MAJOR FEDERAL LEGISLATION

A "LEGAL FOUNDATIONS" STUDY

Report 6 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

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.

Part One

Introduction

Some of the most sweeping Federal legislation relevant to efforts to protect the critical infrastructures was originally conceived, passed into law and implemented long before the proliferation of computer and computer networks, and before the emergence of serious threats to the infrastructures. While the long-standing divisions of authority created by such legislation and the mechanisms that flourished thereunder still appear to be fundamentally sound, some of this legislation may now require modernization so that it may continue to serve its originally intended purpose.

Several pieces of legislation that appear relevant to infrastructure assurance objectives were written before the emergence of a recognizable cyber threat. It is not clear whether such authorities would apply, and should apply, to a cyber-related event. Until the dynamics of such a cyber event are better understood, including the necessary response vehicles, sweeping legislative changes would be premature. However, it is nonetheless possible to identify key issues and to make general recommendations to begin the process of incorporating the full range of infrastructure assurance issues within the legislative framework. It is also possible to identify the additional pieces of legislation relevant to achieving infrastructure assurance objectives and consider whether those acts should be amended or revised, or should act as models to guide the implementation of other specific infrastructure assurance objectives.

Research Issues

The questions at hand include:

- Do major areas of Federal legislation, such as the Defense Production Act of 1950, the Stafford Act/Federal Response Plan, the Computer Security Act of 1987, the War Powers Resolution, and Nunn-Lugar-Domenici legislation adequately take into account threats to, and incidents arising from attacks on critical infrastructures?
- Should these laws be modernized to better account for and address physical or cyber threats, and incidents arising from physical or cyber attacks?

- Can modernization of these laws also accomplish other related infrastructure assurance objectives?

- Alternatively, can infrastructure assurance objectives be more effectively implemented through new and different legislative schemes?

Defense Production Act Of 1950

The Defense Production Act serves as an important legal mechanism for security of the Nation's industrial and technological base. Its authorities, including priorities in contracts, financial incentives, and voluntary agreements, may serve as important vehicles to assist in the reconstitution or recovery of a critical infrastructure necessitated by a physical or cyber event. It may prove productive to review the DPA authorities and triggering mechanisms, and current efforts underway at modernization, to ensure that these powers would available and adequate in light of emerging threats, vulnerabilities, and related challenges.

Background

The Defense Production Act of 1950 (DPA)[1] was enacted to ensure that national security and defense interests would be supported by a strong and dependable industrial and technological base. The DPA vests a great many powers in the President during both times of peace and of national emergency to garner support for national defense from private industry. It is a tool for response *and* prevention. Among the provisions of the DPA are priorities for performance of contracts, requirements for stockpiling, availability of loans and a DPA fund, and recognition of the need to plan and train for emergencies. The DPA, as amended, may also be invoked during civil disasters covered by the Stafford Act, whether catastrophic earthquakes or terrorist events.

Uses of the DPA

The most recent uses of the DPA have centered on the use of priority contract performance to provide military operations (e.g. Desert Shield/Storm) needed computer and communications equipment, global positioning systems, chemical warfare protective clothing and equipment, and medical supplies.[2] The DPA contains a specific priority contract provision that relates to

[1] Codified at 50 App. U.S.C. § 2061 *et seq.*

[2] *See* Interagency Working Group on Modernization of the Defense Production Act, *Final Draft Report on Modernization of the DPA* (December 24, 1997).

"domestic energy supplies" which was used to ensure the timely completion of the Trans-Alaska pipeline and to support accelerated development of oil and gas reserves from the Alaska North Slope.[3] Funds available under the DPA have also been used for innovation in defense technology, such as the $7.6 million spent to qualify active matrix liquid crystal displays for use on Apache Longbow helicopters.[4] The focus on research and development has been to provide incentives for private industry to develop technologies specifically needed by the defense community.[5]

The DPA is a powerful law that, if ever needed, could do much to further infrastructure assurance objectives. However, it was written during an era when national defense was more dependent on such things as energy and weaponry produced by the private sector, than the networks and communications that are currently the focus of information warfare concerns. The powers contained in the DPA may be suitable for use in response to infrastructure-related emergencies, but the law, and its triggering mechanisms, should be reviewed to ensure its availability to respond to serious cyber as well as physical incidents.

Application To Cyber-Incidents

Under the DPA, the President is given broad powers to invoke certain measures after making particularized findings. Though the Act is clearly available during times of national emergency, including civil defense emergencies, as declared by the President, most of its provisions are available prior to such an occurrence in order to prevent a national defense or national security-related crisis. Thus for individual provisions of the Act, priorities in contracts or various financial incentives may be available if an item, resource, or specific industry is essential to the national security strategy and is potentially scarce.

A cyber-related situation could satisfy the requirements to invoke many of the provisions of the DPA. For example, a minor disruption in the energy industry could trigger the authority to set priorities in contracts without regard to the cause. For other industries, however, the bar is set much higher. Thus, it may be necessary to review the individual triggering mechanisms as well as the policy statement for the statute as whole to ensure its availability to prevent crises that may arise out of cyber-related events. A statement specifically establishing the nexus between the critical infrastructures, including the information and communications infrastructure, and national security may be sufficient to update the Act for infrastructure assurance generally, as well as for addressing emerging cyber threats and vulnerabilities to infrastructures.

[3] *DOE Offers U.S. Refineries Assistance Under Defense Production Act*, Inside Energy with Federal Lands, Sept. 17, 1990, *available in* DIALOG, File No. 624.

[4] *Pentagon Proposes $50 Million Commercial Insertion Program*, Vol. 15 Defense Week No. 15 (IAC April 8, 1996).

[5] Under an agreement between DOD and OMB, the only DPA financial incentives currently in use are purchases and purchase commitments.

Current Efforts To Amend The DPA

In the 1995 Amendments to the DPA, an inter-agency study group was given one year to prepare a report on the need to modernize the statute. That report is expected to be transmitted to Congress in September, 1997. The modernization effort focuses on addressing new threats in the post Cold War era, enhancing financial incentives for the availability of materials, services and technologies, and revitalizing the DPA fund. The legislative changes suggested may enhance the availability of DPA powers for infrastructure contingencies, but additional modifications may be in order.

Specifically, the Modernization Report is expected to recommend that the Act be broadened to include "acts of terrorism." Depending on how terrorism is defined, it may or may not be broad enough to encompass cyber threats to critical infrastructures. In addition, expanding the Act to be responsive to "acts of terrorism" essentially only addressed those portions of the act concerning incident response — not prevention. Many of the provisions of the DPA that could be identified as potentially useful for use in the protection of the critical infrastructures could be, and perhaps should be, available *prior to* an incident. These preventive-type measures have been used in the energy industry, for example, to facilitate constructing and repairing pipelines.

Additional Considerations Relating To Infrastructure Assurance

It may be advisable to consider additional modifications to the DPA in order to implement infrastructure assurance measures or to serve infrastructure assurance objectives. While additional study may be needed before recommendations regarding the DPA may be put in specific terms and implemented, there are a few areas which seem to merit attention. First, DPA funds may be available for infrastructure assurance-related research and development or expansion of production capacity of critical infrastructures. Second, DPA priorities may be available to assist in reconstituting critical infrastructures (e.g., by expediting delivery of parts). Third, stockpiling provisions could be considered as possible avenues for ensuring the availability of rare and crucial parts for critical infrastructures.[6] Finally, voluntary agreements may provide a planning mechanism for preparing for infrastructure incidents.

The authority to accomplish many of these uses of the DPA for infrastructure assurance objectives is in many instances already in place. Promoting such uses is a matter of education and awareness of both government and industry of the availability of such resources especially in response to new types of incidents. However, the DPA, even in light of current modernization efforts, may not provide such resources to all of the necessary critical infrastructures under all the necessary circumstances. The statute addresses energy resources specifically, but not communications. While other avenues may be available for maintaining telecommunications in the event of emergency, it may be important to give consideration to the need for and applicability of DPA provisions to all of the critical infrastructures to ensure adequate coverage in

[6] Other independent authorities exist for stockpiling which could be pursued for infrastructure assurance objectives. *See* 50 U.S.C. § 98; 44 C.F.R. Part 328.

the event of a major infrastructure disruption. For example, the priorities in contracts authorities may be invoked when necessary for "national defense" for all of the critical infrastructures, but in the energy industry, specific priorities in performance of contracts may be granted when materials, services or facilities are "scarce, critical and essential" to maintain or expand exploration, production, refining or transportation; to conserve energy supplies; or to construct or maintain energy facilities. Thus, the authorities may be available for cyber incidents in the energy industry, but depending on the prevailing definition of "national defense," not for the telecommunications industry or another critical infrastructure.

Actions for Consideration

Maintenance of the Status Quo

One possibility is based on recent Congressional and Administration attention, that the DPA will be appropriately modified to address emerging threats, such as those from cyber attacks. The most recent amendment to the DPA came in 1995 when Congress asked the President to report on the need to modernize the DPA. This report is due September, 1997. In the 1995 amendments, Congress also expanded "national defense" and "defense" to include emergency preparedness functions described in the Stafford Act. As of this writing, the President's report to Congress is currently in draft and while it does not specifically address infrastructure assurance, it does propose to expand the scope of the DPA to include a wider range of national security and national defense issues including globalization. It also proposes increased funding for the DPA fund. In light of these trends toward expanding the DPA, it may be reasonable to conclude that the DPA will be modernized appropriately under current Congressional thinking.

There are pros and cons to this approach. The DPA is a complex piece of legislation with a significant history, and thus, infrastructure assurance objectives may be more easily achieved apart from DPA structure. It may also be prudent to avoid creating threat of government authority encroaching on private industry resources and functions. However, the Administration might not want to ignore the DPA when designing implementation strategy, and it may make more sense to try to work with what is already there since the President's report on DPA modernization may not adequately address threats to critical infrastructures.

Incorporating Critical Infrastructures Specifically Within the Defense Production Act

Though current, and even proposed expansions of policy address national security, national defense, and civil emergencies, there may nonetheless be value in specifically including critical infrastructures in the statement of policy. Many of the provisions of the DPA could be valuable for infrastructure assurance objectives (e.g., DPA funds for research and development, priorities

in contract performance, etc.). However, without specific inclusion of critical infrastructures into the policy of the DPA, such authorities may be presumed unavailable for infrastructure assurance.

The advantages of such an approach would allow critical infrastructure to be included within the DPA's coverage without a series of technical amendments. It would also leave the basic authorities of the DPA intact and unchanged, and technically will only expand the areas to which they may apply. It would also be necessary to ensure that this approach does not become a quick patch which fails to adequately account for lack of coverage for specific critical infrastructures, or that it does not read as overly broad.

In addition there are precedents in priorities in contracts related to energy which can be studied as a potential model for the other critical infrastructures in order to ensure continued operation and clear authority for use in reconstituting such infrastructures after an event. This is because the DPA designates energy as a strategic and critical resource to receive special treatment within the priorities and allocations section of the statute. This treatment allows the priorities in contracts provisions to be used for a wide variety of purposes including supporting energy construction and repair projects. Such uses do not require as stringent requirements in terms of Presidential findings as do other industries and resources covered generically within the DPA due to energy's special status. This provision of the DPA is potentially useful for avoiding serious disruptions of critical infrastructures, regardless of their cause, or reconstituting the infrastructures once an incident has occurred. It may therefore be prescient for future needs for the Administration and Congress to consider: (1) whether the energy provision is an appropriate model for other critical infrastructures; and (2) whether critical infrastructures would benefit from such additional authorities. This will require consultation with Federal and private bodies and research into analogous authorities contained in other bodies of law, for example in the telecommunications industry.

DPA Fund and Financial Incentives

Additionally, there is the use of DPA funds for research and development to support the resiliency and security of critical infrastructures. DPA funds are currently used to support a wide range of activities including development of new technologies to support national defense. At current rates of spending the DPA fund will soon be depleted. In addition, an agreement between the Office of Management and Budget (OMB) and the Department of Defense (DOD) limits the types of financial incentives that DOD can make available to industry including loan guarantees and loans. The draft of the President's report on modernization of the DPA recommends new funding for the DPA.

Additional funding of the DPA may create a pool of resources that can be used to further infrastructure assurance objectives without needing to specifically make the case for spending on infrastructure assurance to Congress. However, there is no guarantee that funds will be allocated for infrastructure assurance objectives even if put toward the DPA fund.

Incorporation of Provisions by Agencies with Existing DPA Authorities

The Department of Energy recently sent a letter to refinery companies it works with to explain the availability of a certain provision of the DPA to expedite delivery of needed parts during an emergency or other contingency.[7] While no one has yet taken DOE up on the offer, the letter did increase awareness both within the agency and the private sector of the availability of certain authorities in times of necessity. It may be possible to further expand the level of awareness of the DPA and its provisions by other agencies with connections to critical infrastructures undertake a study of the DPA and determine which provisions may be used during an infrastructure incident. These agencies and other partners may opt to incorporate the provisions into their planning for infrastructure emergencies.

Such actions would allow an agency-by-agency/infrastructure-by-infrastructure review of the statute, a process which may also identify any needed legislative changes. It would also allow close coordination with the private sector on how the DPA can be used.

The Stafford Act/Federal Response Plan

The Stafford Act and Federal Response Plan set out the parameters of the Federal response to major disasters as declared by the President. The Federal Emergency Management Agency's (FEMA) authority to prevent, mitigate, and respond to incidents affecting the operation of the critical infrastructures may be unclear under the triggering mechanism currently contained in the statute.

Background

The Stafford Act, and the management structure of the Federal Response Plan (FRP) are the primary means by which the Federal government responds to domestic disasters. The purpose of the Stafford Act is to provide assistance to state and local governments to enhance response capabilities. This assistance may take the form of materials and resources, including personnel and expertise, or Federal funds. However, before such assistance to be available, the statute and thus the FRP management structures must be triggered.

[7] *See* Inside Energy, *supra* note 3.

Stafford Act/FRP Triggering Mechanisms

The triggering event for the Stafford Act is a "major disaster." This includes natural catastrophes (e.g., flood, earthquake, tornado) and fire, flood or explosions regardless of cause.[8] Once a major disaster has occurred, the governor of the affected state must implement the state emergency plan before asking the President to declare a "major disaster." The declaration of a disaster allows the powers of the Stafford Act and the response mechanism set out in the FRP to be activated. Among the assistance the Stafford Act provides are agency resources (personnel, equipment, supplies, facilities, technical and advisory services)[9]; technical and advisory assistance for performance of essential community services; issuance of warnings of risks and hazards, public health and safety information, provision of health and safety measures; and management control and reduction of immediate threats to public health and safety[10]; DOD resources for clearance and removal of debris and wreckage and temporary restoration of essential public facilities and services;[11] and emergency telecommunications[12] and public transportation services.[13] Authorities also exist to take post-disaster steps toward mitigation of future damage.[14]

The potential for infrastructure-based emergencies and even cross-infrastructure catastrophes may one day necessitate that the Federal government mobilize for a coordinated response. The Stafford Act and Federal Response Plan already provide a framework for mobilizing such a response. However, it is not clear that the trigger mechanisms, as they are currently defined, would allow FEMA to become involved in prevention, mitigation and recovery actions for cyber-based infrastructure events (or, for example, to proactively pre-position resources when faced with a sufficiently credible threat). FEMA (and the FBI) would clearly be within statutory bounds to respond to a physical attack on a critical infrastructure involving a bomb or other explosive device. In fact, the Terrorism Annex has recently been added to the FRP to address such incidents and those involving Weapons of Mass Destruction. However, if the disruption to the power supply to a large a geographic area were caused by a cyber-based attack, it is not clear that FEMA would have the necessary authority to act. Such an event is neither a "natural catastrophe" nor need it necessarily cause a "fire, flood, or explosion."

Preparation and Mitigation Authorities

The Stafford Act also has many provisions which could be revised, or merely promoted, to enable actions to protect or mitigate against infrastructure damage. Provisions related to insurance requirements, reimbursement of costs by those liable for damage, hazard mitigation measures and minimum rebuilding standards in conjunction with disaster loans could all be

[8] *See* 42 U.S.C. § 5122.
[9] 42 U.S.C. § 5170a(1).
[10] 42 U.S.C. § 5170a(2).
[11] 42 U.S.C. § 5170b.
[12] 42 U.S.C. § 5185.
[13] 42 U.S.C. § 5186.
[14] *See, e.g.*, 42 U.S.C. § 5170c(a) (Federal funds available for 75 percent of costs of future hazard mitigation efforts); 42 U.S.C. § 5176 (minimum standards for public and private structures in conjunction with disaster loans or grants).

leveraged to further infrastructure assurance objectives. Most of the mitigation-related provisions apply to areas affected by major disasters and receiving Federal assistance. The provisions often do not reach private businesses and do not apply at all to areas that have not yet been struck by such a disaster.

FEMA's authorities also extend to planning. Under the Stafford Act, the President does have authority to establish, *"a program of disaster preparedness that utilizes services of all appropriate agencies and includes:*

(1) preparation of disaster preparedness plans for mitigation, warning, emergency operations, rehabilitation, and recovery;
(2) training and exercises;
(3) post-disaster critiques and evaluations;
(4) annual review of programs;
(5) coordination of Federal, State, and local preparedness programs;
(6) application of science and technology;
(7) *research."*[15]

Other Preparation and Mitigation Authorities

One program, outside of the Stafford Act/FRP framework, where substantial emphasis has been placed on mitigation is the National Earthquake Hazards Reduction Assistance Program. [16] This program was established by a separate piece of legislation, the Earthquake Hazards Reduction Act, in 1977.[17] The program may provide a model for the types of cost-sharing, mitigation-oriented programs be appropriate for FEMA to pursue in the area of infrastructure assurance. Under the program, areas that are at risk apply to FEMA for funds, which it must match, for use in planning for and mitigating the damage that results from earthquakes. Such legislation contrasts with implementation of the Stafford Act which has not to date focused on mitigation and preparation activities to the extent necessary to satisfy some infrastructure assurance objectives.

Scope of Authority

An additional area of concern is the availability of Federal assistance to private industry, including infrastructure owners and operators, in the event of a major infrastructure-disrupting event. The Stafford Act does not provide assistance for private industry. Instead, the Act is designed to create a conduit for assistance from the Federal government to state and local agencies. Then, through the state and local agencies, assistance may be available to private concerns. In terms of direct aid, the Stafford Act provides funding and other assistance authority only for public entities and facilities and for private nonprofit facilities (which may include some

[15] 42 U.S.C. § 5131(a).
[16] *See* 44 C.F.R. Part 361 (1997).
[17] 42 U.S.C. § 7701 *et seq* (1997).

utilities, hospitals, and emergency services, but certainly does not include many of the critical infrastructures).[18] A broad reading of certain provisions of the Stafford Act may allow Federal resources to be used to restore essential services to affected communities, which arguably would include electric power or telecommunications. However, the statute's wording indicates a preference for Federal provision of essential services (e.g., telecommunications) until private providers are restored rather than a Federal role in restoring the private service providers.[19] Other statutory mechanisms do provide some assistance to private industry in restoring operations after a disaster or other emergency. The DPA, for example, can be used to speed delivery of items or provide financial assistance (i.e. loans) to assist in recovery.

The Stafford Act/FRP scheme has been an effective mechanism for responding to natural disasters. There may be significant advantages to considering the benefits of expanding this scheme to cover additional type of incidents. A shift in focus toward greater mitigation and preparedness activities may also serve infrastructure assurance objectives. This may include pre-disaster mitigation measures, conduct of training exercises, and greater integration of cyber elements in current planning.

Actions for Consideration

Maintenance of the Status Quo

In light of recent additions to the FRP (e.g. the Terrorism Annex) and growing responsibilities of FEMA for such things as consequence management with respect to Weapons of Mass Destruction attacks, FEMA may undertake to prepare its authorities as necessary to respond to a critical infrastructure-related incident. Congress may also take appropriate steps to ensure preparedness for infrastructure-related incidents either by tasking FEMA or through another analogous piece of legislation.

Conduct an Additional Study

It may be desirable for a specific agency to engage in a full-scale study of the Stafford Act/Federal Response Plan to determine:

- Its likely applicability to critical infrastructure emergencies, particularly those with a cyber dimension;
- Current mitigation efforts and the need for further legislative or administrative action to supplement them;

[18] *See, e.g.*, 42 U.S.C. § 5172 (repair, restoration, and replacement of damaged facilities).
[19] *See* 42 U.S.C. §§ 5185-86.

- Applicability and desirability of Federal assistance for critical infrastructure owners and operators through the Stafford Act/FRP;

- Suitability of the current management structure of the FRP to respond to critical infrastructure emergencies (and whether there should be a specific annex to the FRP to address such incidents or even an analogous response structure based on the FRP).

While such a study would focus primarily on the Stafford Act and FRP, it could also incorporate other disaster preparedness and response statutes, regulations and programs at the Federal and state levels. If so, it would allow for detailed approach and careful consideration of possible effects of each amendment or revision, and also allow experts on emergency preparedness to drive process and tailor provisions to critical infrastructure issues.

Making Minimal Modifications to Key Definitions to Ensure Response To Serious Cyber Incidents

It may be that definitions of "emergency" and "major disaster," as used in the Stafford Act, ought to be revised to specifically include critical infrastructure incidents and cyber attacks. Amending the triggering mechanism for the Stafford Act and Federal Response Plan would ensure that the response mechanism they create will be available if needed to respond to a critical infrastructure crisis. In addition, amending the circumstances which trigger the Stafford Act also allows the DPA to apply to those incidents.

Such a streamlined approach to amending legislation is likely to provide coverage of cyber-incidents without potentially controversial expansion of scope to private sector, and may be more than adequate to cover infrastructure assurance concerns. However, this strategy could be overly simplistic, may create powers in the President and his delegatees that are more broad than is either necessary or prudent, or, may neglect to create specific requirements, uses of programs or funds, and authority that are necessary for infrastructure assurance objectives. It may also stretch the FRP in directions which it was never intended to go.

Enacting Substantive Amendments

There may be a need for more comprehensive amendments to the Stafford Act to address specific cyber-related issues, including definitional clarifications (see above) and others. These may include revisions to the triggering mechanism, mitigation programs, and funding requirements. Significant study would need to be given before going forward with a specific recommendation for amendment.

New Legislation

New legislation to specifically address similar issues as Stafford Act for the cyber arena may be appropriate. It could include a management structure for responding to emergencies analogous to the FRP.

Information Security In The Federal Government: The Computer Security Act Of 1987 & OMB Circular No. A-130

Background

The primary legal instruments providing for government information security are the Computer Security Act of 1987 (CSA) and OMB Circular A-130 (A-130). The CSA tasks the National Institute of Standards and Technology (NIST) with developing information security standards for the Federal government and A-130 sets out Federal agency requirements for adhering to the NIST standards. While this seems to be a fairly simple paradigm, a number of factors have prevented it from being implemented with maximum success.

NIST Responsibilities Under The CSA

The CSA defines NIST's mission as "developing standards, guidelines, and associated methods and techniques for computer systems."[20] These standards are to be uniform for unclassified systems within the Federal Government.[21] The primary purpose of these standards and guidelines is to protect the integrity and privacy of the information in such systems and to prevent fraud and misuse.[22] The Act requires that NIST submit their recommendations of standards to the Secretary of Commerce for review and promulgation.[23] NIST's other responsibilities under the Act include: setting guidelines for training employees in security awareness and procedures, and developing validation procedures for, and evaluating the effectiveness of, the standards and guidelines they develop. This validation process is to be coordinated with other government and private agencies.[24]

[20] 15 U.S.C. § 278g-3(a)(1) (1997).
[21] 15 U.S.C. § 278g-3(a)(2).
[22] Id.
[23] 15 U.S.C. § 278g-3(a)(4).
[24] 15 U.S.C. § 278g-3(a)(6).

To accomplish the mission and responsibilities of the Computer Security Act, NIST is given the authority to engage in research and studies to determine vulnerabilities and to design security measures for Federal systems; to coordinate with other Federal agencies including, but not limited to, DOD, DOE, NSA, GAO, OTA, and OMB; to work with the Office of Personnel Management (OPM) in developing training regulations for computer security; and to provide technical assistance to Federal agencies for implementation of NIST standards and guidelines.[25] The Act also authorized NIST to "assist the private sector, upon request, in using and applying the results of the programs and activities" developed under the Act.[26]

New NIST/NSA Partnership

Recently, NIST and NSA have teamed up to address information security issues. The primary focus on their effort will on creating testing standards for information systems. Through this partnership, they will then train and certify private sector testers.

Many of the difficulties that appear to arise from the Computer Security Act do not spring directly from a change in technology, but rather from the framework for creating standards and guidelines for security of Federal government systems set out in the CSA and as it has been implemented. One of the primary and most persistent problems has been the lack of funding for NIST to carry out its responsibilities under the Computer Security Act.[27] A new authorization bill, sponsored by Representative Connie Morella (R-MD), should go to the floor of the House of Representatives in September that would increase funding for Computer Security, NIST and the Federal Aviation Administration (FAA) by $14 million. Funding for computer security in the era of the balanced budget has also been a problem for individual agencies. While it has been suggested that information system security be made a budget line item, others have noted that this is usually one of the first areas cut in an agency budget crunch.

OMB and Circular A-130

OMB's role in implementing and enforcing NIST standards and guidelines may also require examination. Circular A-130 sets forth an ambitious agenda. But the Report of the Commission on Protecting and Reducing Government Secrecy states that OMB has put inadequate resources and attention toward computer security.[28] Specifically, the Report states that OMB has only two people assigned to oversee the Federal government's information systems.[29] As it currently stands, there is no oversight of research and development to reduce redundancies in efforts within the Federal government. Even Congressional oversight of computer security issues is dispersed across the jurisdiction of several committees and subcommittees, including House and Senate

[25] 15 U.S.C. § 278g-3(b)(2)-(6).
[26] 15 U.S.C. § 278g-3(b)(1).
[27] See Gov't Secrecy 104; Computers at Risk 197.
[28] Gov't Secrecy 102.
[29] Id. at 107.

Committees on Appropriations, Commerce, Government Reform and Oversight, National Security, and Science, to name just a few.[30]

While OMB may need to put more resources toward overseeing the implementation of A-130, the current division of responsibility in A-130 need not be altered. A-130 is specifically designed to put responsibility for information security with the individual agency Chief Information Officers (CIOs). Legislation such as the Information Technology Management Reform Act (ITMRA) requires CIOs to establish performance measures for information technology systems and report on them as part of the OMB budget review. Similarly, the enforcement mechanism for A-130, as recently revised upon the suggestion of the National Performance Review, requires the reporting of "material weaknesses" in information security also through a budgetary review process (*see* Federal Managers Financial Integrity Act). The strength of this enforcement mechanism is dependent on the weakness being found and reported. Without a mandated audit or additional oversight procedure, this is unlikely to occur.

Additional oversight, under the auspices of OMB, but with greater technological capability and resources, may be a welcome addition to the current framework. Such an entity could have operation responsibility for studying and leading the reform of information security for the government. This would require extensive consultation with the private sector as well as links to the technological resources of NIST and NSA. Ultimately, the process would involve audits of information security systems at each of the individual agencies. Such an oversight body would require substantial study before launching and may require revisions to core Federal information security authorities (such as the CSA, A-130, ITMRA).

Despite volumes of literature criticizing the CSA, its purpose and intent remain fundamentally sound. The Federal government does need minimum information security standards for its unclassified systems. Likewise, the mechanism for enforcing adherence to those standards as set out in A-130 may also become adequate with time and increased attention and awareness. However, in order for the government to have a truly successful information security program these two primary elements must be fully realized. This may require additional resources and concrete direction to agencies already bearing the responsibility, and additional commitments from individual agencies to give information security the attention it deserves.

Actions for Consideration

Maintenance of the Status Quo

Efforts by Representative Morella and others to re-authorize NIST and provide adequate funding may result in satisfactory improvements to the existing legislative scheme.

[30] Id. at 103.

Need for Task Force to Study of Methods for Enhancing Compliance with Standards and Requirements for Information Security in OMB Circular A-130

As the Federal government moves toward management methods more closely resembling those used in the private sector, it may be appropriate to begin to explore the use of internal auditors for such areas as information security. An auditing scheme would fit squarely within the enforcement framework as currently designed and would not require any major modifications to existing legal authorities. However, those studying the issue would likely consider the need for additional legislation or revision of key authorities such as A-130 as part of their study. The study may also consider whether the Inspector General offices within agencies would be an appropriate place to house such a function and what would be necessary to make the expertise needed to perform Information Technology (IT) audits available to IG offices. The utility of such a study would be dependent on the development of a set of standards against which agencies could be audited.

Joint NIST-NSA Partnership Study and Report on an Effective Enforcement Vehicle for Computer Security Within the Federal Government

Rather than creating a task force to study the need for greater enforcement of computer security standards within the Federal government, this approach would utilize the existing partnership and expertise of NIST and NSA. The scope of the study would be essentially the same as in the previous suggested action, but would allow for greater coordination with the standards development process.

Existing resources can be used to undertake the study, which allows considerable knowledge and expertise in computer security issues to look at a difficult problem. However, computer security expertise may not translate into expertise in management of the Federal government. The study group must be sufficiently diverse enough o encourage new thinking in the area.

The War Powers Resolution

'When natural resources were the dominant factor of production, the conquest and control of territory seemed a reliable way to enhance national power. Today, conquest of territory is rarely worth the cost to the nation.' It is both much easier and more profitable to conduct information warfare

against an adversary's knowledge resources than to conduct a conventional war against its armed forces. [31]

Background

The War Powers Resolution is one part of the legal and policy structure that enables the Federal government to defend the nation. The Resolution was written before the emergence of information warfare and cyber threats. As these threats evolve, the mechanisms that enable defense of our nation will need to be reviewed and updated to ensure they enable an adequate and effective response, and instill adequate deterrence where appropriate.

While information warfare is still emerging as a threat to national security, resources and attention are being devoted by the Department of Defense and others charged with protecting the nation. Thus far, the resources have been devoted largely to estimating the threat and developing our own capabilities. The focus has not yet come to rest on the rather important question of how information-based warfare fits within our current structure-- legal, policy, and even practical-- for detecting and responding to attacks on the nation.

The current legal structure for responding to an "attack" has domestic and international components. As a fundamental matter, one must first determine what is an "attack" or act of war. Does it include mechanisms driven by a computer? If a bomb disables a major defense computer station or an important telephone switch, that is clearly an attack. Is it likewise an attack if accomplished with a computer? And what has to be accomplished to be an attack? Electrons crossing a national border is not enough under current law or practice to constitute a violation of a nation's sovereignty.

Depending on the result of an incident, how, considering the anonymity and ready availability at low cost associated with computer technology, can the victim country distinguish between an accident and an attack? There may also be challenges associated with convincing allies to join in retaliatory efforts based on the available evidence. Defining the terms that drive domestic and international warfare policies, such as "attack," "act of war," or "force," will undoubtedly provide an important first step in clarifying the application of such laws, rules and customs to computer-based acts of aggression. However, additional, important questions remain. For example, international law requires that the force of a retaliatory attack be proportionate to that of the aggressor's attack. If a country is subject to an information warfare attack, would it be appropriate for them to use conventional military forces to retaliate? If the country retaliates through electronic means, may it pass through the systems of a neutral country? [32]

---

[31] Sean P. Kanuck, *Information Warfare: New Challenges for Public International Law*, 37 Harv. Int'l L.J. 272, 290 (1996) (quoting Albert J. Edmonds, Address at Seminar on Intelligence, Command, and Control, John F. Kennedy School of Government, Harvard University (Apr. 20, 1995)).

[32] Many of these questions are raised in Greenberg, Goodman & Soo Hoo, *Old Law for a New World: The Applicability of International Law to Information Warfare*, ISAC, Stanford University (February 1997).

As important as each of these questions are to understanding the dynamics of the problem and creating an international consensus on how to approach information-based attacks, an even more fundamental question exists: Are there benefits from this current state of confusion that outweigh the possible benefits of coming to consensus on this issue?

Under the current regimes, it would be difficult to show that any country, whether as an aggressor or in retaliation, acted inappropriately. This can benefit intelligence gathering, defensive maneuvering, and expansion of offensive capabilities. Clearly, when considering how the War Powers Resolution fits into the larger picture and the options that exist for changing the domestic and the international regime of which it is a part, such questions need to be serious considered. The options themselves demonstrate the complexity of the issue. Definitions are an appropriate beginning option, but would have to carefully crafted so as not to be excessively inclusive of seemingly benign applications of information technology. Early warning systems and limiting the information portion of weaponry could also achieve a deterrent effect. However, one of the most unlikely, but perhaps effective forms of deterrence may be the growing transnational complexity and transparency of systems, so that an attacker may not be able to harm the systems of one nation or target without potentially harming his own.[33]

"Infowar" Attacks Under The War Powers Resolution

One part of this structure is indicative of the problem that would confront the nation in the event of an "infowar" attack. The War Powers Resolution, written in the post-Vietnam era, does not contemplate an information-based attack within its parameters. The statute, which sets out the authorities and responsibilities of the President with respect to introducing U.S. troops into hostilities, was written well before the advent of the computer-based threat. Its language clearly anticipates warfare as a physical attack.

In the event of a cyber attack, quick and decisive action may be necessary to launch an effective response. The speed of the nation's response may be significantly slowed if a Congressional declaration of war or a statute authorizing the introduction of forces into hostilities is required. The President is, however, only authorized to introduce forces into hostilities without Congressional approval in the limited circumstances of a national emergency created by an attack upon the U.S.[34] Whether the definitions of "hostilities" and "attack on the U.S." are broad enough to include a cyber attack is unclear.

A similar problem exists with respect to international law. Article 51 of the U.N. Charter uses "armed attack" as the basis for determining whether an armed response is appropriate. The U.N. has not yet addressed how Information Warfare would be treated under its law of use of force. Recommendations in the area include: specifically defining "armed attack" to either include or exclude information warfare; coordinating and harmonizing computer crime laws and

[33] For further discussion of these and other options for deterring information warfare, *see* Timothy Thomas, *Deterring Information Warfare: A New Strategic Challenge*, Parameters 81 (Winter 1996-1997).
[34] *See* 50 U.S.C. § 1541 (1997).

prosecutions on an international scale; and developing a network of agreements, similar to those used for aviation, to protect critical systems on an international level.[35]

The question is, then, does the War Powers Resolution or its international analogues apply to an information-based attack or does the response structure fall outside of its bounds? Should there be a separate response structure for such "infowar" attacks? While the President's ability to act outside the War Powers Resolution has been well documented,[36] a cohesive policy of deterrence and plan for defense to information-based attacks should clarify the manner in which cyber attack fits into the War Powers Resolution. This undertaking is likely broader than amending only the War Powers Resolution. It may require creating a structure capable of answering the question as to whether the U.S. is under cyber attack; setting out jurisdictional boundaries; assigning roles and missions; and perhaps most importantly, translating the national strategy into a comprehensive statement of deterrence. However, to jump-start such a process, it may be possible to draw attention to the need for a new paradigm by highlighting the inadequacies of the War Powers Resolution in the face of these new cyber threats.

The technology necessary to answer many of these policy questions may not yet be available. As these technologies and the analytic capability necessary to support them develop, many important groups will likely begin to address these concerns. It will be important for these groups, in the process of developing a national policy of deterrence, to give substantial thought and consideration to the legal regime that is currently in place and the potential impact of such a regime on national policy.

Actions for Consideration

Maintenance of the Status Quo

This resolution has historically reflected tension between the Executive and Legislative branches of government, and may not be a good lead vehicle for addressing a complex new issue such as infrastructure assurance.

Development of an "Infowar" Strategy

The President may direct the National Security Council and Department of Defense develop a comprehensive strategy for responding to cyber attack, taking into account effects of the War Powers Resolution and international law. Such a strategy could clearly outline under what circumstances a cyber incident would be considered an act of war, thus acting as a bridge to

[35] *See* Greenberg, Goodman, et. al, *supra* note 32.
[36] *See, e.g.*, Hansen & Banks, *From Vietnam to Desert Shield: The Commander in Chief's Spending Power*, 81 Iowa L. Rev. 79 (1995).

existing authorities. The strategy may also provide an opportunity to clearly enunciate a policy of deterrence for information-based attacks on the U.S. and its critical infrastructures.

Articulating what will be considered an "attack" may alleviate some confusions regarding Federal jurisdiction for cyber incidents and provide an opportunity to make a clear statement to U.S. enemies regarding U.S. intentions in event of an information-based attack. Such a definition would also serve to clarify responsibilities under the War Powers Resolution and International law.

On the other hand, it may be difficult and potentially undesirable for the U.S. to establish clear definitions, for purposes of deterrence and clarity of international obligations, of concepts that might in turn restrict U.S. activities or available options. There may be significant strategic benefits to operating in "murky waters" until a greater degree of international consensus develops.

Amendment of Key Definitions

Congress may wish to add a definitions section to the War Powers Resolution that specifically includes cyber attack and cyber responses within the framework set out by the Act. This enhancement would ensure that cyber attack is covered by the framework for responding to attacks on U.S., and would also serve as a de facto deterrence policy indicating U.S. readiness to consider certain serious cyber attacks as potential acts of war. However, for the reasons mentioned earlier, the controversial history of the Act may preclude quick action.

Nunn-Lugar-Domenici Legislation

The Nunn-Lugar-Domenici legislation creates a partnership involving many Federal agencies and state and local governments in an effort to increase the capability to respond to weapon of mass destruction incidents across the United States. This legislation focuses on providing training, access to equipment, and information to local first responders. While these programs are in their initial phases, already state and local police, fire, and medical officials are requesting an expanded effort in this area. Infrastructure assurance concerns may require more resources for training and equipment and may also demand that the effort be expanded in scope to address infrastructure-threatening events.

Background

The Nunn-Lugar-Domenici legislation included in the Department of Defense Authorization for 1997 sets out a comprehensive plan for dealing with terrorist threats from "Weapons of Mass Destruction." The legislation defines a Weapon of Mass Destruction (WMD) as, "any weapon or device that is intended, or has the capability, to cause death or serious bodily injury to a significant number of people through the release, dissemination, or impact of…toxic or poisonous chemicals…, a disease organism; or radiation or radioactivity."[37] The legislation is specifically designed to "enhance the capability of Federal, state, and local emergency response agencies to prevent and respond to domestic terrorist incidents involving weapons of mass destruction."[38]

The DOD role in assisting emergency response to WMD events has focused on providing assessments to major cities and conducting training for local first responders. In addition, DOD was tasked with developing a rapid response team and is creating a hotline and help line to provide technical advice during emergencies. A web site will provide information on WMD issues on a routine basis. To accomplish these goals, DOD is working with FEMA, DOE, HHS, EPA and the Department of Justice.

In the *President's Report on Government Capabilities to Respond to Terrorist Incidents Involving Weapons of Mass Destruction*, dated February 26, 1997, additional needs are highlighted. The report generally identifies the initiatives undertaken by the FBI, DOD and FEMA, including the training and support function of DOD in relation to state and local governments. Among the identified needs to continued progress in the fight against WMD, the President's report identifies: continued funding with State and local contributions, expanded training programs and updated materials, specialized equipment and protective gear for the FBI, annual updating of the Rapid Response Information System, additional exercises and legislation.

Such expanded efforts may be consistent and necessary to further objectives for infrastructure assurance as they relate to Chemical or Biological weapons. In addition, depending on the success of the Nunn-Lugar-Domenici legislation, it may be an appropriate vehicle for objectives not currently included within its scope or an appropriate model for a separate initiative.

Actions for Consideration

Maintenance of the Status Quo

[37] P.L. 104-724, § 1403 (1996).
[38] DOD Background Briefing-Part I, 1997 WL 10369097 (May 16, 1997).

It may be preferable for Congress to make no changes regarding the scope or coverage of Nunn-Lugar-Domenici to infrastructure events, continue to support the program initiated by the original legislation and expand its coverage as necessary. It may also be deemed that other avenues would be more appropriate for achieving desired infrastructure assurance objectives.

Nunn-Lugar-Domenici is Expanded to Include Attacks on Critical Infrastructures

On the other hand through a simple legislative revision, coverage could be extended to critical infrastructures. Considerable thought and planning would be required to implement the Nunn-Lugar-Domenici program for infrastructure assurance efforts (e.g., deciding what sort of training, equipment and other resources to provide), which may require further study by either Congress or the Administration.

Nunn-Lugar-Domenici is Studied as a Potential Model for Infrastructure Assurance Legislation

Nunn-Lugar-Domenici legislation may be highlighted as an embodiment of useful principles, including partnership, the Federal government enabling State and local responders, and information sharing. It appears to accomplish many of the goals which would benefit infrastructure assurance, including training and education, information sharing, enhanced cooperation, sharing of resources, and funding.

A study group from the Administration or Congress perhaps should study the Nunn-Lugar-Domenici legislation as a model for an infrastructure assurance statute and determine:

- Whether the legislation is suitable to use as a model;
- Which infrastructure assurance objectives could be achieved through such legislation;
- What sort of revisions would be necessary;
- What additional programs would need to be designed and who should be responsible
- What level of funding would be necessary.

The group could then draft legislation for Congressional consideration.

Part Two

Conclusions

Several pieces of legislation appear relevant to infrastructure assurance objectives, but were written before the emergence of a cognizable cyber threat. It is not clear whether such authorities would apply, and should apply, to a cyber-related event. Until the dynamics of such a cyber event are better understood, including the necessary response vehicles, sweeping legislative changes would be premature. Nevertheless, it is possible to identify key issues and to make general recommendations to begin the process of incorporating the full range of infrastructure assurance issues within a legislative framework. It is also possible to identify additional pieces of legislation relevant to achieving infrastructure assurance objectives, and to consider whether those acts should be amended or revised, or even act as models to guide the implementation of infrastructure assurance objectives.

Defense Production Act

The Defense Production Act serves as an important legal mechanism for security of the Nation's industrial and technological base. Its authorities, including priorities in contracts, financial incentives, and voluntary agreements, may serve as important vehicles to assist in the reconstitution or recovery of a critical infrastructure necessitated by a physical or cyber event. Accordingly, it may prove productive for:

- The Administration and Congress to consider amending the DPA Declaration of Policy to include a finding that critical infrastructures are essential to national security;
- Lead Agencies associated with the critical infrastructures to study the energy provision for priorities in contracts as a potential model for other critical infrastructures in order to ensure continued operation and clear authority for use in reconstituting such infrastructures after an event;
- Congress to support funding for the DPA Fund and financial incentives and to consider making such funds available for research and development related to the critical infrastructures; and

- The Administration to direct Federal agencies with authorities pertaining to the critical infrastructures to review the DPA's authorities and work with industry to make available such authorities when needed to respond to a critical infrastructure incident.

Stafford Act/Federal Response Plan

The Stafford Act and Federal Response Plan set out the parameters of the federal response to major disasters as declared by the President. The Federal Emergency Management Agency's authority to prevent, mitigate, and respond to incidents affecting the operation of the critical infrastructures is unclear under the triggering mechanism currently contained in the statute.

A study should be undertaken of the Stafford Act and Federal Response Plan mechanisms to determine their applicability and suitability to cyber-induced disasters as well as their current implementation with regard to prevention and mitigation. Such a study would also take into account other disaster recovery authorities and their potential impacts on infrastructure assurance goals as well as the desirability of direct assistance to infrastructure owners and operators.

War Powers Resolution

The War Powers Resolution is one part of the legal and policy structure that enables the federal government to defend the nation. The Resolution was written before the emergence of information warfare and cyber threats. As these threats evolve, the mechanisms that enable defense of our nation will need to be reviewed and updated to ensure they enable an adequate and effective response, and instill adequate deterrence where appropriate.

Meanwhile, the Administration, including the National Security Council, Department of Defense, Department of State, Department of Justice, and other interested agencies, could ensure that the U.S. strategy for responding to an information warfare attack addresses the potential legal issues associated with current definitions of "attack" contained in important domestic and international legislation, including, but not limited to, the War Powers Resolution.

Nunn-Lugar-Domenici Legislation

The Nunn-Lugar-Domenici legislation created a partnership involving many Federal agencies and state and local governments in an effort to increase the capability to respond to weapon of mass destruction incidents across the United States. This legislation focused on providing training, access to equipment, and information to local first responders. While these programs are in their initial phases, already state and local police, fire, and medical officials are requesting an expanded effort in this area. There may be more resources required for training and equipment and demand may also build that the effort be expanded in scope to address other infrastructure-related events.

Congress could consider whether the current Nunn-Lugar-Domenici program should be expanded to incorporate other critical infrastructure issues, including physical attacks on infrastructures by means other than Weapons of Mass Destruction, as well as the need for training, awareness, and information sharing efforts directed at state and local responders on the potential impact of disruptions of critical infrastructures, particularly information and communications, on emergency response efforts.