i).

[93] 49 U.S.C. § 13931.

The Federal Railroad Administration (FRA) has the responsibility for the establishment of safety standards for railroads as well as investigatory authority over rail accidents. The FRA has a two-part role in transportation infrastructure assurance. First, during national emergencies the FRA is responsible for the acquisition of transportation requirements. In doing so, the FRA may draw on the President's prioritization authority under the Defense Production Act. In addition, the FRA has been active in a counter-terrorism effort designed at protecting the rail system from attack. Criminal statutes are already in place which prohibit targeting of organizations engaged in interstate commerce or property of the United States. Through the Railroad Police Rule, implemented under the Crime Control Act of 1990, railroad police officers are authorized to enforce the laws of any state where their employer owns property so long as their enforcement action is for the limited purpose of protecting railroad property, personnel, passengers, or cargo. The FRA has also drafted an anti-terrorism bill to afford the rail system greater protection from terrorist attack.

The Federal Aviation Agency (FAA) is authorized to adopt and enforce reasonable rules, regulations, orders and minimum safety standards for civil aviation. The FAA has also been granted authority over regulation and enforcement of screening procedures of air passengers and cargo for weapons, overall federal responsibility for air piracy, airport security including foreign airports, transportation of hazardous materials, and drug trafficking.

Water Supply Systems

Under the Federal Water Pollution Control Act and the Coast Guard's federal law enforcement activities, DOT may have some responsibility for assuring the safety of the water supply.

Federal Emergency Management Agency (FEMA)

FEMA, unlike many of the other agencies discussed, is not a regulatory agency and relies primarily on grants to elicit compliance with its programs. FEMA's programs are not limited to disaster response, and indeed encompass preparation, mitigation and coordination activities. FEMA's preparedness and mitigation authority and activities may be more beneficial to infrastructure assurance objectives than its disaster relief function.

FEMA is authorized to study and develop emergency preparedness measures to protect life and property, including research and study of the "best methods of

treating the effects of hazards," "developing shelter designs," and "developing equipment or facilities and effecting the standardization thereof to meet emergency preparedness requirements."[94] This grant of power is particularly broad when the statutory definitions of "hazard" and "emergency preparedness" are considered. A "hazard" is defined as an emergency or disaster resulting from either a natural disaster or an accidental or human-caused event."[95] "Emergency Preparedness," defined in the same section, includes all activities "to prepare for or minimize the effects of a hazard upon the civilian population, to deal with the immediate emergency conditions which would be created by the hazard, and to effectuate emergency repairs to, or the emergency restoration of, vital utilities and facilities destroyed or damaged by the hazard."[96] Specific measures mentioned in the statute include: development of organizations, operational plans and training and recruitment of personnel; control of traffic; fire, rescue and medical services; monitoring for danger of special weapons; unexploded bomb reconnaissance, and essential repair or restoration of vital facilities.[97] In addition, the powers granted to the Director of FEMA for emergency preparedness measures include coordination among federal agencies, promoting development of interstate compacts for disaster response and development of emergency communications and warning systems.[98]

When an area is declared a disaster by the President, FEMA is authorized by the Stafford Act to make grants to the states of up to 75 percent of the cost of measures designed to substantially reduce the risk of future loss in that area. [99] Additionally, FEMA may take appropriate action to mitigate future hazards when it makes emergency repairs to, or rebuilds, buildings damaged by disaster.[100] FEMA has statutory authority for mitigation of flood[101]and earthquake hazards,[102] and for dam safety.[103]

FEMA is authorized by the President to coordinate, review, and evaluate plans for emergency preparedness by executive agencies.[104] This charge includes such

---

[94] 42 U.S.C. § 5196(e).

[95] 42 U.S.C. 5195a(a)(1).

[96] *Id.* § 5195a(a)(3).

[97] *Id.*

[98] *See* 42 U.S.C. § 5196(c), (g) & (h).

[99] 42 U.S.C. § 5170.

[100] *Id.* § 5171(c).

[101] 42 U.S.C. § 4001 *et seq.*

[102] 42 U.S.C. § 7701 *et seq.*

[103] 33 U.S.C. § 467h.

[104] *See* Exec. Order 12148 (1979).

facets of emergency preparedness as warning systems, state emergency preparedness plans, and planning to reduce the consequences of terrorist incidents. With respect to national security preparedness, FEMA is to work with the National Security Council and coordinate activities with federal agencies and state and local governments.[105]

FEMA is also charged with responding to disasters by rendering assistance to state governments and other federal agencies in the following circumstances. FEMA may assist a federal agency during a disaster by making repairs to Federal facilities.[106] In addition, FEMA may render disaster assistance when the President determines that there is an emergency in an area where the United States exercises exclusive or preeminent responsibility.[107]

Department of Commerce

The Department of Commerce has limited, but important, legal authority for protecting critical national infrastructures. Its role in infrastructure assurance, in many instances, is related to the export of products. The Department plays a crucial role in continuity of government services through internal and external regulations regarding information and technology security.

Telecommunications

The National Telecommunications and Information Administration (NTIA) is authorized to assign radio frequencies to federally-owned systems under 47 U.S.C. § 902(b)(2)(A). This power is administered through the Office of Spectrum Management. All government frequencies are collected in a database called the Government Master File (GMF). This database will be duplicated and stored in an additional location in order to create redundancy. NTIA does not allow remote access to its mainframe in order to protect this database.

Executive Order 12472 governs management and allocation of telecommunications resources during both non-wartime and wartime crises and emergencies. The Joint Telecommunications Resources Board (JTRB), as created by the Office of Science and Technology Policy (OSTP), within the Executive Office of the President, is given the primary authority for managing

---

[105] *See* Exec. Order 12656 (1988).

[106] 42 U.S.C. § 5171.

[107] 42 U.S.C. § 5191(b).

telecommunications resources during non-wartime emergencies. NTIA is a member of the JTRB. The telecommunications function for the National System for Emergency Coordination (NSEC) is performed by JTRB.

During wartime, NTIA may work with the National Security Council (NSC) and OSTP in advising the President with regard to radio spectrum priorities.[108] The NTIA Emergency Readiness Plan for Use of the Radio Spectrum is currently under review. The plan addresses actions that may be taken to prepare for, respond to, or recover from all emergency situations. Part III of the plan will contain telecommunications service priorities for Radiocommunications for use in a Presidentially-declared emergency under the Communications Act of 1934, as amended.[109]

Under the Communications Satellite Act of 1962,[110] NTIA may make recommendations to the President to ensure the availability and appropriate utilization of the communications satellite system for general government purposes. No mechanisms are currently in place for making or implementing recommendations.

The Bureau of Export Administration (BXA), through the Defense Priorities and Allocations System (DPAS), administers the Defense Production Act (DPA), as amended by the Stafford Act. Under the authority of these statutes, DPAS may set priorities in contracts and orders for industrial resources to meet national defense requirements. "National defense," as defined by the Stafford Act, includes civil "emergency preparedness." Thus, priority for government contracts and orders may be used to prepare for, respond to, or recover from both natural and human-made disasters.

Electrical Power Systems

The BXA may use its power under the DPA for creating priority for government contracts and orders for industrial resources for national defense requirements to reconstitute critical infrastructures after attack. The Secretary of Commerce has additional authority under the International Emergency Economic Powers Act[111] to impose export controls on dual use items.[112] A dual use item is one that has

---

[108] Exec. Order 12472 § 2(c).

[109] 47 U.S.C. § 606.

[110] 47 U.S.C. § 721(a)(6).

[111] 50 U.S.C. § 1701 *et seq.*

[112] The structure of these export controls is based on a prior law, since lapsed, the Export Administration Act of 1979 (EAA), 50 U.S.C. app. § 2401 *et seq.* The International

both potential commercial and military applications. The export controls are administered by the BXA and may be used to protect national security, foreign policy, and domestic shortages. Current regulations in place include export controls for most types of weaponry, crude oil, and exports to countries supporting terrorist organizations.[113]

Gas and Oil Storage and Transportation

See discussion of priorities in contracts under Electrical Power Systems *supra* p.26.

Transportation

See discussion of priorities in contracts under Electrical Power Systems *supra* p. 26.

Water Supply Systems

See discussion of priorities in contracts under Electrical Power Systems *supra* p. 26.

Continuity of Government Operations

The Department of Commerce has measures in place for the continuity of its specific government services. The Bureau of Census and the National Technical Information Service have mechanisms in place for the continuity of their own functions and for the protection of the information they store. Census has three basic mechanisms for protecting information and ensuring continued operation. 13 U.S.C. § 9 ensures the confidentiality of data submitted to Census from public disclosure. In addition, the Bureau has a plan for the protection of vital records. These records include plans and procedures for accomplishment of mission, standby emergency documents and delegations of authority, lines of succession, program documentation and budget estimates, vital ADP records, programs, software, specifications, customer directories and mailing lists, survey designs, demographic and economic data, Current Population Survey, Census of Manufacturing, and geographic and cartographic reference files. Census also has a disaster recovery/contingency plan. It is designed to ensure continued normal operation during emergencies. The plan includes a number of elements such as priorities, emergency chain of command, computer system information, a plan for

Emergency Economic Powers Act (IEEPA), 50 U.S.C. § 1701 *et seq*., has replaced the EAA as the relevant legal authority, but the implementing regulations have remained unchanged.

[113] *See* 15 C.F.R. Part 730.

dealing with physical disruptions including electric power, descriptions of alarm systems, and the functions of the various post-disaster teams that are needed for recovery.

The National Institute of Standards and Technology (NIST) plays a key role in setting government-wide standards and guidelines to assist Federal agencies in protecting their information technology resources under authority granted by the Information Technology Management Reform Act of 1996,[114] and the Computer Security Act of 1987.[115] The latter charges NIST with creating computer security standards for the federal government. The Office of Management and Budget Circular No. A-130 mandates that government agencies follow the NIST standards. NIST is given additional authority to conduct research and development, to coordinate efforts with other agencies, and to assist the private sector as necessary to effectuate the goals of the Computer Security Act. Most recently, NIST has entered into a partnership arrangement with the National Security Agency to establish testing methods and objective measures for computer security products and to accredit private labs to certify such products.[116]

The NTIA also has a Continuity of Operations Plan which is currently in draft form. It was created pursuant to Department Administrative Order 210-10, February 23, 1996. Additional requirements for NTIA's continuity plan come from Federal Preparedness Circular 60, which requires that NTIA be able to function out of three locations in case of emergencies.

Department of the Treasury

The Department of the Treasury's legal authority relevant to infrastructure assurance is concentrated in the area of banking and finance. The Treasury's authority and responsibility for the federal government's financial transactions, both payments and collections, also impacts the continuity of government operations.

[114] Pub. Law No. 104-106.

[115] Pub. Law No. 100-235.

[116] *See also* discussion of NSA authorities and the National Information Assurance Partnership *infra* p. 31.

Banking and Finance

The Department of the Treasury can influence or control the efficiency and security of the financial marketplace through different mechanisms. The President's Working Group on Financial Markets (FMWG), created by Executive Order 12631, is chaired by the Secretary of the Treasury. The FMWG facilitates information exchange among the government agencies with responsibility for the financial markets and regulation of securities and commodity firms and banks. FMWG has already begun to focus on disruptions of financial markets or major market participants from both physical and cyber causes. The Group is in a position both to mitigate the effects of disruption and to work to limit systemic risk and lower the damage that accompanies disruption. While FMWG has no statutory authority of its own, it is nonetheless in the position to influence policy with regard to banking and finance infrastructure assurance.[117]

Through its statutory authority to regulate government securities brokers and dealers, the Treasury may be able to enact measures for greater infrastructure assurance. Currently, Treasury has recordkeeping and reporting requirements in place, in addition to rules regarding financial responsibility and related practices. The Treasury submission suggests that the recordkeeping and reporting requirements, and its statutory authority, may be broad enough to impose standards for protection of information and telecommunications systems.

Continuity of Government Operations

Treasury has two functions that relate to the continuity of government operations in the face of infrastructure disruption. First, the Department of Treasury is charged with the issuance of Treasury debt which is administered through the Bureau of Public Debt. The Treasury's authority in this area is derived from a variety of statutory sources including 31 U.S.C. § 3121 *et seq*. and 12 U.S.C. § 391. Second, the Financial Management Service (FMS), located within Treasury, is responsible for making payments for government programs and providing the system for collecting government receipts, including federal taxes. Both of these functions rely extensively on the Federal Reserve Banks. The banks used by the Financial Management Service are required by agreement to comply with the Computer Security Act of 1987 and related standards and guidelines. FMS conducts audits to ensure compliance with these requirements.

---

[117] The Treasury submission notes that FMWG can wield influence both by raising visibility of an issue and through the rule making roles of its member agencies. The members of FMWG include: the Board of Governors of the Federal Reserve System, the Securities and Exchange Commission, and the Commodity Futures Trading Commission. Other agencies that participate in FMWG meetings include: the Comptroller of the Currency, the Federal Deposit Insurance Corporation, Federal Reserve Bank of New York, the National Economic Council, and the Council of Economic Advisors.

Department of Justice

The Department of Justice (DOJ) plays a unique role in infrastructure assurance. Unlike many of the other agencies and departments surveyed which have roles relating to particular infrastructures, the Department of Justice and the Attorney General are expected to play a primary role in responding to terrorist incidents under authorities such as Presidential Decision Directive 39 (PDD-39) and the Terrorism Incident Annex to the Federal Response Plan. For terrorist matters that occur within the United States and have no significant foreign involvement, the Department of Justice, through the FBI, handles coordination of federal agency efforts.

Perhaps the most visible role for the Department of Justice with respect to infrastructure assurance is in enforcing federal laws through the investigatory authorities of the FBI and prosecutorial resources of DOJ and the United States Attorneys' Offices. The Department's 94 United States Attorneys' offices are acquiring their own expertise in these important areas. Within the past several years, These offices have appointed, and the Department has specially trained, attorneys to handle crisis response issues (Attorney Critical Response Group Attorneys--ACIRGs) and computer and telecommunications-related crimes (Computer and Telecommunications Coordinators--CTCs).

Other Department components have responsibilities with important ties to infrastructure assurance policies. Within DOJ's Criminal Division, the Computer Crime and Intellectual Property Section and the Terrorism and Violent Crime Section play a pivotal role not only in prosecuting offenses against the critical infrastructures, but in developing policy initiatives and legislative proposals to improve laws and enforcement in these areas.

Increasingly, the Department of Justice, in coordination with the Department of State, is involved in international agreements to facilitate U.S. enforcement efforts concerning cyber-crime and physical threats to critical infrastructures. Bilateral and multilateral agreements address issues such as extradition, mutual legal assistance, and evidence sharing. Increasingly, such agreements address substantive and investigative issues relating to computer crime. The Department of Justice also administers a rewards program designed to encourage cooperation with counterterrorism enforcement efforts.

The Office of Intelligence Policy and Review works closely with law enforcement and the intelligence community to facilitate sharing of information between the communities, and also assists in the investigation of terrorism-related cases under the Foreign Intelligence Surveillance Act. The elements of the Office of

Justice Programs-- the National Institute of Justice, the Bureau of Justice Statistics, and others may be involved in future studies of infrastructure assurance issues and efforts to develop a better understanding of the scope of the problem facing the nation and the proper role of law enforcement. The Office of Justice Programs also provides funds to state and local law enforcement agencies to bolster preparedness in the event of a terrorist attack.

With respect to information sharing, the Civil Division of DOJ should play a role in predicting the liability climate surrounding effective implementation and operation of an information sharing and threat warning capability. The Antitrust Division can serve as a focal point for issues relating to private-sector to private-sector sharing of threat and vulnerability information.

National Security Agency

The National Security Agency (NSA) identified its role in infrastructure assurance as deriving from three legal sources-- Executive Order 12333, "United States Intelligence Activities," National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems," and the Computer Security Act of 1987. These three documents give NSA substantial authority for the communications security of the United States.

Executive Order 12333 designated the Secretary of Defense as the executive agent for the United States for communications security activities, except as limited by the National Security Council.[118] NSA is authorized to carry out the Secretary of Defense's responsibilities for communications security under the executive order.

Consistent with Executive Order 12333, National Security Directive 42 assigns the Secretary of Defense responsibility for the government's National Security Telecommunications and Information Systems Security. As part of this Directive, the Director, NSA, is named the National Manager for this function. Among the duties this role entails are: (1) examining national security systems and evaluating their vulnerability to foreign interception and exploitation; (2) acting as the U.S. government focal point for telecommunications and information systems security for national security systems; (3) assessing the overall security posture of and disseminating information on threats to and vulnerabilities of national security systems; (4) reviewing and approving all standards, techniques, systems, and equipment related to the security of national

[118] Exec. Order 12333 § 1.11(e) (1981).

security systems; and (5) coordinating with the National Institute of Standards and Technology (NIST) in accordance with the provisions of the Computer Security Act of 1987.

Executive Order 12333 and NSD 42 limit NSA's role to national security systems, which NSA recognizes as a potential limit on its role in assuring the security of the nation's critical information infrastructure. However, NSA has assumed a role in assisting NIST with its responsibilities under the Computer Security Act of 1987. NSA and NIST have agreed on a division of labor, memorialized in "Memorandum of Understanding Between the Director of the National Institute of Standards and Technology and the Director of the National Security Agency Concerning the Implementation of the Public Law 100-235," March 24, 1989. Under this MOU, NSA provides technical guidelines to NIST for sensitive information in federal computer systems, conducts assessments of hostile intelligence and foreign exploitation threats to information systems upon request of federal agencies, provides technical guidance and endorses products to secure information systems, and supports NIST in its role in assisting the private sector with information security issues.

The NSA-NIST partnership has been formalized recently as the National Information Assurance Partnership. This Partnership is designed to combine the expertise of the two entities to assist both government and the private sector in improving the quality of their computer security. To accomplish this goal, the Partnership is working to establish testing methods and objective measures for computer security products and to accredit private sector labs to conduct such testing and, ultimately, certify products.

United States Customs Service

The primary missions of the Customs Service of the Department of Treasury are to ensure that all merchandise coming into the United States is lawfully imported and to protect the borders of the United States. The Customs Service enforces laws relating to the importation and exportation of merchandise including laws requiring: the collection of duties and tax on imported goods; monitoring the clearing of arriving and departing vessels, vehicles and aircraft; detecting and preventing smuggling operations and fraudulent importations, and seizing merchandise and conveyances involved in such activities; excluding prohibited merchandise (*e.g.*, unlicensed munitions) from entry; controlling imports subject to quotas (*e.g.*, textiles), other international agreements, and

intellectual property protection; and enforcing export laws pertaining to critical technology, munitions and embargoes.[119]

In addition to the authority to enforce customs laws, the Customs Service is authorized to enforce all federal laws at the borders of the United States. The Customs Service's unique position at the nation's borders allows it to exercise broad search and seizure and arrest functions. Customs officers may search persons, conveyances, baggage, cargo, and merchandise entering the United States without a search warrant and without suspicion of criminality.[120] Customs officers may stop vehicles and board vessels and aircraft without warrants to perform inquiries and searches.[121] Customs officers carry firearms and are authorized to make warrantless arrests for any federal violations occurring in their presence.[122] In addition, a customs officer may conduct undercover investigations and seek and obtain search warrants, court orders authorizing interception of communications, and administrative summonses. Any merchandise or conveyance involved in a Customs violation is generally subject to civil forfeiture and may be seized by Customs officers without a warrant.[123] These authorities also apply to outbound goods, conveyances and people.[124]

The Customs Service also has emergency powers. Customs may take the following actions to protect against attacks and to minimize the damage from such attacks: close ports; remove a customhouse to a secure location; seize and forfeit vessels seeking to enter a closed port; and refuse to clear for export vehicles with suspect cargoes.[125] The President may authorize the Secretary of Treasury, who has delegated the power to the Commissioner of Customs, to extend the time provided under the Tariff Act of 1930 for the performance of any act and also to allow for the importation free of duty of certain supplies used in emergency relief work. Under the International Emergency Economic Powers Act,[126] the Secretary of Treasury, or his designee, may restrict entry, prevent movement, and take other authorized action during time of national emergency. In addition, during a Presidentially declared emergency, restrictions on imports and exports may be imposed when there is "any unusual and extraordinary threat, which has its source in whole or in substantial part outside the U.S. to

---

[119] *See* Title 19, United States Code.

[120] *See* 19 U.S.C. §§ 482, 1499, 1581 & 1582.

[121] *See* 19 U.S.C. §§ 482, 1467 & 1581; 19 C.F.R. Part 122.

[122] 19 U.S.C. § 1589a.

[123] *See* 19 U.S.C. §§ 482, 1581 & 1595a.

[124] *See, e.g.*, 31 U.S.C. § 5317(b); 22 U.S.C. § 401; United States v. Ajlouny, 629 F.2d 830 (2d Cir. 1980).

[125] 50 U.S.C. §§ 219-226.

[126] 50 U.S.C. § 1701 *et seq*.

the national security, foreign policy, or economy of the United States." During emergencies such as war, insurrection, invasion, or disturbance to international relations, the Secretary of Treasury may allow the Customs Service to take possession and control of vessels away from officers and crews.[127] The Secretary may also impose severe controls during times of insurrection-- a power which has not been used since the Civil War.[128]

Bureau of Alcohol, Tobacco and Firearms

The Bureau of Alcohol, Tobacco and Firearms (ATF) operates under the umbrella of the Department of Treasury. The ATF's primary authorities relevant to infrastructure assurance pertain to emergency services and continuity of government operations.

ATF's mission, as a law enforcement agency, includes reducing violence, collecting revenue, and protecting consumers. Its jurisdiction extends to alcohol, tobacco, firearms and explosive matters. The most important aspects of ATF's role in infrastructure assurance pertain to its enforcement authority for provisions of title 18, United States Code, related to importation, manufacture, distribution and possession of firearms and ammunition,[129] explosives,[130] and arms and implements of war.[131]

United States Secret Service

The Secret Service is a law enforcement agency under the Department of Treasury and is charged with the protection of the President and Vice President, their families, foreign heads of state and the White House. The Secret Service is

[127] 50 U.S.C. § 191. During World War I, Customs officials physically seized German vessels in U.S. ports under this law.

[128] 50 U.S.C. §§ 205-226.

[129] 18 U.S.C. Chapter 44.

[130] 18 U.S.C. Chapter 40.

[131] 22 U.S.C. § 2778.

also charged with the detection and arrest of individuals who violate criminal laws relating to coins, obligations, and other securities of the United States and foreign governments, electronic fund transfers, credit or debit card fraud, false identification documents, and fraud committed against certain financial institutions, such as the Federal Deposit Insurance Corporation.

Banking and Finance

The Secret Service has exclusive jurisdiction for investigations involving the counterfeiting of coins, obligations and other securities of the United States and foreign governments.[132] Among the obligations and securities investigated by the Secret Service are U.S. coins and currency, Treasury checks, Department of Agriculture food stamps coupons, and postage stamps. The counterfeiting of these obligations and securities is criminalized by the provisions of Chapter 25 of Title 18, United States Code. In order to reduce opportunities for counterfeiting, the Secret Service works extensively with other federal agencies, including the Bureau of Engraving and the Federal Reserve Bank, and banking institutions to raise awareness, provide counterfeit detection seminars, improve security of currency design, and maintain the effectiveness of currency sorting equipment.

Under the authority granted by 18 U.S.C. § 3056 and Public Law 101-509, the Secret Service has jurisdiction over the investigation of other crimes within the banking and finance industry, including financial institution fraud, access device fraud, and computer crime. The Secret Service uses investigations into financial crimes as an important source of data regarding systemic vulnerabilities. This information is shared with industry in an effort to raise security and awareness.

Telecommunications

The Secret Service's investigative authority under 18 U.S.C. § 1029, Access Device Fraud, and 18 U.S.C. § 1030, Computer Fraud, allows it to investigate criminal activity affecting components of the Telecommunications Infrastructure.

Continuity of Government Operations

The Secret Service is responsible for the safety of the President, Vice President, their immediate families, major Presidential and Vice Presidential candidates, former Presidents, and visiting foreign heads of state.[133] The Secret Service is also charged with protecting the White House Complex and the Vice President's residence. As part of its charge to protect the President, the Secret Service

[132] 18 U.S.C. § 3056.

[133] *Id.*; 3 U.S.C. § 202.

investigates threats against the President, successors to the Presidency, former presidents and certain other persons protected by the Secret Service.[134]

Department of Education

The Department of Education may provide funding for the education of school children on computer ethics and use of technology. The funding authorities that may be used for these purposes include the Fund for the Improvement of Education,[135] the Partnerships in Character Education Pilot Project,[136] and the Technology for Education Act of 1994.[137] In addition, state educational agencies may seek funding to educate school children in computer ethics through Goals 2000: Educate America Act.[138]

In addition to the funding available for educating school children on computer ethics and technology, the Department of Education also plays a role in continuity of government operations. The Department has issued internal policies relating to cyber disruptions.

General Services Administration

The General Services Administration (GSA) plays a critical role in the continuity of government operations in maintaining federal buildings and government telecommunications. These activities, as well as others carried out by GSA, also have an impact on the assurance of other critical infrastructures.

---

[134] 18 U.S.C. § 871 & 879.

[135] *See* 20 U.S.C. § 8001 (authority to carry out programs directly or to use grants or contracts with state and local educational agencies, institutions of higher learning, and other public and private agencies and organizations on programs authorized under 20 U.S.C. § 8003).

[136] *See* 20 U.S.C. § 8003 (authority to provide grants to state educational agencies on character education programs incorporating civil virtue).

[137] *See* 20 U.S.C. § 6801 *et seq*. (designed to promote use of technology in education directly or through contracts or grants with state or local educational agencies, institutions of higher education, or other public or private organizations).

[138] 20 U.S.C. § 5801 *et seq*.

Continuity of Government Operations

GSA, under authority granted by the Federal Property and Administrative Services Act of 1949 and the Public Buildings Act of 1959, acquires and manages public buildings and space.[139] Under GSA's current appropriations act,[140] GSA is required to use its funding for constructing, altering, managing and protecting public buildings to meet minimum security standards provided by current law. GSA has indicated that its public buildings-related responsibilities can be leveraged to create structures better able to avoid or survive infrastructure attack.

In addition to the management of federal buildings, GSA is also responsible for procuring and supplying personal property and nonpersonal services for the federal government. Under 41 U.S.C. §§ 405 & 421, GSA, DOD and NASA have joint responsibility for issuing the Federal Acquisition Regulation (FAR), under the overall direction of the Office of Federal Procurement Policy. The FAR[141] is the basic regulation for acquiring services and supplies.[142] GSA has indicated that government purchase of supplies can be used to encourage private industry to develop products and services better able to achieve the infrastructure goals of the PCCIP.

Under Executive Order 12656 of November 1988, GSA is given lead responsibility for developing National Security/Emergency Preparedness (NS/EP) plans and procedures related to federal buildings (including shelter management programs), and supplies and public utility services needed by federal agencies during national emergencies.

Continuity of Government Operations and Telecommunications

GSA has the current responsibility for managing the FTS 2000 program and coordinating the follow-on program.[143] The current program provides government-wide telecommunications services for federal users, principally under two long-distance service contracts expiring in 1998. In addition to

---

[139] *See* 40 U.S.C. § 471 *et seq*. & 40 U.S.C. §§ 601-619, 490. Implementing regulations are found in the Federal Property Management Regulations (FPMR) system, 41 C.F.R. Chapter 101.

[140] Pub. Law No. 104-208.

[141] 48 C.F.R. Chapter 1.

[142] GSA's Federal Supply Schedules are located at FAR Subpart 8.4 and Part 38.

[143] *See* Pub. Law No. 104-106, section 5124(b) (The Information Technology Management Reform Act, or the Clinger-Cohen Act).

management under normal circumstances, GSA is also directed to ensure that federally owned or managed domestic communications facilities and services meet the National Security and Emergency Preparedness requirements of Federal civilian departments, agencies and entities.[144] GSA's current appropriations law makes funding available for this purpose, specifically for "the interagency funding of [NS/EP] telecommunications initiatives which benefit multiple Federal departments, agencies, or entities, as provided by [Executive Order 12472]."[145]

In the implementation of FTS2000 and the planned follow-on contracts NS/EP is a priority. In order to ensure that the network is maintained in a state of readiness for national emergencies, contractors must meet requirements related to grade of service, service reliability, interoperability, and restoration capabilities (including government-controlled priorities). Certain critical users may also use National Communications System (NCS) Government Emergency Telecommunications Service (GETS).[146] The implementation of the FTS program has been designed to meet the goals of the National Information Infrastructure; to support implementation of IT recommendations of the National Performance Review (NPR); and to provide the bulk of the telecommunications services for the emerging Government Services Information Infrastructure (GSII).

Telecommunications

By President's Memorandum, "Facilitating Access to Federal Property for the Siting of Mobile Services Antennas," August 10, 1995, the President directed GSA, and other federal agencies, to assist in "infrastructure buildout" by developing "procedures necessary to facilitate the appropriate access to Federal property for the siting of mobile services antenna." This Memorandum directs the implementation of the authority to "outlease" federal rooftops under the Public Buildings Cooperative Act of 1976[147] to provide federal property, rights-of-way, and easements for siting of new telecommunications services dependent on Federal spectrum rights for transmission contained in the Telecommunications Act of 1996.[148] A Federal Property Management Regulation Bulletin was scheduled for issue in May of 1997.

---

[144] *See* Exec. Order 12472, "Assignment of National Security and Emergency Preparedness Telecommunications Functions."

[145] Pub. Law No. 104-208, Title VI at § 619.

[146] *See* Exec. Order 12472 § 1.

[147] 40 U.S.C. § 490(a)(17)-(19).

[148] Pub. Law No. 104-104 § 704(c).

Transportation and Gas and Oil

Pursuant to the Federal Motor Vehicle Fleet, GSA acquires and manages alternative fueled vehicles.[149] GSA has indicated that this program plays a modest role in infrastructure assurance by reducing the nation's dependence on oil while expanding the alternative fuel infrastructure. But, it is a valuable example of how the government's purchasing power can be used to diversify critical components of the economy, thereby lessening the harm that would befall one component's incapacitation.

Federal Communications Commission

The Federal Communications Commission (FCC) is an independent federal agency that reports directly to Congress. The FCC has general jurisdiction over interstate and international communications by radio, television, wire, satellite and cable.[150] The extent of the FCC's regulatory jurisdiction within each of these areas does vary. The passage of the Telecommunications Act of 1996 and the adoption of the February 1997 World Trade Organization Treaty on Basic Telecommunications may both effect infrastructure assurance objectives, although the results are, at this time, unknown.

Telecommunications Carriers

FCC jurisdiction over common carriers is set out in Title II of the Communications Act of 1934.[151] This jurisdiction is for the purpose of regulating the provision of interstate and foreign (international) telecommunications service by carriers. "Telecommunications" is defined by the Act as "the transmission, between points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received."[152] This definition of "telecommunications" creates an obligation on the part of carriers to protect the integrity of the information being carried. This obligation

---

[149] *See* 40 U.S.C. §§ 481 & 491 and 41 C.F.R. Part 101-38 (Federal Property and Administrative Services Act of 1949); 42 U.S.C. § 6201 et seq. (Energy Policy and Conservation Act); Pub. Law No. 102-486 (Energy Policy Act of 1992); Exec. Order 13031, December 13, 1996 (Federal Alternative Fueled Vehicle Leadership); and Exec. Order 12844, April 21, 1993 (Federal Use of Alternative Fueled Vehicles).

[150] *See* 47 U.S.C. § 1 *et seq*. (The Communications Act of 1934).

[151] 47 U.S.C. §§ 201-276.

[152] 47 U.S.C. § 2(43).

implicitly requires that the carrier protect its infrastructure in order to safeguard the information transmitted.[153] In addition, the FCC under its general statement of purpose from Congress may be able to take further action as necessary[154] to fulfill its mandate to "make available, so far as possible, to all the people of the United States … a rapid and efficient … Communications service with adequate facilities…for the purpose of the national defense, and for the purpose of promoting safety of life and property through the use of wire and radio communication."[155] The Communications Act of 1934 also grants power to the President in times of emergency for the setting of preferences or priorities for communications and the suspension of rules and regulations applicable to stations capable of emitting electromagnetic radiations.[156]

Wireline Telecommunications Carriers

The FCC requires wireline telecommunications carriers to report major service disruptions (generally disruptions that cause loss of service to more than 30,000 customers for more than 30 minutes).[157] The FCC's Federal Advisory Committee, the Network Reliability and Interoperability Council (NRIC), is responsible for analyzing this data. Of the 700 disruptions reported in 1996, all were traceable to physical causes. The most substantial physical "threat" to wireline carriers are dig-ins usually attributable to the failure of the excavator to contact the facility operator before beginning work. While no reported disruptions have to date been attributed to cyber threats, fraud against telecommunications carriers and their customers is believed to cost between 1 and 5 billion dollars annually. The Department of Justice and the Secret Service have primary jurisdiction over these fraud cases. Among the causes of these losses are unauthorized access to customers' PBX network for making long-distance calls, calling card theft and various kinds of pay phone fraud. NRIC is currently studying whether the Telecommunications Act of 1996 has increased the vulnerability of wireline networks to cyber attack, by providing greater access for competitors to telecommunications carrier transmission elements, switching elements and operating systems. Its final report was due Summer of 1997.

The FCC has also attempted to provide protection from harm caused by connection of terminal equipment and associated wiring through uniform

---

[153] *See* 47 U.S.C. §§ 3(44) & 3(46).

[154] 47 U.S.C. § 4(i) provides that the Commission may perform "any and all acts, make such rules and regulations, and issues such orders not inconsistent with this Act as may be necessary in the execution of its functions."

[155] 47 U.S.C. § 1.

[156] *See* 47 U.S.C. § 706.

[157] *See* 47 C.F.R. § 63.100.

standards.[158] Using terminal equipment to defeat telephone billing systems is a harm to the network, and to prevent these harms the Commission has, for example, required PBX machines to return answer supervision signals to the central office. Under the authority of section 208 of the Act, the FCC may hear complaints against carriers. This authority is used to address billing complaints involving fraud caused by third parties, most often through PBX systems.[159]

The FCC's regulations include a couple of seldom used provisions which could be used for infrastructure assurance objectives. 47 U.S.C. § 605 prohibits any person assisting in receiving or transmitting interstate or foreign communication from divulging the communications except through authorized channels. Also, under the authority of 47 U.S.C. § 214(d), the FCC may require, after an opportunity for a full hearing, that a carrier provide itself with adequate facilities for the expeditious and efficient performance of its service as a common carrier. This section has a few exceptions which include those carriers who provide interstate service only through interconnection with facilities of unrelated carriers.[160]

Wireless Telecommunications Carriers

The primary focus of the FCC's regulation of wireless communications is the avoidance of radio frequency interference. The Commission has broad authority over radio services licensees.[161] In addition to the general authority over licensees, the FCC is specifically granted the authority to "suspend the license of any operator upon proof sufficient to satisfy the Commission that the licensee--(C) has willfully damaged or permitted radio apparatus or installations to be damaged."[162] This authority could support additional infrastructure assurance-related regulations.

NRIC has recommended that wireless carriers establish processes for reporting service disruptions, but has not recommended, nor has the FCC required, wireless carriers to follow the reporting requirements placed on wireline carriers. Terrestrial wireless carriers do report disruptions of service of 90 continuous

---

[158] *See* 47 C.F.R. Part 68.

[159] Generally, the FCC has found the customer, rather than the telephone company, liable for fraudulent charges where the customer had the capability to restrict access to and egress from its PBX at all times, particularly where the customer took no steps available to it to detect or prevent unauthorized calls.

[160] *See* 47 U.S.C. § 2(b)(2).

[161] *See* 47 U.S.C. § 303(r).

[162] 47 U.S.C. § 303(m)(1)(C).

days or discontinued service.[163] Satellite wireless carriers file semi-annual reports which include discussions of the causes of any unscheduled transponder outages lasting more than 30 minutes.[164]

Terrestrial wireless carriers are protected from fraud by criminal provisions such as 18 U.S.C. § 1343. Law enforcement agencies have jurisdiction over the criminal prosecutions of those who steal phones or alter electronic serial numbers or mobile identification numbers. Under 47 U.S.C. § 302(d), the FCC has prohibited the intercepting of cellular radio transmissions using certain "scanning devices." Satellite wireless carriers are protected from unauthorized access by 18 U.S.C. § 1367 which criminalizes the intentional or malicious interference with the operation of a satellite.[165] Other provisions prevent unauthorized use, interception and disclosure of communications such as 47 U.S.C. § 605 (prohibits use of radio communications without being "entitled"); 18 U.S.C. §§ 2511-21; and 47 U.S.C. § 333 (prohibits willful or malicious interference with licensed radio communications).

Non-Telecommunications Communications Facilities

The FCC also regulates broadcast television, broadcast radio (AM and FM), shipboard radio, other safety and special radio services, and cable television. The Emergency Alert System (EAS)[166] requires broadcast networks; cable networks and program suppliers; AM, FM, and TV broadcast stations, Low Power TV stations, cable systems and other entities to operate on an organized basis during emergencies. This system allows the President, and local officials during local emergencies, to address the general public. The Plan for the Security Control of Air Traffic and Air Navigation Aids[167] defines the responsibilities of the Commission for the security control of non-federal air

---

[163] *See* 47 C.F.R. § 22.317. NRIC has studied terrestrial wireless service disruptions in cellular radio service based on voluntarily provided data and has concluded that the primary causes of service outages are software design, hardware failure, and procedural error. Network Reliability-- The Path Forward, http://www.fcc.gov/oet/nric, Network Reliability Performance at 6.3. In addition, NRIC has reviewed the performance of terrestrial wireless networks after natural disasters. The Council found that the networks were fairly robust because of the presence of multiple service providers and the mobility of the infrastructure. Portable infrastructure can be imported into an impacted area and service can be quickly restored.

[164] *See* 47 C.F.R. § 25.210(j)(2). New technologies in satellites-- onboard management of individual switched subscriber connections, moving tracking antennas-- will create more complex reliability issues and may necessitate further study.

[165] 18 U.S.C. § 1367 was in response to an incident of unauthorized access to a satellite in 1986-- the so-called "Captain Midnight" event. There was a second incident in 1987.

[166] 47 C.F.R. Part 11.

[167] 47 C.F.R. Part N, §§ 87.393-397.

navigation aids. The Public Safety National Plan[168] specifies special policies and procedures governing the Public Safety Radio Services and the Special Emergency Radio Service.

Continuity of Government Operations

The FCC has a well-developed internal program for protecting the security of its own computer networks and its continued operation. FCC Instruction 1479.1, the FCC Computer Security Program Directive for employees and contractors, sets the policy for ensuring the availability of data and computer systems, the integrity of data and system, and the confidentiality of Commission data.[169] The FCC Computer Security Officer maintains a Two-Year Strategic Plan outlining major Information Technology Center (ITC) tasks and establishes appropriate milestones and anticipated expenditures. The Computer Security Officer also conducts training in compliance with the Computer Security Act of 1987. The FCC requires that contractors work with the Commission to abide by the Computer Security Program Directive and has incorporated this requirement into their contracts.

On a quarterly basis, the Computer Security Officer conducts automated analysis of key systems, in fulfillment of the requirements of the Computer Security Act of 1987. The results are used to eliminate potential system threats and to brief management. Periodic account audits are also conducted on critical systems as another method for collecting threat information. In 1995, the FCC Inspector General and the Computer Security Program began using "Tiger Teams" to identify system security deficiencies. The Computer Security Officer, FCC Telecommunication System Manager and Inspector General are working on addressing similar security concerns for the FCC telecommunications system.

FCC computer hardware is protected through the FCC Physical Security and Guard Force program. Through a series of sensors, monitor stations, closed circuit cameras, and alarms, FCC Physical Security Guard forces are notified when key electronic assets are placed near strategically located sensors. Computer networks managed by ITC also have protective barriers. According to preset conditions, intruders are locked out automatically when the conditions or thresholds are met. Systems either automatically reset after a period of time or

---

[168] 47 C.F.R. § 90.16.

[169] The FCC Computer Security Program is designed to meet all requirements set forth in Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Information Resources, Public Law 100-235, The Computer Security Act of 1987, and other federal mandates for providing computer security support to Federal agency systems. The document details proper use and penalties for misuse of FCC systems, use of identification and authentication for controlling access, as well as guidance on use of electronic mail, intranet and Internet services.

require system management intervention for resetting. The FCC also has a five layer program for controlling computer viruses. The ITC has prepared for emergencies by establishing a Computer Emergency Response Team (CERT). The ITC CERT responds to incidents ranging from inappropriate e-mail to computer intrusions. The FCC also participates in the NIST, Federal Computer Incident Response Capability (FedCIRC) and the NIST Federal Information System Security Manager Forum.

United States Postal Service

Continuity of Government Operations

The U.S. Postal Service is an important element in the continuity of government operations, as well as the continued communication of private businesses and individuals. The Postal Service, an independent establishment of the Executive Branch, has broad authority to accomplish its mission-- the delivery of parcels throughout the world.[170] In addition to the authority to prescribe regulations necessary and appropriate for carrying out its function, the Postal Service also has authority to determine its expenditures.[171] Postal revenues are permanently appropriated to the Postal Service Fund and the Postal Service may also borrow funds within certain prescribed limits.[172]

The Postal Service also has the authority for the investigation and enforcement of all civil and criminal statutes of the United States pertaining to the Postal Service and the mails.[173] This authority is delegated to the Postal Inspection Service,[174] which investigates and enforces both generic statutes governing federal property, employees, and processes as they pertain to the Postal Service, as well as provisions that deal specifically with the Postal Service and the mails.[175] The Postal Service is currently negotiating a memorandum of understanding with the Department of Justice and the Federal Bureau of

---

[170] *See* 39 U.S.C. §§ 201, 403(a); *see also* 39 U.S.C. § 407 (international postal arrangements).

[171] 39 U.S.C. § 401(2), (10); 39 U.S.C. § 401(3).

[172] 39 U.S.C. §§ 2003(b), 2401(a); 39 U.S.C. § 2005(a).

[173] 39 U.S.C. § 404(a)(7); 18 U.S.C. § 3061.

[174] 39 C.F.R. § 224.233.

[175] Specific criminal statutes relating to the mails include: 18 U.S.C. §§ 876-77 (mailing threatening communications); 18 U.S.C. §§ 1701-03 (obstruction of the mails); 18 U.S.C. § 1705 (destruction of a letter box or mail); 18 U.S.C. § 2115 (breaking into post office).

Investigation which will give the Postal Service jurisdiction over crimes involving electronic commerce services offered by the Postal Service. The general powers of the Postal Service also include security guards who may exercise the authority of special police.

Under the Part 26 of Executive Order 12656, Assignment of Emergency Preparedness Responsibilities, the Postal Service has lead responsibility for plans and programs to provide essential postal services during a national security emergency. The Postal Service would also assist other agencies in locating and leasing privately owned property for federal use in such an emergency. Federal Preparedness Circular 60, Continuity of the Executive Branch of the Federal Government at the Headquarters Level During National Security Emergencies, designates the Postal Service as a Category I organization, required to provide a capability for uninterrupted emergency operations during a national security emergency. Procedures for individuals post offices and Headquarters for dealing with disruptions of normal operations are set out in the Postal Service's Headquarters Emergency Plan (February 1991) and the Emergency Planning Manual (December 1981). Both of these plans are currently being considered for update.

Department of the Interior

The bureaus and organizations that comprise the Department of the Interior are the principal federal authority for the proper use and protection of federal lands. The Department's jurisdiction ranges from national parks to Indian reservations. While the Department of the Interior has little direct authority related to infrastructure assurance, the authority that it exercises over federal lands affects many of the critical infrastructures identified in Executive Order 13010. The Department of the Interior also has a limited role in law enforcement for the protection of public safety and public lands and resources. This role provides for cooperation with other law enforcement bodies at the federal, state and local levels.[176] Authorities related to Indian lands are administered by the Bureau of Indian Affairs (BIA). These authorities may have an impact on the infrastructure physically located on Indian lands or infrastructure services provided to the inhabitants of Indian Reservations.[177] Similarly, the National

[176] *See* 446 DM Chapter 1; 43 U.S.C. § 1733, and BLM Law Enforcement General Order 23.

[177] *See, e.g.*, 25 U.S.C. §§ 311-328 and 25 C.F.R. Part 169 (right-of-way through Indian lands for telecommunications purposes); Indian Mineral Development Act of 1982, 25 U.S.C. §§ 2101-09 and 25 C.F.R. Parts 225-27 (oil and gas agreements); American Indian Trust Fund Management Reform Act, 25 U.S.C. §§ 4001-4061; Indian Dams Safety Act, 25 U.S.C. §§

Park Service (NPS) and U.S. Fish and Wildlife Service (FWS) have authority to regulate the conduct of certain infrastructures physically located on National Park and FWS lands.[178]

Emergency Services and Telecommunications

The Bureau of Land Management (BLM) owns a radio, satellite, and microwave communications system, the National Interagency Fire Center (NIFC), designed to coordinate information and communications relevant to wildland fire-fighting operations. The BLM also responds to natural disasters using the National Incident Radio Support Cache, a system of equipment and human resources trained and maintained to travel worldwide. BLM's personnel and telecommunications network cannot assist any state or local jurisdiction absent an interagency agreement or request by the jurisdiction.

BLM also has authority for the physical protection of infrastructures under 18 U.S.C. § 1362, which prohibits the willful or malicious injury or destruction, or willful or malicious attempt to injure or destroy, any of the works, property, or material of any radio, telegraph, telephone or cable, line, station, or system or other means of communication operated or controlled by the United States, whether such system is constructed or under construction. It is also a crime to hinder, delay or obstruct the transmission or communication over such a line or system. BLM has authority to enforce criminal laws protecting satellites and satellite transmissions.[179] Its law enforcement officers also have authority over specific acts on federal land.[180]

Emergency Services

BLM has trained personnel and equipment ready to respond to emergencies involving BLM-owned facilities. These resources include law enforcement, firefighting and environmental response personnel as well as police cars and fire engines. Among the more important authorities granted to the Secretary of Interior for emergencies is the power to enter into cooperative agreements for the protection of federal lands, which includes management as well as law

3801-3804 (maintenance and repair of dams located on Indian lands); Indian Law Enforcement Reform Act, 25 U.S.C. §§ 2801-2809.

[178] 16 U.S.C. § 1 *et seq.*; *See, e.g.*, 16 U.S.C. § 5 & § 79 and 36 C.F.R. § 14 (telecommunications facilities and electric power).

[179] *See* 18 U.S.C. § 1367.

[180] *See, e.g.*, 18 U.S.C. § 1864 (prohibits use of a hazardous or injurious device on federal land).

enforcement functions.[181] Under certain circumstances, the Department is authorized to respond to emergencies absent a cooperative arrangement. 42 U.S.C. § 1856 allows mutual aid in fire protection and emergency assistance in extinguishing fires in the vicinity of agency facilities.

Other important cooperative arrangements exist between Interior and other federal agencies. Via an interagency agreement, NRC is able to use BLM's telecommunications system and personnel for the protection of nuclear facilities under its jurisdiction. BLM has also made an interagency agreement with FEMA to assist state and local governments during emergencies or disasters upon the request of such governments. This interagency agreement is also triggered by Presidentially declared disasters. BLM and NPS are also signatories to the Inter-Departmental MOU allowing Cross-Deputation of Law Enforcement power within the federal government in appropriate cases, including requests for assistance made through the Incident Command System. This System is a federal government wide method that is used in appropriate cases for any federal officer or group of federal officers requesting assistance in an emergency.

At the state level, BLM has MOUs in place with local and state law enforcement and fire prevention offices. Such MOUs and ongoing relationships could be relevant to the provision of emergency services in the event of an attack or natural disaster. One example is the 1993 Cooperative Fire Protection Agreement in the State of Alaska. This agreement designates pre-determined fire protection responsibility areas in Alaska regardless of whether the lands are administered by the federal or state governments, native corporations, boroughs, or the military. The National Park Service has entered into similar agreements for cooperation with law enforcement and fire prevention agencies at the state and local levels. 4 D.C. Code § 201 *et seq*. provides special authority for the Park Police in the District of Columbia and its environs. The NPS may also close park areas for public safety purposes.

Under the National Wildlife Refuge System Administration Act of 1966 certain FWS personnel have law enforcement authority on Service lands.[182] A bill has been pending in Congress since 1995 to give Bureau of Reclamation personnel law enforcement authority to better administer Reclamation lands.

The United States Geological Survey (USGS) research and data collection functions may assist the federal, state and local governments during emergencies. Among the more relevant functions to infrastructure assurance are

---

[181] *See* 43 U.S.C. 1737; Chapter XI-Law Enforcement Cooperation., H-9260-1 BLM Law Enforcement Management.

[182] 16 U.S.C. § 668dd(f).

the Global Seismographic Network (a network of high-quality digital instruments that measure record ground shaking, which can serve as the principal source of public information on earthquakes and explosions occurring internationally),[183] National Water Quality Assessment,[184] and Committee on Civil Applications of Classified Overhead Photography (CAC).[185]

Electric Power

BLM law enforcement officers are authorized to enforce 18 U.S.C. § 1366 which makes it a crime to knowingly or willfully damage or attempt to damage an energy facility. "Energy facility" includes a company involved in the production, storage, transmission, or distribution of electricity, fuel, or another form or source of energy, or research, development, or demonstration facilities related thereto.

The Secretary of the Interior is responsible for preventing "unnecessary or undue degradation of the [public] lands."[186] The Secretary also has the power to grant rights-of-way over, public lands for systems for the generation, transmission, and distribution of electrical energy.[187]

Oil and Gas Storage and Transportation

Under the Mineral Leasing Act[188] similar authority to that in the electric power arena has been granted to the Secretary of the Interior for oil and gas pipelines. BLM enforces 18 U.S.C. § 1366 for oil and gas facilities as well as electric power facilities. In this context, the power to grant rights-of-way for pipelines also includes the authority to impose stipulations addressing damage to public or private property and hazards to public health and safety.[189] If necessary to protect public health, safety, or the environment, the Secretary may order the immediate temporary suspension of activities within the right-of-way or permit area.[190]

---

[183] *See* 15 U.S.C. §§ 5652 (The Land Remote Sensing Policy Act of 1992); 42 U.S.C. §§ 7701 *et seq*. (The Earthquake Hazards Reduction Act of 1977).

[184] *See* Pub. Law No. 102-580 (Water Resources Act of 1992).

[185] Authority for this program is set out is a classified Presidential Directive from 1975.

[186] 43 U.S.C. § 1732(b).

[187] FLPMA § 501(a)(4).

[188] 30 U.S.C. § 185.

[189] 30 U.S.C. § 185(h).

[190] 30 U.S.C. § 185(o).

The Secretary also has the authority to regulate drilling and surface-disturbing activities on public lands. The Secretary is required to set standards for reclamation and restoration after the cessation of oil and gas activities. This standard-setting authority could be used to regulate the rebuilding and the cleanup process on public lands.[191] The Minerals Management Service (MMS) is responsible for all of DOI's oil and gas leasing activities on the Outer Continental Shelf (OCS). Under the Outer Continental Shelf Lands Act,[192] the Secretary of the Interior not only may lease OCS tracts for gas and oil exploration and production, but may also regulate and approve all production plans, including safety and construction specifications; inspect and require reports sufficient to mandate compliance with regulatory standards; and impose civil penalties on lessees not in compliance. This regulatory authority extends to operating procedures, pipelines, and offshore storage of oil and gas. This authority is implemented by 30 C.F.R. Part 250, Oil and Gas and Sulphur Operations in the Outer Continental Shelf. Overlap in the authority of the MMS and the Coast Guard is governed by a MOU providing for coordination. Coordination of overlapping jurisdiction with the Department of Transportation is governed by an MOU dated December 10, 1997, entitled "Memorandum of Understanding Between the Department of Transportation and the Department of Interior Regarding OCS Pipelines."

Transportation

The Department of the Interior only has authority over transportation related to federal lands. However the authority over the transportation infrastructure on federal lands is quite broad, including the authority to grant rights-of-way,[193] enforce criminal laws protecting federal lands,[194] to permit or even require construction and maintenance,[195] and to order immediate temporary suspension of activities on a right-of-way area.[196]

Water

The Bureau of Reclamation (Reclamation) develops, manages, and protects water and related resources in an environmentally sound manner in the interest of the

---

[191] *See* 30 U.S.C. § 226(g).

[192] 43 U.S.C. § 1331 *et seq*.

[193] 43 U.S.C. § 1763.

[194] 18 U.S.C. § 1361 (willful injury of any property of the U.S.); 18 U.S.C. § 1864 (use of a hazardous or injurious device on federal lands).

[195] 43 U.S.C. § 1762(a)-(b).

[196] 43 C.F.R. § 2803.3.

American public. The general authority for Reclamation's activities is found in the Reclamation Act of 1902[197] and the Reclamation Project Act of 1939.[198] Under these acts the Secretary of the Interior is authorized to "perform any and all acts and to make such rules and regulations as may be necessary and proper for the purpose of carrying the provisions of this Act into full force and effect." This includes developing and delivering water supplies for authorized purposes. Under 43 U.S.C. §§ 390b, 485h(c) & 521, the Secretary may enter into contracts to supply water for purposes other than irrigation.[199] Responsibility for operation and management of Reclamation projects may be transferred from the government to water user organizations. This transfer may include provisions for the protection of water supply systems via contract or regulation.[200]

The Reclamation Safety of Dams Act[201] authorizes the Secretary of the Interior to perform such modifications on Reclamation dams as reasonably required to preserve their "structural safety." In the case of an emergency, or unusual conditions, the Commissioner of Reclamation may use emergency funds set aside from the Reclamation fund.[202] For this purpose, "unusual or emergency conditions" means, "…generator failures, damage to transmission lines, or other physical failures or damage, or acts of God, or of the public enemy, fires, floods, drought, epidemics, strikes, or freight embargoes, or conditions, causing or threatening to cause interruption in water or power service."[203] Specific regulations govern the conduct at Reclamation dams, including prohibitions on carrying explosives or willful destruction.[204]

Continuity of Government Operations

On or about October 1, 1997, all BLM law enforcement manual and electronic files, both at the national level and in the field, will be switched on line to a system called LAWNET. The system has been built to deny access to "unauthorized personnel" and to protect the information contained therein from penetration.

---

[197] 43 U.S.C. § 373.

[198] 43 U.S.C. § 485i.

[199] Authority to enter into contracts for irrigation is provided by 43 U.S.C. § 485h(d) & (e).

[200] *See* 43 U.S.C. §§ 498-499.

[201] 43 U.S.C. § 506.

[202] 43 U.S.C. § 502.

[203] 43 U.S.C. § 503.

[204] *See, e.g.*, 43 C.F.R. § 421 (Rules of Conduct at Hoover Dam).

There are also several initiatives being sponsored at the Secretary level which may impact infrastructure assurance. The DOI All-Hazard Coordination Group (AHCG) has representatives from all significant DOI bureaus and offices. AHCG was chartered in 1995 to facilitate interbureau and interagency standardization prior to and during the course of a major, complex incident. The objectives of the group are to provide timely information to policy officials in the Department, Administration and Congress; minimize the loss of life, property and resources; minimize costs of response; function on an interagency basis with other Federal Agencies as well as interstate, state, local and tribal officials; and respond to incidents effectively and in a coordinated manner through sharing of resources, information and personnel within the Department. In addition an interagency agreement with the USDA provides for cross-designation of law enforcement officers to allow supplementation of agency law enforcement personnel resources for law enforcement emergencies, violations in progress, or needs specifically identified. FEMA has delegated its role for all stages of Presidentially declared disasters under the Stafford Act to DOI until FEMA arrives (usually after the first 24 hours). DOI has also created an Emergency Communications Plan for Alaska Operations. DOI is currently in the process of assessing the maintenance and repair issues for its facilities. The study is being conducted by the DOI Planning, Design, and Construction Council and should be completed in June 1997.

Department of State

The Department of State administers itself, or in coordination with other agencies, authorities directed toward detection and control of international terrorism that could be targeted against any or all of the infrastructure areas listed in Executive Order 13010.[205]

Telecommunications

22 U.S.C. § 2707 provides for oversight of foreign policy related to international communications and information policy, and the Department operates the world-wide Diplomatic Telecommunications System serving posts overseas and linking them to Washington.

[205] *See, e.g.*, 18 U.S.C. § 113B; Pub. Law No. 99-399; 22 U.S.C. §§ 2711-12 & 2708; 22 U.S.C. Chapter 64 (aviation security); Pub. Law No. 101-298 (Biological Weapon Control); 22 U.S.C. § 3244 & Pub. Law No. 99-399 (Nuclear Terrorism).

Transportation, Gas and Oil Storage, Water Supply Systems

Executive Order 11423 authorizes the Secretary of State to receive applications for permits and to grant or deny permits for facilities at borders connecting the U.S. with a foreign country, specifically pipelines for petroleum, water or sewage facilities, and facilities for the transport of person or property (*e.g.*, monorail). The Secretary of State also is authorized to administer travel controls into and out of the U.S. for aliens and citizens.[206]

Emergency Services

22 U.S.C. § 2709 authorizes special agents of the Department of State and Foreign Service to exercise specific protective and arrest functions.

Continuity of Government Operations

The Department of State has lead responsibility under Part 13 of Executive Order 12656 for continuity of government and other national emergency activities that affect foreign relations.

United States Information Agency

The U.S. Information Agency (USIA) is responsible for overseas information and education and cultural exchanges. Under the President's mandated reorganization of Foreign Affairs Agencies, USIA will be integrated with the State Department within the next two years. Much of USIA's functions are performed using communications systems, including the Internet and electronic databases and radio and television broadcasts. USIA uses electronic means to link with foreign media, government and academia. It also controls all U.S. non-military international broadcasting, including the Voice of America. Many of the broadcast services are dependent on satellites. However, USIA does not currently have in place any authorities relating to infrastructure assurance though they do have many infrastructure related assets.

[206] *See* 22 U.S.C. § 211a; 8 U.S.C. § 1185; 18 U.S.C. §§ 1541-1546.

Nuclear Regulatory Commission

Electrical Power Systems

The Atomic Energy Act of 1954 (AEA), as amended,[207] and section 201 of the Energy Reorganization Act of 1974[208] provide the NRC with licensing and related regulatory authority over commercial nuclear power plants. Under section 103 of the AEA,[209] the NRC issues commercial licenses for production or utilization facilities including nuclear power plants. The NRC may issue additional standards or instructions to govern the possession and use of special nuclear material as necessary or desirable to promote the common defense and security or to protect health or minimize danger to life or property.[210] The NRC also has authority under the AEA for the protection of restricted data,[211] to guard against the loss or diversion of special nuclear material, and to govern any activity authorized by the AEA. The NRC may require reports, recordkeeping and inspections for activities conducted under section 103 licenses.[212] The NRC may revoke licenses,[213] or impose civil penalties for violations of rules, regulations, or licensing provisions.[214] Criminal penalties are also available for violation of AEA provisions or acts of sabotage. The Attorney General enforces such provisions.[215]

These statutory authorities are implemented by chapter 1 of Title 10 of the Code of Federal Regulations. The NRC has promulgated regulations governing the criteria and procedures for determining eligibility for access to restricted data,

---

[207] 42 U.S.C. § 2011 *et seq*.

[208] 42 U.S.C. § 5811.

[209] 42 U.S.C. § 2133.

[210] *See* 42 U.S.C. § 2201(b).

[211] The NRC has further authority for prescribing rules and regulations necessary to prevent unauthorized disclosure of a licensee's or applicant's safeguards information. *See* 42 U.S.C. § 2167.

[212] This includes a provision of the Energy Reorganization Act of 1974 that requires that directors and responsible officers of companies constructing, owning, operating, or supplying components for AEA licensed activities report to the NRC that a facility, activity, or basic component supplied to such facility fails to comply with AEA provisions or any applicable NRC rule, regulation, order or license pertaining to safety hazards. 42 U.S.C. § 5846.

[213] 42 U.S.C. § 2236.

[214] 42 U.S.C. § 2282. Injunctive relief for violations of the AEA, or regulations thereunder, is also available with the assistance of the Attorney General of the United States. 42 U.S.C. § 2280.

[215] *See* 42 U.S.C. § 2271 *et seq*.

national security information, special nuclear material and employment clearance; reporting of defects and noncompliance; domestic licensing of production and utilization facilities; physical protection of plants and materials; material control and accounting of special nuclear material; and security facility approval and safeguarding of national security information and restricted data.

Transportation

Implementation of authority to impose requirements for transportation of nuclear materials is limited to safe packaging requirements to ensure radiological health and safety, and to safeguard requirements to assure the security of designated shipments of nuclear material from sabotage. The NRC has the authority to establish by rules, regulation, or order such standards and instructions to govern the possession and use of special nuclear material as the NRC may deem necessary or desirable to promote the common defense and security or to promote health or to minimize danger to life or property.[216] The NRC may also promulgate rules or regulations to guard against the loss or diversion of special nuclear material and to prevent such use or disposition thereof as the NRC determines to be inimical to the common defense and security.[217]

Federal Energy Regulatory Commission

The Federal Energy Regulatory Commission (FERC) was established by the Department of Energy Organization Act.[218] FERC has authorities relating to many aspects of interstate energy generation, transmission and sale covering electric facilities, hydroelectric facilities, and oil and gas facilities.

Electric Facilities (Non-Hydroelectric)

Under the Federal Power Act (FPA),[219] FERC has the following authorities over interstate transmission and wholesale sale of electric power: (1) reporting requirements; (2) investigatory authority; (3) authority to require interconnection

[216] 42 U.S.C. § 2201(b).

[217] 42 U.S.C. § 2201(i). The implementing regulations are located at 10 C.F.R. Parts 71 (packaging and transportation of radioactive material) & 73 (physical protection of plants and materials).

[218] 42 U.S.C. §§ 7101-7352.

[219] 16 U.S.C. §§ 791a-825r.

and services; (4) rate and service oversight authorities; and (5) consultation and other general authorities.

More specifically, FERC has the general authority, delegated from DOE, to require public utilities to file periodic or special reports "as necessary or appropriate to assist the Commission in the proper administration of this Act [FPA]."[220] In addition, FERC has the authority to require public utilities to make reports regarding anticipated shortages, to make and periodically revise contingency plans to deal with shortages, and to accommodate any shortages in a manner that gives due consideration to public health and safety.[221] Such statutory authority and the implementing rules were written to insure continuity of service to customers of public utilities. FERC also requires information to be transmitted annually by transmitting utilities regarding available transmission capacity and known constraints.[222]

FERC has authority to conduct investigations regarding violations of the FPA or its regulations and to acquire information to serve as a basis for recommending further legislation.[223] FERC's rules relating to investigations are contained in 18 C.F.R. Part 1b.

Upon application of a State commission or any person engaged in the transmission or sale of electric energy, FERC may direct a public utility to establish physical connection of its transmission facilities with other facilities, and to sell and exchange energy. This authority is subject to a public interest standard, and may not be used to compel the enlargement of generating facilities, or if the connection would impair the ability of the utility to render adequate service to its customers.[224] Under a similar procedure, after a complaint by a State Commission, FERC may require a utility to provide an adequate level of service as determined by FERC.[225]

FERC's rate and service oversight authorities allow review of rules, regulations, contracts and practices affecting rates within it jurisdiction to determine whether they are unjust, unreasonable, or unduly discriminatory. Upon such a finding,

---

[220] 16 U.S.C. § 825c (by delegation from DOE per Delegation Order No. 0204-1).

[221] *See* 16 U.S.C. § 824a(g); 18 C.F.R. Part 294.

[222] 16 U.S.C. § 8241; 18 C.F.R. § 141.300 (requiring filing of Form No. 715).

[223] 16 U.S.C. § 825f; 16 U.S.C. § 825j (by delegation from DOE per Delegation Order No. 0204-1).

[224] *See* 16 U.S.C. § 824a(b); *see also* 16 U.S.C. § 824i (additional interconnection authorities).

[225] 16 U.S.C. § 824f.

FERC may determine just and reasonable terms to be thereafter observed.[226] FERC noted this authority as having potential applications for addressing reliability concerns. FERC has used related authorities to promulgate rules regarding the requirements for rate schedules, offer of non-discriminatory open access transmission,[227] and utility participation in electronic information systems.[228]

Under PURPA, DOE is to consult with FERC with respect to requesting, from time to time, the reliability councils or other appropriate persons (including federal agencies) to examine and report concerning any electric utility reliability issue; and recommending industry standards for reliability to the electric utility industry, including standards with respect to equipment, operating procedures, and training of personnel.

In addition to these authorities, FERC also has general authority to "perform any and all acts…as it may find necessary or appropriate to carry out of the provisions of this Act [FPA]."[229] FERC may seek court orders to enforce provisions of the FPA or any rule or order thereunder.

FERC Order No. 889[230] requires that public utilities that own, control, or operate interstate transmission facilities to participate in an electronic information system (OASIS) in order to disseminate transmission information on a uniform basis. FERC included in the rule security measures that were proposed by industry including data encryption, firewalls, and use of passwords. The initial phase of compliance with these requirements was to be completed in January 1997. FERC is considering a second phase of implementation that would require additional functions and performance requirements. FERC does not view potential cyber threats as posing a significant danger to the OASIS system because it is not directly linked to industry operating systems.

Hydroelectric Facilities

FERC's authority to issue licenses for hydroelectric facilities includes regulations regarding the keeping of records, investigatory authorities, and requirements for construction, maintenance and operation. Many of FERC's regulations in this

---

[226] *See* 16 U.S.C. §§ 824d & 824e.

[227] *See* 18 C.F.R. Part 35.

[228] *See* 18 C.F.R. Part 37.

[229] 16 U.S.C. § 825h.

[230] 61 Fed. Reg. 21,737 (May 10, 1996), FERC Stats. & Regs. Para. 31.035 (1996), *order on reh'g*, Order No. 889-A, 62 Fed. Reg. 12,484 (March 14, 1997), FERC Stats. & Regs. Para. 31,049 (1997), *reh'g pending.*

area require coordination or adherence to other federal entity rules or regulations. FERC works closely in this area with many other interested parties, such as the U.S. Coast Guard, U.S. Army Corps of Engineers, the Bureau of Reclamation, NRC, DOE, FEMA, and the Washington State Department of Ecology. These entities, and additional regional agencies, were all identified by FERC as having a stake in infrastructure assurance for hydroelectric facilities.

Gas and Oil Storage and Transportation

FERC has authority, delegated from DOE, to approve or disapprove the siting, construction and operation of new domestic facilities at the place of entry for imports or exit for exports, unless the Assistance Secretary exercises this disapproval authority. FERC also has authority over the rates and charges of natural gas companies. Rates must be filed with FERC and must be just and reasonable. It has authority to alter natural gas tariffs if found not to be just and reasonable, and to require natural gas companies to extend or improve their gas transportation facilities and to establish physical connections with other facilities. FERC must provide approval before any natural gas company can undertake or complete construction, operation, acquisition, extension, or improvement of facilities used for the transportation of gas in interstate commerce. It may impose reasonable conditions on such authorizations. All such authorities are derived from the Natural Gas Act (NGA).[231]

FERC also has authority over the rates and practices of oil pipelines pursuant to the Interstate Commerce Act.[232] FERC's authority to review oil company tariffs and to impose terms and conditions could be used to further infrastructure assurance objectives.

Department of Agriculture

The Department of Agriculture (Agriculture) has numerous grant and loan programs in place to assist rural areas in receiving important services that touch on many of the critical infrastructures. They include the Rural Utilities Service, the Rural Housing Service, and the Rural Business-Cooperative Service. These loan and grant programs are used to foster telecommunications, electric, oil and gas, water, transportation and banking and finance related services in rural areas. Loans and grants are also available to improve emergency services such as fire and rescue squads. These programs usually require compliance with

[231] 15 U.S.C. §§ 717b *et seq.*

[232] 49 U.S.C. §§ 1(5), 2, 6, 15(1) & 15(7).

Agriculture regulations in constructing or operating facilities with loan or grant funds. The Department of Agriculture currently notes that these regulations do not specifically take into account the need to withstand physical or cyber attack, or other infrastructure assurance related issues. Additional programs, such as the Distance Learning and Telemedicine project may also need to be reviewed to ensure that they adequately take into account cyber and other threats in their operations and regulations.

The Securities and Exchange Commission

The Securities and Exchange Commission (SEC) has various authorities to respond to emergencies under the Securities Exchange Act of 1934 and the Investment Company Act of 1940. The SEC's emergency authorities may generally be invoked when there is a major market disturbance characterized by the occurrence or substantial threat of either sudden or excessive price volatility or substantial disruption of the safe or efficient operation for clearance and settlement.[233] In the event of such an emergency, the SEC may: (1) suspend all trading in nonexempt securities on an exchange or off-exchange for up to 90 calendar days; (2) suspend trading of nonexempt individual securities and groups of securities for no more than 10 business days; (3) alter existing Commission and self-regulatory organization (SRO) rules or impose new restrictions and approve SRO rules on an expedited basis; and (4) take emergency action with respect to mutual fund redemptions. The Commission is also authorized to approve SRO rules which allow some exchanges to conduct trading halts in response to national security situations. Individual SRO trade halts have been used infrequently, but have been successful enough to obviate the need for the SEC to invoke its authority to halt trading.

Board of Governors of the Federal Reserve System

The Board of Governors of the Federal Reserve System (Federal Reserve) has authority related directly to only one of the critical infrastructures being studied

[233] 15 U.S.C. § 781(k)(6).

by the Commission—banking and finance. However, the Federal Reserve also may exercise certain powers, such as making properly secured loans to individuals, partnerships or corporations, which may indirectly impact the other critical infrastructures listed in Executive Order 13010.[234]

Banking and Finance

The Federal Reserve has authority to examine certain depository institutions and other financial institutions for the purpose of addressing the safety and soundness of their business practices. The institutions include member banks of the Federal Reserve System;[235] registered bank holding companies;[236] Edge Act corporations and agreement corporations;[237] foreign branches of U.S. member banks;[238] U.S. branches, agencies, and affiliates of foreign banks;[239] representative offices of foreign banks;[240] and Federal Reserve banks.[241] Among the enforcement actions that the Federal Reserve may take against these financial institutions are cease and desist orders,[242] orders of removal and prohibition,[243] and orders of assessment of civil monetary penalties.[244] Bank Service Corporations are also subject to examination and regulation by appropriate federal banking agencies.[245]

The Bank Protection Act[246] permits the Federal Reserve, the Comptroller of the Currency, the Federal Deposit Insurance Corporation, and the Director of the Office of Thrift Supervision, to issue rules establishing minimum standards for banks and savings and loan associations with regard to the installation, maintenance, and operation of security devices and procedures, in order to

---

234 *See, e.g.,* 12 U.S.C. §§ 343 & 347c.

235 12 U.S.C. §§ 325-326.

236 12 U.S.C. § 18439c.

237 12 U.S.C. §§ 625 & 602.

238 12 U.S.C. § 602.

239 12 U.S.C. § 3105.

240 12 U.S.C.. § 3107.

241 12 U.S.C. § 248(j), 485.

242 12 U.S.C. § 1818(b).

243 12 U.S.C. § 1818(e).

244 12 U.S.C. §§ 1818(i) & 1847.

245 *See* 12 U.S.C. §§ 1861-67.

246 12 U.S.C. §§ 1881-84.

discourage robberies, burglaries, and larcenies and to assist in the identification and apprehension of persons who commit such acts.[247]

The Federal Reserve has several unique authorities that may allow for reconstitution of the banking and finance infrastructure. Under sections 10(b) and 13(8) of the Federal Reserve Act,[248] a Federal Reserve Bank may make appropriately secured advances to member banks at appropriate rates subject to rules and regulations of the Reserve Board.[249] The Board of Governors may suspend, for a period not to exceed thirty days, any reserve requirements specified in the Federal Reserve Act.[250] The Board is also responsible for the circulation of sufficient currency to meet the needs of the economy.[251] In addition to its rulemaking authority for the automation of the check processing system,[252] the Federal Reserve may suspend certain requirements regarding the availability of funds deposited by check in the event of any interruption of communication facilities, suspension of payments by another institution, war, or other emergency beyond the control of the depository institution.[253]

Federal Deposit Insurance Corporation

The Federal Deposit Insurance Corporation (FDIC) takes a very active role in the assurance of the banking infrastructure. Through its regulatory authority to conduct examinations of insured banks and depository institutions,[254] the FDIC has put in place regulations and policies intended to respond to the risks posed to banks by the integration of computer technology into retail banking operations. In February 1997, the FDIC issued the Electronic Banking Safety and Soundness Procedures and Financial Institution Letter (FIL) 14-97 to all insured financial institutions. The issuance resulted from requests of the banking industry for guidance on safety and soundness of practices in electronic banking. The Procedures not only identify risks, but also require examiners to monitor bank practices to ensure the appropriate safeguards are in place. The safeguards

---

247 *See* Regulation P, 12 C.F.R. Part 216.

248 12 U.S.C. §§ 347b & 347.

249 *See generally* Regulation A, 12 C.F.R. § 201.

250 12 U.S.C. § 248(c).

251 12 U.S.C. §§ 411-421 & 428(o).

252 12 U.S.C. § 4008 (Expedited Funds Availability Act).

253 12 U.S.C. § 4003(d); 12 C.F.R. § 229.13(f).

254 *See, e.g.*, 12 U.S.C. §§ 1819-1820 & 1868.

include capabilities to detect and prevent unauthorized access and duplicate transactions. The Procedures address: (1) system planning and deployment; (2) system operating policies and procedures; (3) transactional audit procedures; (4) legal and regulatory matters; (5) administration and systems operation; and (6) vendors and outsourcing.

In addition, FDIC issued guidance in July 1997 emphasizing the need to plan for the restoration of service resulting from any interruption of a key information system.[255] The FDIC policy reflects the revised policy guidance of the interagency Federal Financial Institutions Examination Council (FFIEC) on Corporate Business Resumption and Contingency Planning. The FDIC policy specifically names the board of directors as being responsible for ensuring that appropriate plans have been implemented for each financial institution. Contingency plans are evaluated by examiners during regular supervisory reviews of institutions.

The FDIC submission also noted that banks are required to report known or suspected criminal violations of federal law or suspicious transactions related to money laundering activity or a violation of the Bank Secrecy Act.[256] The Suspicious Activity Reporting (SAR) is currently administered by the Financial Crimes Enforcement Network (FinCEN) on behalf of federal banking and credit union regulators (including FDIC, OCC, OTS, Federal Reserve, and the NCUA). FinCEN acts as a central collection point and includes all SARs in a database available to law enforcement and regulatory agencies.

International Trade Commission

The International Trade Commission (ITC) is an independent, quasi-judicial agency established to govern trade-related matters. ITC has various investigative and adjudicative powers related to unfair trade practices, including import practices that harm U.S. businesses, patent infringement, economic effects of trade agreements and collection of trade-related data and statistics.

The primary area of ITC operations concerned with infrastructure assurance relates to the internal security of the agency, which includes both physical and information security. Information security is governed by a series of ITC Directives. U.S. ITC Directive 1345.0 established an Information Security Committee composed of management, general counsel, and external relations

[255] *See* FDIC, Financial Institution Letter 68-97 (July 14, 1997).

[256] *See* 12 U.S.C. §§ 1818-1819; 31 U.S.C. § 5318; 12 C.F.R. Part 353.

representatives. The Committee is responsible for developing, defining, inspecting and advising on the agency's facilities, procedures and controls for safeguarding national security information, sensitive information, and confidential business information in the possession and control of the ITC. Included within the ITC information security directives are requirements that employees report all possible compromises to ITC data and specific penalties for violations of ITC policy.

Conclusion

There are some very general conclusions that can be drawn from this federal "landscaping" exercise. First, there are many robust laws and regulations in place that serve to protect and assure our nation's critical infrastructures. Many of these laws and regulations were put in place with objectives other than infrastructure assurance in mind, but they nonetheless contribute to the infrastructures' resistance to threats of many kinds. However, the emerging cyber threat has only been addressed in very discrete areas. And as agencies begin to address the cyber threat they do so in a largely uncoordinated effort across the federal government. Coordination is going to be crucial for successful infrastructure assurance efforts because of the large number of federal organizations involved, not to mention state and local, international, and private concerns. This report can act as an important roadmap in considering who should be brought to the table from the federal government to plan and coordinate use of particular sets of legal authorities.

As infrastructure assurance efforts progress into the future, additional legal work is going to be crucial. This first attempt to survey and present the legal authorities of federal agencies with missions related to infrastructure assurance has only been a small part of the much larger task. The larger task that should be accomplished is closer review of the relevant authorities, mechanisms, and programs to ensure that they are appropriately compatible, that there are not unnecessary redundancies, that jurisdictional boundaries have been drawn properly, and that each crucial component has found a home within a responsible federal organization. This report may act as a starting point for this activity by focusing attention on such areas as priorities in restoration of service, new infrastructure assurance concerns such as interdependencies, and demonstrating the link between infrastructure assurance and agency missions that may be suitable for inclusion in agency strategic planning efforts. In addition, future efforts should begin to fold state and local, international and private authorities, mechanisms and policies into the large picture of the legal landscape for infrastructure assurance.

Table of Authorities

Statutes

12 U.S.C. § 1818(b) _____ 58

12 U.S.C. § 1818(e) _____ 58

12 U.S.C. § 18439c _____ 58

12 U.S.C. § 248(c) _____ 58

12 U.S.C. § 248(j), 485 _____ 58

12 U.S.C. § 3105 _____ 58

12 U.S.C. § 391 _____ 29

12 U.S.C. § 4003(d) _____ 59

12 U.S.C. § 4008 _____ 59

12 U.S.C. § 602 _____ 58

12 U.S.C. §§ 1818(i) & 1847 _____ 58

12 U.S.C. §§ 1818-1819 _____ 60

12 U.S.C. §§ 1819-1820 & 1868 _____ 59

12 U.S.C. §§ 1861-67 _____ 58

12 U.S.C. §§ 1881-84 _____ 58

12 U.S.C. §§ 325-326 _____ 58

12 U.S.C. §§ 343 & 347c _____ 57

12 U.S.C. §§ 347b & 347 _____ 58

12 U.S.C. §§ 411-421 & 428(o) _____ 58

12 U.S.C. §§ 625 & 602 _____ 58

12 U.S.C.. § 3107 _____ 58

13 U.S.C. § 9 _____ 27

Statutes (continued)

15 U.S.C. § 717b(a) 19

15 U.S.C. § 717z 19

15 U.S.C. § 781(k)(6) 57

15 U.S.C. §§ 3362-3363 19

15 U.S.C. §§ 5652 47

15 U.S.C. §§ 717b *et seq.* 56

16 U.S.C. § 1 *et seq.* 45

16 U.S.C. § 2601 *et seq.* 19

16 U.S.C. § 5 & § 79 45

16 U.S.C. § 668dd(f) 47

16 U.S.C. § 791a *et seq.* 17

16 U.S.C. § 8241 54

16 U.S.C. § 824-2(b) 17

16 U.S.C. § 824a(b) 54

16 U.S.C. § 824a(g) 54

16 U.S.C. § 824f 54

16 U.S.C. § 824i 54

16 U.S.C. § 825c 54

16 U.S.C. § 825f 54

16 U.S.C. § 825h 55

16 U.S.C. § 825j 54

16 U.S.C. § 825s 17

16 U.S.C. § 837g-1 17

16 U.S.C. § 839 17

16 U.S.C. §§ 791a-825r 53

16 U.S.C. §§ 824d & 824e 54

Statutes (continued)

18 U.S.C. § 1029 ____ 35

18 U.S.C. § 1030 ____ 16, 35

18 U.S.C. § 113B ____ 50

18 U.S.C. § 1343 ____ 41

18 U.S.C. § 1361 ____ 48

18 U.S.C. § 1362 ____ 45

18 U.S.C. § 1366 ____ 47

18 U.S.C. § 1367 ____ 41, 45

18 U.S.C. § 1705 ____ 44

18 U.S.C. § 1864 ____ 45, 48

18 U.S.C. § 2115 ____ 44

18 U.S.C. § 2153 ____ 16

18 U.S.C. § 2511 ____ 16

18 U.S.C. § 3056 ____ 34, 35

18 U.S.C. § 3061 ____ 44

18 U.S.C. § 641 ____ 16

18 U.S.C. § 871 & 879 ____ 35

18 U.S.C. §§ 1541-1546 ____ 51

18 U.S.C. §§ 1701-03 ____ 44

18 U.S.C. §§ 2511-21 ____ 41

18 U.S.C. §§ 793-94 ____ 16

18 U.S.C. §§ 876-77 ____ 44

18 U.S.C. Chapter 40 ____ 34

18 U.S.C. Chapter 44 ____ 34

19 U.S.C. § 1589a ____ 33

19 U.S.C. § 482 ____ 33

Statutes (continued)

20 U.S.C. § 5801 *et seq.* 36

20 U.S.C. § 6801 *et seq.* 36

20 U.S.C. § 8001 36

20 U.S.C. § 8003 36

20 U.S.C. § 8003 36

22 U.S.C. § 211a 51

22 U.S.C. § 2707 51

22 U.S.C. § 2709 51

22 U.S.C. § 2778 34

22 U.S.C. § 3244 50

22 U.S.C. § 401 33

22 U.S.C. §§ 2711-12 & 2708 50

22 U.S.C. Chapter 64 50

23 U.S.C. § 125 21

25 U.S.C. §§ 2101-09 45

25 U.S.C. §§ 2801-2809 45

25 U.S.C. §§ 311-328 45

25 U.S.C. §§ 3801-3804 45

25 U.S.C. §§ 4001-4061 45

28 U.S.C. § 533 15

3 U.S.C. § 202 35

30 U.S.C. § 185 47

30 U.S.C. § 185(h) 48

30 U.S.C. § 185(o) 48

30 U.S.C. § 226(g) 48

31 U.S.C. § 3121 *et seq.* 29

Statutes (continued)

31 U.S.C. § 5317(b) _____ 33

31 U.S.C. § 5318 _____ 60

33 U.S.C. § 1225, 1231 _____ 21

33 U.S.C. § 467h _____ 24

39 U.S.C. § 2005(a) _____ 43

39 U.S.C. § 401(2), (10) _____ 43

39 U.S.C. § 401(3) _____ 43

39 U.S.C. § 404(a)(7) _____ 44

39 U.S.C. § 407 _____ 43

39 U.S.C. §§ 2003(b), 2401(a) _____ 43

39 U.S.C. §§ 201, 403(a) _____ 43

40 U.S.C. § 471 *et seq.* _____ 36

40 U.S.C. § 490(a)(17)-(19) _____ 38

40 U.S.C. §§ 481 & 491 _____ 38

40 U.S.C. §§ 601-619, 490 _____ 36

41 U.S.C. § 251 *et seq.* _____ 18

41 U.S.C. §§ 405 & 421 _____ 36

42 U.S.C. § 1856 _____ 46

42 U.S.C. § 2011 *et seq.* _____ 17, 52

42 U.S.C. § 2133 _____ 52

42 U.S.C. § 2167 _____ 52

42 U.S.C. § 2201(b) _____ 52, 53

42 U.S.C. § 2201(i) _____ 53

42 U.S.C. § 2236 _____ 52

42 U.S.C. § 2271 *et seq.* _____ 52

42 U.S.C. § 2280 _____ 52

Statutes (continued)

42 U.S.C. § 2282 ____ 52

42 U.S.C. § 4001 *et seq.* ____ 24

42 U.S.C. § 5170 *et seq.* ____ 11, 24, 26, 50

42 U.S.C. § 5171 ____ 24

42 U.S.C. § 5191(b) ____ 24

42 U.S.C. § 5196(c), (g) & (h) ____ 24

42 U.S.C. § 5196(e) ____ 23

42 U.S.C. § 5811 ____ 52

42 U.S.C. § 5846 ____ 52

42 U.S.C. § 6201 *et seq.* ____ 38

42 U.S.C. § 7701 *et seq.* ____ 24

42 U.S.C. § 8301 *et seq.* ____ 19

42 U.S.C. §§ 6231-6241 ____ 18

42 U.S.C. §§ 7101-7352 ____ 53

42 U.S.C. §§ 7270a-7270b ____ 18

42 U.S.C. §§ 7701 *et seq.* ____ 47

42 U.S.C. 5195a(a)(1) ____ 23

43 U.S.C. § 1331 *et seq.* ____ 48

43 U.S.C. § 1732(b) ____ 47

43 U.S.C. § 1733 ____ 45

43 U.S.C. § 1762(a)-(b) ____ 49

43 U.S.C. § 1763 ____ 48

43 U.S.C. § 373 ____ 49

43 U.S.C. § 485h(d) & (e) ____ 49

43 U.S.C. § 485i ____ 49

43 U.S.C. § 502 ____ 49

Statutes (continued)

43 U.S.C. § 503 ____ 49

43 U.S.C. § 506 ____ 49

43 U.S.C. § 620 *et seq.* ____ 17

43 U.S.C. §§ 390b ____ 49

43 U.S.C. §§ 498-499 ____ 49

43 U.S.C. 1737 ____ 46

46 U.S.C. § 3703 ____ 21

46 U.SC. § 3306 ____ 21

47 U.S.C. § 1 ____ 39

47 U.S.C. § 1 *et seq.* ____ 38

47 U.S.C. § 2(43) ____ 39

47 U.S.C. § 2(b)(2) ____ 40

47 U.S.C. § 214(d) ____ 40

47 U.S.C. § 302(d) ____ 41

47 U.S.C. § 303(m)(1)(C) ____ 41

47 U.S.C. § 303(r) ____ 41

47 U.S.C. § 333 ____ 42

47 U.S.C. § 4(i) ____ 39

47 U.S.C. § 605 ____ 40, 41

47 U.S.C. § 606 ____ 25

47 U.S.C. § 706 ____ 39

47 U.S.C. § 721(a)(6) ____ 26

47 U.S.C. § 902(b)(2)(A) ____ 25

47 U.S.C. §§ 201-276 ____ 39

47 U.S.C. §§ 3(44) & 3(46) ____ 39

49 U.S.C. § 13931 ____ 22

Statutes (continued)

49 U.S.C. § 5307(d)(1)(J)(i) _____ 22

49 U.S.C. § 5321 _____ 21

49 U.S.C. § 60102 _____ 20

49 U.S.C. § 60103 _____ 20

49 U.S.C. § 60123 _____ 20

49 U.S.C. §§ 1(5), 2, 6, 15(1) & 15(7) _____ 56

49 U.S.C. app. §§ 1801-19 _____ 21

50 U.S.C. § 1701 *et seq.* _____ 26, 33

50 U.S.C. § 1701 *et seq.* _____ 26

50 U.S.C. § 191 _____ 34

50 U.S.C. § 402(I)(1) _____ 15

50 U.S.C. § 403 _____ 15

50 U.S.C. § 403-3(c) _____ 15

50 U.S.C. § 403-3(d)(1) _____ 14

50 U.S.C. § 403-4(e) _____ 15

50 U.S.C. § 413b(a) & (e) _____ 15

50 U.S.C. § 7270b(a) _____ 18

50 U.S.C. §§ 205-226 _____ 34

50 U.S.C. §§ 219-226 _____ 33

50 U.S.C. §§ 401 *et seq.* _____ 14

50 U.S.C. §§ 403a *et seq.* _____ 14

50 U.S.C. app. § 2061 *et seq.* _____ 10,17, 18, 19, 26

50 U.S.C. app. § 2071(a) _____ 17

50 U.S.C. app. § 2071(c) _____ 17

50 U.S.C. app. § 2158 _____ 19

50 U.S.C. app. § 2160 _____ 19

Statutes (continued)

50 U.S.C. app. § 2401 *et seq.* 26

8 U.S.C. § 1185 51

Title 18 U.S.C. Chapter 25 35

Pub. Law No. 99-399 50

Pub. Law No. 100-235 20, 27, 28, 29, 30, 31, 41, 42

Pub. Law No. 101-298 50

Public Law 101-509 35

Pub. Law No. 102-486 38

Pub. Law No. 102-580 47

Pub. Law No. 103-62 14

Pub. Law No. 104-104 38

Pub. Law No. 104-106 14, 27, 37

Pub. Law No. 104-201 11, 15

Pub. Law No. 104-208 36, 37

Title 19, United States Code 32

Regulations

10 C.F.R. § 1048.5 18

12 C.F.R. § 201 58

12 C.F.R. § 229.13(f) 59

12 C.F.R. Part 216 58

12 C.F.R. Part 353 60

15 C.F.R. Part 730 26

18 C.F.R. § 141.300 54

18 C.F.R. Part 1b 54

18 C.F.R. Part 294 54

18 C.F.R. Part 35 54

Regulations (continued)

18 C.F.R. Part 37 ____ 54

19 C.F.R. Part 122 ____ 33

23 C.F.R. Part 668 ____ 21

25 C.F.R. Part 169 ____ 45

25 C.F.R. Parts 225-27 ____ 45

28 C.F.R. Part 0.85 ____ 15

28 C.F.R. Part 0.85(a) ____ 15

30 C.F.R. Part 250 ____ 48

36 C.F.R. § 14 ____ 45

39 C.F.R. § 224.233 ____ 44

41 C.F.R. Chapter 101 ____ 36

41 C.F.R. Part 101-38 ____ 38

43 C.F.R. § 2803.3 ____ 49

43 C.F.R. § 421 ____ 49

47 C.F.R. § 22.317 ____ 41

47 C.F.R. § 25.210(j)(2) ____ 41

47 C.F.R. § 63.100 ____ 40

47 C.F.R. § 90.16 ____ 42

47 C.F.R. Part 11 ____ 42

47 C.F.R. Part 68 ____ 40

47 C.F.R. Part N, §§ 87.393-397 ____ 42

48 C.F.R. Chapter 1 ____ 37

49 C.F.R. § 192.613 ____ 20

49 C.F.R. § 192.615 ____ 20

49 C.F.R. § 195.402 (c)-(d) ____ 20

49 C.F.R. § 195.403 ____ 20

Regulations (continued)

49 C.F.R. §§ 192.614 & 195.442 _____ 20

49 C.F.R. §§ 192.705 & 192.721 _____ 20

49 C.F.R. §§ 195.116, 195.254, & 195.258 _____ 20

49 C.F.R. §§ 195.430 & 195.436 _____ 20

49 C.F.R. Part 190 _____ 20

49 C.F.R. Part 192, subpart D _____ 20

49 C.F.R. Part 193 _____ 20

61 Fed. Reg. 21,737 (May 10, 1996) _____ 55

62 Fed. Reg. 12,484 (March 14, 1997) _____ 55

Title 10 of the Code of Federal Regulations _____ 52

Presidential Authorities

Executive Order 10485 _____ 17

Executive Order 11423 _____ 51

Executive Order 12148 _____ 24

Executive Order 12333 _____ 14, 15, 30, 31

Executive Order 12472 _____ 25, 37

Executive Order 12631 _____ 28

Executive Order 12656 _____ 24, 37, 44, 51

Executive Order 12844 _____ 38

Executive Order 13010 _____ 1, 45, 50, 57

Executive Order 13031 _____ 38

National Security Directive 42 _____ 31

Presidental Memorandum, Facilitating Access to Federal Property for the Siting of Mobile Services Antennas _____ 38

Agency Authorities

BLM Law Enforcement General Order 23 _____ 45

FERC Order No. 889 _____ 55

Agency Authorities (continued)

1993 Cooperative Fire Protection Agreement in the State of Alaska _____ 46

DOE Delegation Order No. 0204-1_____ 54

Electronic Banking Safety and Soundness Procedures and Financial Institution Letter (FIL) 14-97 _____ 59

FCC Instruction 1479.1_____ 42

FDIC, Financial Institution Letter 68-97_____ 59

Federal Preparedness Circular 60 _____ 27, 44

Federal Response Plan_____ 11, 12

H-9260-1 BLM Law Enforcement Management_____ 46

Inter-Departmental MOU allowing Cross-Deputation of Law Enforcement_____ 46

Memorandum of Understanding Between the Department of Transportation and the Department of Interior Regarding OCS Pipelines _____ 48

Memorandum of Understanding Between the Director of the National Institute of Standards and Technology and the Director of the National Security Agency Concerning the Implementation of the Public Law 100-23532

NTIA Emergency Readiness Plan for Use of the Radio Spectrum _____ 25

OMB Circular No. 1-119 _____ 30

OMB Circular No. A-130 _____ 42

Other Authorities

4 D.C. Code § 201 *et seq*. _____ 46

Cases

United States v. Ajlouny, 629 F.2d 830 (2d Cir. 1980)_____ 33

Reference Materials

Argonne National Laboratory, *Overview of the Impacts of Regulatory Agency Practices on Critical Infrastructure Protection*_____ 8, 11

Critical Infrastructure Working Group Report _____ 30

Network Reliability Performance (NRIC)_____ 41

Network Reliability-- The Path Forward (NRIC) _____ 41

Appendix

Federal Agency Contacts

CENTRAL INTELLIGENCE AGENCY
Tom Benjamin
Jonathan Fredman

FEDERAL BUREAU OF INVESTIGATION
M. E. Brown, Associate General Counsel
Marion Bowman

DEPARTMENT OF ENERGY
Samuel Bradley

DEPARTMENT OF TRANSPORTATION
Steve Metoyer
David Tochen

FEDERAL EMERGENCY MANAGEMENT AGENCY
Joseph Flynn

DEPARTMENT OF COMMERCE
Roman W. Sloniewsky

DEPARTMENT OF TREASURY
Virginia Rutledge

DEPARTMENT OF JUSTICE
Vincent Garvey, Civil Division, Federal Programs Branch
Chris Kelly, Antitrust Division
Jeffrey Axelrad, Civil Division, Torts Branch
Sarah Locke, Civil Division, Torts Branch
Roger Pincus, Office of Intelligence Policy and Review
Rosemary Hart, Office of Legal Counsel

NATIONAL SECURITY AGENCY
Richard Marshall, Associate General Counsel

U.S. CUSTOMS SERVICE
Ellen Y. McClain, Deputy Assistant Chief Counsel (Enforcement)

BUREAU OF ALCOHOL, TOBACCO & FIREARMS
David Lieberman, Attorney

U.S. SECRET SERVICE
Mark Mulligan, Attorney/Advisor

DEPARTMENT OF EDUCATION
Deborah Friendly

GENERAL SERVICES ADMINISTRATION
Michael Ettner, Senior Assistant General Counsel

FEDERAL COMMUNICATIONS COMMISSION
Jim Keegan, Associate Chief, Networks

U.S. POSTAL SERVICE
Fred Eggleston, Chief Counsel
Andrew German

DEPARTMENT OF INTERIOR
Arthur Gary, Senior Attorney

DEPARTMENT OF STATE
Michael Matheson, Acting Legal Advisor
K. E. Malmborg, Attorney/Advisor
Idris M. Diaz

U.S. INFORMATION AGENCY
Gordon John Dickey, Assistant General Counsel

NUCLEAR REGULATORY COMMISSION
Martin Malsch, Deputy General Counsel
Kathryn L. Winsberg, Senior Attorney

FEDERAL ENERGY REGULATORY COMMISSION
Robert C. Fallon, Senior Counsel to the Chair, FERC
David N. Cook, Deputy General Counsel

DEPARTMENT OF AGRICULTURE
Michael W. Kelly, Assistant General Counsel

SECURITIES AND EXCHANGE COMMISSION
Marva Simpson, Attorney/Advisor

BOARD OF GOVERNORS OF THE FEDERAL RESERVE
Stephen L. Siciliano, Special Assistant to the General Counsel for Administrative Law

FEDERAL DEPOSIT INSURANCE CORPORATION

INTERNATIONAL TRADE COMMISSION
Richard Liebeskind, Deputy Assistant Director, Bureau of Competition

COMMODITY FUTURES TRADING COMMISSION
Harold L. Hardman, Assistant General Counsel

U.S. INTERNATIONAL TRADE COMMISSION
Mark Morin

DEPARTMENT OF DEFENSE
Mary De Rosa
Stuart Aly