Case Number: 2006-0191-F

FOIA MARKER

This is not a textual record. This is used as an administrative marker by the Clinton Presidential Library Staff.

Folder Title: Transnational Threats (formerly Global Affairs) Chron Files, February 1998 [13]
Staff Office-Individual: TNT-Clarke
Original OA/ID Number: 1381

Row:	Section:	Shelf:	Position:	Stack:
49	3	7	2	V

Withdrawal/Redaction Sheet
Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
001a. memo	William Wechsler to James Steinberg; re: Deputies Committee Meeting on PDDs on Counter-Terrorism & Critical Infrastructure Protection (6 pages)	02/02/1998	P1/b(1), P5
001b. paper	re: Discussion Paper for NSC Deputies Committee Meeting on Unconventional Threats to U.S. (9 pages)	01/24/1998	P1/b(1)
001c. memo	For VPOTUS et al; re: Protection Against Unconventional Threats to the Homeland & Americans Overseas (12 pages)	circa, 02/1998	P1/b(1)
002a. memo	Richard A. Clarke to Jacob J. Lew; re: PDDs (2 pages)	02/23/1998	P1/b(1), P5
002b. memo	Richard A. Clarke to Jacob J. Lew; re: OMB Concerns with PDDs (1 page) [Released on Appeal]	02/09/1998	P5
002c. memo	Michael Deich to Dick Clarke; re: OMB Concerns with PDDs (1 page) [Released on Appeal]	02/12/1998	P5
002d. memo	POTUS to VPOTUS et al; Excerpt fromPresidential Decision Directive (2 pages)	circa, 02/1998	P1/b(1)
003. memo	Steve Simon & Carolyn Dollar to Officer-in-Charge; re: Request for Appointments (partial) (1 page)	02/02/1998	P6/b(6)

COLLECTION:
Clinton Presidential Records
National Security Council
Richard A. Clarke (Transnational Threats (TNT))
OA/Box Number: 1381

FOLDER TITLE:
February Chron - 1998 [13]

2006-0191-F
jp280

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.
PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).
RR. Document will be reviewed upon request.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

~~SECRET~~
NSC/RMO PROFILE

RECORD ID: 9820092
RECEIVED: 02 FEB 98 16

TO: STEINBERG

FROM: WECHSLER
CLARKE

DOC DATE: 02 FEB 98
SOURCE REF:

KEYWORDS: INFRASTRUCTURE
COUNTERTERRORISM

PDD
DC

PERSONS:

SUBJECT: BACKGROUND PAPER FOR FEB DC MTG ON COUNTERTERRORISM & INFRASTRUCTURE PROTECTION

ACTION: NOTED BY STEINBERG DUE DATE: 05 FEB 98 STATUS: C

STAFF OFFICER: WECHSLER LOGREF: 9820047 9820068

FILES: IFM NSCP: CODES:

D O C U M E N T D I S T R I B U T I O N

FOR ACTION	FOR CONCURRENCE	FOR INFO
		BARTLETT
		CLARKE
		NSC CHRON
		WECHSLER

COMMENTS: _____

DISPATCHED BY _____ DATE _____ BY HAND W/ATTCH

OPENED BY: NSSWD CLOSED BY: NSTMH DOC 1 OF 1

~~SECRET~~

ACTION DATA SUMMARY REPORT

DOC	ACTION OFFICER	CAO	ASSIGNED	ACTION REQUIRED
001	STEINBERG	Z	98020218	FOR INFORMATION
001		X	98031011	NOTED BY STEINBERG

National Security Council
The White House

PROOFED BY: _____ LOG # 20092

URGENT NOT PROOFED: _____ SYSTEM PRS (NSC) INT ARS

BYPASSED WW DESK: _____ DOCLOG _____ A/O _____

	SEQUENCE TO	INITIAL/DATE	DISPOSITION
Cosgriff			
Rice			
Davies	1	6 2/2	
Kerrick			
Steinberg	2	Deputy Natl Sec Advisor has seen	
Berger			
Situation Room			
West Wing Desk	3	TMA 3:10	N
Records Mgt.			

A = Action I = Information D = Dispatch R = Retain N = No Further Action

cc:

COMMENTS: DC on PDD-39

EB 2 7:17

xec Sec Office has diskette yes

Withdrawal/Redaction Marker
Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
001a. memo	William Wechsler to James Steinberg; re: Deputies Committee Meeting on PDDs on Counter-Terrorism & Critical Infrastructure Protection (6 pages)	02/02/1998	P1/b(1), P5

COLLECTION:
Clinton Presidential Records
National Security Council
Richard A. Clarke (Transnational Threats (TNT))
OA/Box Number: 1381

FOLDER TITLE:
February Chron - 1998 [13]

2006-0191-F
jp280

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advise between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.
PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).
RR. Document will be reviewed upon request.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

NSC DEPUTIES COMMITTEE MEETING ON UNCONVENTIONAL THREATS AGAINST THE U.S. (PDD-XX, PDD-YY)

DATE: Wednesday, February 4, 1998
LOCATION: 208 - OEOB
TIME: 11:00 a.m.- 12:30 p.m.

AGENDA

I. Introduction . . . . . NSC

II. Discussion Paper. . . . . ALL

III. Other Issues . . . . . .ALL

IV. Next Steps . . . . . .ALL

~~SECRET~~
Classified by: Glyn Davies
Reason: 1.5(b)
Declassify on: 01-28-08

Withdrawal/Redaction Marker
Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
001b. paper	re: Discussion Paper for NSC Deputies Committee Meeting on Unconventional Threats to U.S. (9 pages)	01/24/1998	P1/b(1)

COLLECTION:
Clinton Presidential Records
National Security Council
Richard A. Clarke (Transnational Threats (TNT))
OA/Box Number: 1381

FOLDER TITLE:
February Chron - 1998 [13]

2006-0191-F
jp280

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advise between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.
PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).
RR. Document will be reviewed upon request.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

Withdrawal/Redaction Marker
Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
001c. memo	For VPOTUS et al; re: Protection Against Unconventional Threats to the Homeland & Americans Overseas (12 pages)	circa, 02/1998	P1/b(1)

COLLECTION:
Clinton Presidential Records
National Security Council
Richard A. Clarke (Transnational Threats (TNT))
OA/Box Number: 1381

FOLDER TITLE:
February Chron - 1998 [13]

2006-0191-F
jp280

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advise between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.
PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).
RR. Document will be reviewed upon request.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

PRESIDENTIAL DECISION DIRECTIVE/NSC-YY

TO: The Vice President
The Secretary of State
The Secretary of the Treasury
The Secretary of Defense
The Attorney General
The Secretary of Commerce
The Secretary of Health and Human Services
The Secretary of Transportation
The Secretary of Energy
The Administrator, Environmental Protection Agency
The Director, Office of Management and Budget
The Representative of the United States to the United Nations
The Director of Central Intelligence
The Chairman, Joint Chiefs of Staff
The Administrator, Agency for International Development
The Direction, Federal Bureau of Investigations
The Director, Federal Emergency Management Agency
The Director, National Security Agency
The Assistant to the President for National Security Affairs
The Assistant to the President for Science and Technology Policy

SUBJECT: Critical Infrastructure Protection (U)

I. A Growing Potential Vulnerability (U)

The United States possesses both the world's strongest military and its largest national economy. Those two aspects of our power are mutually reinforcing and dependent. They are also increasingly reliant upon certain critical infrastructures and upon cyber-based information systems. (U)

Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include but are not limited to telecommunications, energy, banking and finance, transportation, water systems, and emergency services, both governmental and private. As a result of advances in information technology and the necessity of improved efficiency, these infrastructures have become increasingly automated and interlinked. These same advances, however, have created new vulnerabilities to both physical and cyber attacks. (U)

Because of our military superiority, future enemies, be they nations, groups or individuals, may seek to harm us in non-traditional ways including attacks within the United States. Because our economy is increasingly reliant upon interdependent and cyber-supported infrastructures, non-traditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy. (U)

II. President's Intent (U)

It has long been the policy of the United States to assure the continuity and viability of critical infrastructures. I intend that the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems. (U)

III. A National Goal (U)

No later than the year 2000, the United States shall have achieved an initial operating capability, and no later than five years from today the United States shall have achieved and shall maintain the ability to protect our nation's critical infrastructures from intentional acts that would significantly diminish the abilities of:

- o the United States Government to perform essential national security missions and to ensure the general public health and safety;

- o state and local governments to maintain order and to deliver minimum essential public services;

- o the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial, and transportation services. (U)

Any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States. (U)

IV. A Public-Private Partnership to Reduce Vulnerability (U)

Since the targets of attacks on our critical infrastructure would likely include both facilities in the economy and those in the government, the elimination of our potential vulnerability requires a closely coordinated effort of both the government and the private sector. The government is not the unique source of wisdom on either the vulnerabilities or their remedies. To succeed, this partnership must be genuine, mutual, and cooperative. In seeking to meet our national goal to eliminate the vulnerabilities of our critical infrastructure, therefore, we should to the extent feasible seek to avoid outcomes that increase government regulation or expand unfunded government mandates to the private sector. (U)

For each of the major sectors of our economy that are vulnerable to infrastructure attack, the U.S. Government will appoint from a designated Lead Agency a senior officer of that agency as the Sector Liaison Official to work with the private sector. Sector Liaison Officials, after discussions and coordination with with private sector entities of their infrastructure sector, will identify a private sector counterpart (Sector Coordinator) to represent their sector. (U)

Together these two individuals and the departments and corporations they represent shall contribute to a sectoral National Infrastructure Assurance Plan by:

- o assessing the vulnerabilities of the sector to cyber or physical attacks;

- o recommending a plan to eliminate significant vulnerabilities;

- o proposing a system for identifying and preventing attempted major attacks;

- o developing a plan for alerting, containing, and rebuffing an attack in progress and then rapidly reconstituting minimum essential capabilities in the aftermath of an attack. (U)

During the preparation of the sectoral plans, the National Coordinator (see section VI), in conjunction with the Lead Agency Sector Liaison Officials, shall ensure their overall coordination and the integration of the various sectoral plans, with a particular focus on interdependencies. (U)

V. Guidelines (U)

In addressing this potential vulnerability and the means of eliminating it, I want those involved to be mindful of the following general principles and concerns. (U)

- o The protection of our critical infrastructures is necessarily a shared responsibility and partnership between owners, operators, and the government. Furthermore, the U.S. government shall encourage international cooperation to help manage this increasingly global problem. (U)

- o As technology and the nature of the threats to our critical infrastructures will continue to change rapidly, so must our protective measures and responses be robustly adaptive. (U)

- o Frequent assessments shall be made of our critical infrastructures' existing reliability, vulnerability and threat environment. (U)

- o To the maximum extent possible, market incentives shall be brought to bear in our efforts to protect our critical infrastructures. These incentives, along with other actions, shall be designed to help private sector owners and operators to achieve and maintain the maximum feasible security. (U)

- o Care must be taken to respect privacy rights. Consumers and operators must have confidence that information will be handled accurately, confidentially, and reliably. (U)

- o The U.S. government shall, through its research, development and procurement, encourage the introduction of increasingly capable methods of infrastructure protection. (U)

- o The U.S. government shall serve as a model to the private sector on how infrastructure assurance is best achieved, and shall to the extent feasible distribute the results of its endeavors. (U)

- o The full resources of the government, including law enforcement, regulation, foreign intelligence and defense preparedness shall be available to ensure that critical infrastructure protection is achieved and maintained. (U)

VI. Structure and Organization (U)

The United States Government will be organized for the purposes of this endeavor around four components (elaborated in Annex A). (U)

1. Lead Agencies for Sector Liaison: For each infrastructure sector that could be a target for significant cyber or physical attacks, there will be a single U.S. government department which will serve as the lead agency for liaison. Each Lead Agency will designate one individual of Assistant Secretary rank or higher to be the Sector Liaison Official for that area and to cooperate with the private sector representatives (Sector Coordinators) in addressing problems related to critical infrastructure protection and, in particular, in recommending components of the National Infrastructure Assurance Plan. Together, the Lead Agency and the private sector counterparts will develop and implement a Vulnerability Awareness and Education Program for their sector. (U)

2. Lead Agencies for Special Functions: There are, in addition, certain functions related to critical infrastructure protection that must be chiefly performed by the U.S. Government (national defense, foreign affairs, intelligence, law enforcement). For each of those special functions, there shall be a Lead Agency which will be responsible for coordinating all of the activities of the U.S. Government in that area. Each lead agency will appoint a senior officer of Assistant Secretary rank or higher to serve as the Functional Coordinator for that function for the Federal Government. (U)

3. Interagency Coordination: The Sector Liaison Officials and Functional Coordinators of the Lead Agencies, as well as representatives from other relevant departments and agencies will meet to coordinate the implementation of this directive under the auspices of a Critical Infrastructure Coordinating Group (CICG), chaired by the National Coordinator for Security, Critical Infrastructure and Counter-terrorism. The National Coordinator will be appointed by me and report to me through the Assistant to the President for National Security Affairs, as described in PDD-XX. Agency representatives to the CICG should be at a senior policy level (Assistant Secretary or higher). (U)

4. National Infrastructure Assurance Council: On the recommendation of the Lead Agencies and the National Coordinator, I will appoint a panel of major infrastructure providers and state and local government officials to serve as my National Infrastructure Assurance Council. I will appoint the Chairman. The National Coordinator will serve as the Council's Executive Director. The National Infrastructure Assurance Council will meet periodically to enhance the partnership of the public and private sectors in protecting our critical infrastructures and will provide reports to me as appropriate. Senior federal government officials will participate in the meetings of the National Infrastructure Assurance Council as appropriate. (U)

VII. Protecting Federal Government Critical Infrastructures (U)

Every department and agency of the U.S. government shall be responsible for protecting its own critical infrastructure, especially its cyber-based systems. Every department and agency Chief Information Officer (CIO) shall be responsible for information assurance. Every department and agency shall appoint a Chief Infrastructure Assurance Officer (CIAO) who shall be responsible for the protection of all of the other aspects of that department's critical infrastructure. The CIO may be double-hatted as the CIAO at the discretion of the individual department. No later than 120 days from today, every department and agency shall develop a plan for protecting its own critical infrastructure, including but not limited to its cyber-based systems. The National Coordinator shall be responsible for coordinating analyses required by the departments and agencies of inter-governmental dependencies and the mitigation of those dependencies. The Critical Infrastructure Coordinating Group (CICG) shall sponsor an expert review process for those plans. No later than two years from today, those plans shall have been implemented and shall be updated every two years. In meeting this schedule, the United States Government shall present a model to the private sector on how best to protect critical infrastructure. (U)

VIII. Tasks (U)

Within 120 days, the Principals Committee should submit to me a schedule for completion of a National Infrastructure Assurance Plan with milestones for accomplishing the following subordinate and related tasks. (U)

1. Vulnerability Analyses: For each sector of the economy and each sector of the government that might be a target of infrastructure attack intended to significantly damage the United States, there shall be an initial vulnerability assessment, followed by periodic updates. As appropriate, these assessments shall also include the determination of the minimum essential infrastructure in each sector. (U)

2. Remedial Plan: Based upon the vulnerability assessment, there shall be a recommended remedial plan. The plan shall identify timelines for implementation, responsibilities, and funding. (U)

3. Warning: A national center to warn of significant infrastructure attacks will be established immediately (see Annex A). As soon thereafter as possible, we will put in place an enhanced system for detecting and analyzing such attacks, with maximum possible participation of the private sector. (U)

4. Response: We shall develop a system for responding to a significant infrastructure attack while it is underway, with the goal of isolating and minimizing damage. (U)

5. Reconstituting: For varying levels of successful infrastructure attacks, we shall have a system to reconstitute minimum required capabilities rapidly. (U)

6. Education and Awareness: There shall be Vulnerability Awareness and Education Programs within both the government and the private sector to sensitize people to the importance of security and to train them of security standards, particularly regarding cyber systems. (U)

7. Research and Development: Federally sponsored research and development in support of infrastructure protection shall be coordinated, subject to multi-year planning, take into account private sector research, and be adequately funded to

minimize our vulnerabilities on a rapid but achievable timetable. (U)

8. Intelligence: The Intelligence Community shall develop and implement a plan for enhancing collection and analysis of the foreign threat to our national infrastructure, to include but not be limited to the foreign cyber/information warfare threat. (U)

9. International Cooperation: There shall be a plan to expand cooperation on critical infrastructure protection with like-minded and friendly nations, international organizations, and multinational corporations. (U)

10. Legislative and Budgetary Requirements: There shall be an evaluation of the executive branch's legislative authorities and budgetary priorities regarding critical infrastructure, and ameliorative recommendations shall be made to me if necessary. (U)

The CICG shall also review and schedule the taskings listed in Annex B. (U)

IX. Implementation (U)

In addition to the 120 day report, the National Coordinator shall report to me annually through the Principals Committee on the implementation of this directive. The report should include an updated threat assessment, a status report on achieving the milestones identified for the National Plan, and additional policy, legislative and budgetary recommendations. In addition, following the establishment of an initial operating capability in the year 2000, the National Coordinator shall conduct a zero-based review of the entire issue. (U)

Annex A: Structure and Organization (U)

Lead Agencies: Clear accountability within the U.S. government must be designated for specific sectors and functions. The following assignments of responsibility will apply. (U)

Lead Agencies for Sector Liaison:

Commerce	Information and communications
Treasury	Banking and finance
EPA	Water supply
Transportation	Aviation Highways (including trucking and intelligent transportation systems) Mass transit Pipelines Rail Waterborne commerce
Justice	Emergency law enforcement services
FEMA	Emergency fire service Continuity of government services
HHS	Emergency medicine and public health services
Energy	Electric power Oil and gas production and storage

Lead Agencies for Special Functions:

Justice	Law enforcement and internal security
DCI	Intelligence
State	Foreign affairs
Defense	National defense (U)

In addition, OSTP shall be responsible for coordinating research and development agendas and programs for the government through the National Science and Technology Council. (U)

National Coordinator: The National Coordinator for Security, Critical Infrastructure and Counter-terrorism shall be responsible for coordinating the implementation of this directive. The National Coordinator will report to me through the Assistant to the President for National Security Affairs. The National Coordinator will chair the interagency coordination committee, the Critical Infrastructure Coordinating Group (CICG). The Sector Liaison Officials and Special Function Coordinators shall attend the CIGC's meetings. Departments and agencies shall each appoint to the CIGC a senior official (Assistant Secretary level or higher) who will regularly attend its meetings. (U)

The National Coordinator will be assisted by a National Plan Coordination (NPC) staff of no more than 20 professionals, who shall be contributed on a non-reimbursable basis by the departments and agencies. The NPC staff shall be responsible for assisting the National Coordinator in his duties including coordinating legislative and public affairs, integrating the various sector plans into a National Infrastructure Assurance Plan and its successors, and coordinating analyses of the U.S. Government's own dependencies on critical infrastructure. Beginning in FY99, the Commerce Department shall serve as Executive Agent for administration of the NPC. The Defense Department shall continue to serve as Executive Agent for the Commission Transition Office, which will form the basis of the NPC, during the remainder of FY98. The Office of Personnel Management shall provide the necessary assistance in facilitating the NPC's operations. The NPC will terminate at the end of FY01, unless extended by Presidential directive. (U)

Warning and Information Centers

As part of a national warning and information sharing system, I immediately authorize the FBI to expand its current organization to a full scale Infrastructure Protection Center (IPC). This organization shall serve as a national critical infrastructure threat assessment, warning, vulnerability, investigation and response entity. During the initial period of six to twelve months, I also direct the National Coordinator and the Sector Liaison Officials, working together with the Sector Coordinators and the Special Function Coordinators, as appropriate, to consult with owners and operators of the critical infrastructures to encourage the creation of a private sector sharing and analysis center, as described below. (U)

Infrastructure Protection Center (IPC): The IPC will include FBI, USSS, and other investigators experienced in computer crimes and infrastructure protection, as well as representatives detailed from the Department of Defense, the Intelligence Community, and Lead Agencies. It will also have representatives from the private sector hired as full-time government employees or as contractors. It will be linked electronically to the rest of the U.S. government, including other warning and operations centers, as well as any private sector sharing and analysis centers, perhaps one as proposed below. Its mission will include providing timely warnings of intentional threats (as opposed to natural disasters, system failures, etc.), comprehensive analyses, and law enforcement investigation and response. (U)

The IPC will provide the locus of crisis management support and, in some cases, crisis management action, under the coordination of the National Coordinator and augmented as appropriate with persons determined by the National Coordinator. The FBI, through the IPC, shall have lead responsibility for operational response to infrastructure attacks. All executive departments and agencies shall cooperate with the IPC and provide such assistance, information and advice and the IPC may request, to the extent permitted by law. All executive departments shall also share with the IPC information about threats and warning of attacks, and about actual attacks on critical government and private sector infrastructures, to the extent permitted by law. The IPC will include at least a National Critical Indications and Warning Office, a National Critical Infrastructure Management Office, a Computer and Operations Section and a Liaison Section whose mission will be to establish its own relations directly with others in the private sector and to link up with any information sharing and analysis entity that the private sector may create, such as the Information Sharing and Analysis Center suggested below. (U)

The IPC, in conjunction with the information originating agency, will sanitize law enforcement and intelligence information for inclusion into analyses and reports that it will provide, in appropriate form, to relevant federal, state and local agencies; the relevant owners and operators of critical infrastructures; and to any private sector information sharing and analysis entity. Whether as sanitized or unsanitized reports, the IPC will issue attack warnings or alerts to increases in threat condition to any private sector information sharing and analysis entity and to the owners and operators. These warnings may also include guidance regarding additional protection measures to be

taken by owners and operators. Except in extreme emergencies, the IPC shall coordinate with the National Coordinator before issuing warnings of imminent attacks by international terrorists, foreign states, or other malevolent foreign powers. (U)

The IPC will be responsible for developing ties with first responders, to include state and local governments, to an attack on critical infrastructures. The IPC shall build on FBI's long-standing relationship with state and local law enforcement through mechanisms like the Joint Terrorism Task Forces to conduct outreach, provide training, share law enforcement techniques and information and provide channels of communication during crises. (U)

The IPC will provide a national focal point for gathering information on threats to the infrastructures. Additionally, the IPC will provide the principal means of responding to an incident, mitigating attacks, and investigating threats. As such, the IPC will maintain the ability, in the event of a foreign threat, to transfer primary responsibility to the Intelligence Community or the Defense Department, depending on the nature of the emergency. Depending on the nature and level of the threat/attack, protocols established between special function agencies (DoJ/DoD/CIA), and the ultimate decision of the President, the IPC may be placed in a direct support role to either DoD or the Intelligence Community. (U)

Information Sharing and Analysis Center (ISAC): The National Coordinator, working with Sector Coordinators and Sector Liaison Officials, shall consult with owners and operators of the critical infrastructures to encourage the creation of a private sector information sharing and analysis center. Such a center could serve as a mechanism for gathering, analyzing, and disseminating information regarding critical infrastructure protection, including information about vulnerabilities, threats, intrusions, and anomalies. The actual design and functions of the center and its relation to the IPC will be determined by the private sector, in consultation with and with assistance from the federal government.

Annex B: Additional Taskings (U)

Studies (U)

The National Coordinator shall commission studies on the following subjects: (U)

- o Liability issues arising from participation by private sector companies in the information sharing process. (U)

- o Existing legal impediments to information sharing, with an eye to proposals to remove these impediments, including through the drafting of model codes in cooperation with the American Legal Institute. (U)

- o The necessity of document and information classification and the impact of such classification on useful dissemination, as well as the methods by which threat and vulnerability information can be shared while avoiding disclosure to those who will misuse it. (U)

- o The protection of industry trade secrets and other confidential business data, law enforcement information and evidentiary material, classified national security information, unclassified material disclosing vulnerabilities of privately owned infrastructures, and apparently innocuous information that, in the aggregate, it is unwise to disclose. (U)

- o The implications of sharing information with foreign entities where such sharing is deemed necessary to the security of U.S. infrastructures. (U)

- o The potential benefit to security standards of mandating insurance for selected critical infrastructure providers and requiring insurance tie-ins for foreign critical infrastructure providers hoping to do business with the United States. (U)

Public Outreach

In order to foster a climate of enhanced public sensitivity to the problem of infrastructure protection, the following actions shall be taken: (U)

o The White House, under the oversight of the National Coordinator, together with the relevant Cabinet agencies shall sponsor a series of conferences: (1) that will bring together national leaders in the public and private sectors to propose programs to increase the commitment to information security; (2) that convoke academic leaders from engineering, computer science, business and law schools to review the status of education in information security and will identify changes in the curricula and resources necessary to meet the national demand for professionals in this field; (3) on the issues around computer ethics as these relate to the K through 12 and general university populations. (U)

o The National Academy of Sciences and the National Academy of Engineering shall establish a round table bringing together federal, state and local officials with industry and academic leaders to develop national strategies for enhancing infrastructure security. (U)

o The intelligence community and law enforcement shall expand existing programs for briefing infrastructure owners and operators and senior government officials. (U)

o The National Coordinator shall (1) establish a program for infrastructure assurance simulations involving senior public and private officials, the reports of which might be distributed as part of an awareness campaign, and (2) in coordination with the private sector, launch a continuing national awareness campaign, emphasizing improving infrastructure security. (U)

Internal Federal Government Actions

In order for the federal government to improve its infrastructure security, these immediate steps shall be taken: (U)

o The Department of Commerce, the General Services Administration, and the National Security Agency shall assist federal agencies in the implementation of best practices for information assurance within their individual agencies. (U)

o Every federal agency shall have a chief information officer (CIO) who shall be responsible for information systems assurance. Every department and agency shall also appoint a Chief Infrastructure Assurance Officer (CIAO) who shall be

o The White House, under the oversight of the National Coordinator, together with the relevant Cabinet agencies shall sponsor a series of conferences: (1) that will bring together national leaders in the public and private sectors to propose programs to increase the commitment to information security; (2) that convoke academic leaders from engineering, computer science, business and law schools to review the status of education in information security and will identify changes in the curricula and resources necessary to meet the national demand for professionals in this field; (3) on the issues around computer ethics as these relate to the K through 12 and general university populations. (U)

o The National Academy of Sciences and the National Academy of Engineering shall establish a round table bringing together federal, state and local officials with industry and academic leaders to develop national strategies for enhancing infrastructure security. (U)

o The intelligence community and law enforcement shall expand existing programs for briefing infrastructure owners and operators and senior government officials. (U)

o The National Coordinator shall (1) establish a program for infrastructure assurance simulations involving senior public and private officials, the reports of which might be distributed as part of an awareness campaign, and (2) in coordination with the private sector, launch a continuing national awareness campaign, emphasizing improving infrastructure security. (U)

Internal Federal Government Actions

In order for the federal government to improve its infrastructure security, these immediate steps shall be taken: (U)

o The Department of Commerce, the General Services Administration, and the National Security Agency shall assist federal agencies in the implementation of best practices for information assurance within their individual agencies. (U)

o Every federal agency shall have a chief information officer (CIO) who shall be responsible for information systems assurance. Every department and agency shall also appoint a Chief Infrastructure Assurance Officer (CIAO) who shall be

responsible for the protection of all of the other aspects of that department's critical infrastructure. The CIO may be double-hatted as the CIAO at the discretion of the individual department. These officials shall establish procedures for obtaining expedient and valid authorizations to allow vulnerability assessments to be performed on government computer and physical systems and the Department of Justice shall establish legal guidelines for providing for such authorizations. (U)

o All federal agencies shall make clear designations regarding who may authorize access to their computer systems. (U)

o The Intelligence Community shall elevate and formalize the priority for enhanced collection and analysis of information on the foreign cyber/information warfare threat to our critical infrastructure. (U)

o The Federal Bureau of Investigations, the Secret Service and other appropriate agencies shall (1) vigorously recruit undergraduate and graduate students with the relevant computer-related technical skills for full-time employment as well as for part-time work with regional computer crime squads, and (2) facilitate the hiring and retention of qualified personnel for technical analysis and investigation involving cyber attacks. (U)

o The Department of Transportation, in consultation with the Department of Defense, shall undertake a thorough evaluation of the vulnerability of the Global Positioning System including sponsoring an independent, integrated assessment of risks to civilian users of GPS-based systems, with a view to basing decisions on the ultimate architecture of the modernized NAS on these evaluations. (U)

o The Federal Aviation Administration shall develop and implement a comprehensive National Airspace System Security Program to protect the modernized NAS from information-based and other disruptions and attacks. (U)

o GSA shall identify large procurements (such as the new Federal Telecommunications System, FTS 2000) related to infrastructure assurance, study whether the procurement process reflects the importance of infrastructure protection

Withdrawal/Redaction Marker
Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
002a. memo	Richard A. Clarke to Jacob J. Lew; re: PDDs (2 pages)	02/23/1998	P1/b(1), P5

COLLECTION:
Clinton Presidential Records
National Security Council
Richard A. Clarke (Transnational Threats (TNT))
OA/Box Number: 1381

FOLDER TITLE:
February Chron - 1998 [13]

2006-0191-F
jp280

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advise between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.
PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).
RR. Document will be reviewed upon request.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20504

February 9, 1998

MEMORANDUM FOR JACOB J. LEW
DEPUTY DIRECTOR
OFFICE OF MANAGEMENT AND BUDGET

FROM: RICHARD A. CLARKE

SUBJECT: OMB Concerns with PDDs - XX/YY

I would like to arrange a meeting early this week to address the concerns that you raised in the Deputies Committee meeting.

Specifically, I have in mind briefings for you on the PHS and Secret Service counter-terrorism roles and missions. Both agencies seemed to have the impression that OMB did not understand what they currently do in the counter-terrorism arena.

Please let me know times early this week when you can schedule either one 90 minute session or two 45 minute sessions. If we can find a mutually agreeable time , we will convene the appropriate members of the CSG. Steve Simon (456-9351) is my point of contact for arranging these meetings.

In addition, you again raised concern with the use of the term "robust" for the President to describe his goals for funding counter-terrorism and WMD protection programs. We continue to think it is appropriate for the President to express his view that this protection of the American people against terrorism and WMD should be a high budgetary priority. You will note that the draft says that they budget review should be part of the normal OMB budgetary process. If you have alternative language, we have not seen it and remain eager to see it.

Indeed, if you have a proposed alternative language for either PDD, we would welcome a chance to review it so that the NSC dialogue with OMB can advance from the general discussions we have had for months, to more specifics, and a mutually agreeable text.

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

MEMORANDUM FOR DICK CLARKE

CC: JACK LEW
JIM STEINBERG

FEB 12 1998

FROM: MICHAEL DEICH

SUBJECT: OMB Concerns with PDD XX and PDD YY

Thanks for your note. I've discussed your ideas with Jack, and would like to offer the following suggestions for addressing OMB's remaining concerns about the draft PDDs.

1. Budget issues regarding PDDs XX and YY. We need to identify which of the responsibilities described in the draft PDDs could be carried out with the resources requested by the President's Budget for FY99 and beyond, and which of the responsibilities would require additional resources. In order to resolve the issue quickly, I would like to consider the matter at a meeting of all the affected agencies. In lieu of a meeting, however, the PDD could include the following language: "Agencies shall implement the policies described in this PDD within the resource levels requested in my Budget for fiscal years 1999 - 2003." Finally, to clear up apparent confusion about the President's Budget request, OMB will send a memo to the affected agencies clarifying which agencies and what functions would be eligible for funding under the FY 99 request for $34 million for infrastructure protection.

2. National special security events. Rather than getting a separate briefing from Secret Service, I'd like to have a single meeting with the Secret Service, the FBI, OMB and NSC to agree on the roles of the Secret Service and the FBI in providing protection at special events. If you are unwilling to have such a meeting, the draft PDD should make clear that it contemplates no change in the role of the Secret Service in special events.

3. Balancing National Security/law enforcement and Economic Security in PDD YY. OMB continues to believe that PDD YY gives short shrift to the role of the private sector in infrastructure protection. To correct the imbalance, we believe that the NEC should co-chair the CICG. In addition, the National Plan Coordination office should be housed at Commerce and staffed by permanent Commerce employees (both to avoid an 'augmentation' of NSC resources and to reflect the significant role that the private sector will have to play in achieving infrastructure protection goals).

4. Other. I've asked Ken Schwartz and David Morrison to meet with Steve Simon to review a number of instances in which we believe the drafts to be factually incorrect, and to get from Steve clarification of certain instances in which we find the language of the draft PDDs to be unclear.

Please let me know how you'd like to proceed on these issues.

The current draft of PDD-YY includes the following language on the National Plan Coordination staff:

A National Plan Coordination (NPC) staff will be contributed on a non-reimbursable basis by the departments and agencies. The NPC staff will integrate the various sector plans into a National Infrastructure Assurance Plan and coordinate analyses of the U.S. government's own dependencies on critical infrastructures. The NPC staff will also help coordinate a national education and awareness program, and legislative and public affairs. (U)

Beginning in FY99, the Commerce Department shall serve as Executive Agent for administration of the NPC. The Defense Department shall continue to serve as Executive Agent for the Commission Transition Office, which will form the basis of the NPC, during the remainder of FY98. The Office of Personnel Management shall provide the necessary assistance in facilitating the NPC's operations. The NPC will terminate at the end of FY01, unless extended by Presidential directive. (U)

Withdrawal/Redaction Marker
Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
002d. memo	POTUS to VPOTUS et al; Excerpt fromPresidential Decision Directive (2 pages)	circa, 02/1998	P1/b(1)

COLLECTION:
Clinton Presidential Records
National Security Council
Richard A. Clarke (Transnational Threats (TNT))
OA/Box Number: 1381

FOLDER TITLE:
February Chron - 1998 [13]

2006-0191-F
jp280

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advise between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.
PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).
RR. Document will be reviewed upon request.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

The current draft of PDD-YY includes the following language on the role of the NEC:

Interagency Coordination: The Sector Liaison Officials and Functional Coordinators of the Lead Agencies, as well as representatives from other relevant departments and agencies, including the National Economic Council, will meet to coordinate the implementation of this directive under the auspices of a Critical Infrastructure Coordinating Group (CICG), chaired by the National Coordinator for Security, Critical Infrastructure and Counter-terrorism. The National Coordinator will be appointed by me and report to me through the Assistant to the President for National Security Affairs, who shall assure appropriate coordination with the Assistant to the President for Economic Affairs. Agency representatives to the CICG should be at a senior policy level (Assistant Secretary or higher). (U)

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20504

February 3, 1998

MEMORANDUM FOR BRONYA CLARK

FROM: CAROLYN DOLLAR

SUBJECT: Cancellation of Travel Authorizations XK8E17 and XKS8E38

Due to the needs of the service, authorized travel for Messrs. Simon and Metzl were cancelled. Airline Ticket Refund Receipt No. 1029002 for Jamie Metzl's airline fare in the amount of $2,028.00 has been received from American Express (White House Travel Office) and is being forwarded for close-out of his authorization. Airline tickets were not picked up from American Express for Mr. Simon prior to cancellation of travel.

Please deobligate, as unexpended funds, the two travel authorizations for their full amounts as follows:

XK8E17 - $3765.00

XKS8E38 - $2311.00

Attachments

Tab I Travel Authorization XK8E17 w/refund receipt/Doc 20042
Tab II Travel Authorization XKS8E38/Doc 20041

Withdrawal/Redaction Marker
Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
003. memo	Steve Simon & Carolyn Dollar to Officer-in-Charge; re: Request for Appointments (partial) (1 page)	02/02/1998	P6/b(6)

COLLECTION:
Clinton Presidential Records
National Security Council
Richard A. Clarke (Transnational Threats (TNT))
OA/Box Number: 1381

FOLDER TITLE:
February Chron - 1998 [13]

2006-0191-F
jp280

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P1 National Security Classified Information [(a)(1) of the PRA]
P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P3 Release would violate a Federal statute [(a)(3) of the PRA]
P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P5 Release would disclose confidential advise between the President and his advisors, or between such advisors [a)(5) of the PRA]
P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.
PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).
RR. Document will be reviewed upon request.

Freedom of Information Act - [5 U.S.C. 552(b)]

b(1) National security classified information [(b)(1) of the FOIA]
b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

REQUEST FOR APPOINTMENTS

To: Officer-in-charge
Workers and Visitor Entrance System
Room 562, OEOB

Please admit the following appointments on **Tuesday, February 3, 1998**

for a meeting with Steve Simon of NSC Global Affairs

NAME	DATE OF BIRTH	(Non-US) COUNTRY CODE
GRAY, Joseph G	12/5/35	66 U.S.
KNOUSS, Robert F	7/3/44	U.S.
CAMPANA, Rinaldo A	7/3/46	U.S.
CLARK, William	8/29/38	U.S.
McCOY, William (Bill)	1/28/45	U.S.
SHARRO, Stephen	11/27/48	U.S.
NOLIN, Patricia	3/12/53	U.S.

MEETING LOCATION

Building OEOB — Requested by Steve Simon/Carolyn Dollar

Room No. 208 — Room No.303 — Telephone 456-9361

Time of Meeting 3PM – 4 PM — Date of request 2/2/98

Additions and/or changes made by telephone should be limited to five (5) names or less.

WAVES Center: WHITE HOUSE - 456-6742

UNITED STATES SECRET SERVICE — Format from SSF 2037 (09/91)