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 [12]
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
~~001. letter~~	~~Richard A. Clarke to David Leelaire; re; Addition to Staff [1 page RELEASED ON APPEAL] (page)~~	~~01/30/1998~~	~~P5~~
~~002. talking points~~	~~re: Talking Points for POTUS-Prime Minister Blair Meeting (2 pages)~~	~~circa, 02/1998~~	~~P1/b(1)~~ VZ 9/21/2023
003. list	re: UNIKOM Issues - Iraq Pol-Mil Plan (1 page)	circa, 02/1998	P1/b(1)
004a. 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
~~004b. paper~~	~~re: Discussion Paper for NSC Deputies Committee Meeting on Unconventional Threats to U.S. (9 pages)~~	~~01/24/1998~~	~~P1/b(1)~~ VZ 9/21/2023
004c. memo	For VPOTUS et al - Presidential Decision Directive; 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 [12]

2006-0191-F
jp279

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]

****
*** TX REPORT ***
****

TRANSMISSION OK

TX/RX NO	1888
CONNECTION TEL	95865670
CONNECTION ID	DP-1
ST. TIME	02/02 08:59
USAGE T	00'48
PGS.	2
RESULT	OK

NATIONAL SECURITY COUNCIL

FAX COVER SHEET

NATIONAL SECURITY COUNCIL
Office of Global Affairs

17th & Penn, N.W.
Washington, D.C.
20504

Did you get a complete, clear transmission? If not,

From: Richard A. Clarke

To: Mr. David Leclaire

Agency: Department of Energy

Fax Number: (202) 586-5670

Date/Time: Monday, February 02, 1998

No. of pages to follow: cover plus 1

Message: re: our telephone conversation on Friday, January 30, 1998. Tried to send this fax earlier.

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20504

January 30, 1998

Mr. David Leclaire
Deputy Assistant Secretary
Program Support - Defense Program
Department of Energy DP40, GTN

Dear Mr. Leclaire:

The new terrorism Presidential Decision Directive (PDD) will establish the position of National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism. In view of the broad scope of this office, the President has authorized the creation of Assistant Secretary level interagency working groups to support its work and coordinate the implementation of the PDD.

The Assistant to the President for National Security has asked Lisa Gordon-Hagerty, a DOE employee, to join my staff as a detailee to manage the most challenging of the PDD working groups. In this position, Ms. Gordon-Hagerty will coordinate interagency activities related to national, government-wide programs, including domestic WMD emergency preparedness, consequence management, and prevention of WMD ingress into the United States.

Since her responsibilities will be so wide-ranging and require her to interact routinely as a peer with senior officials at the Assistant Secretary level and above, I request that Ms. Gordon-Hagerty be promoted to senior level rank as soon as possible.

If you have any questions, do not hesitate to contact me. Your help in this matter is greatly appreciated.

Sincerely

Richard A. Clarke
Special Assistant to the President

TIME OF TRANSMISSION: TIME OF RECEIPT:

WHITE HOUSE SITUATION ROOM

PRECEDENCE: **IMMEDIATE**

CLASSIFICATION: ~~**CONFIDENTIAL**~~

RELEASER: _____

DATE/TIME: **2/2/98**

MESSAGE #: _____

FROM: **LEONARD HAWLEY** PH: **456-9351** ROOM: **302**

SUBJECT: **TALKING POINTS FOR POTUS MTG W/PM BLAIR** PAGES: **3**

PLEASE DELIVER TO:

LOCATION	DELIVER TO	ROOM	PHONE
STATE/IO	**MOLLY WILLIAMSON**		**647-9600**

SPECIAL DELIVERY INSTRUCTIONS/REMARKS:

Molly, Princeton cleared these points on Saturday, before he left.
Len.

TALKING POINTS FOR POTUS-PM BLAIR MEETING

Security Council Expansion

Background: We are working with the P3&2 Group (US, UK, FR & Japan, Germany) in New York to hammer out a framework resolution for Security Council reform in 1998. There are two contentious issues. First, size of expansion - we are holding at 21 seats, while everyone else wants 24. Second, veto for new permanent members - we are firm that the veto question should not be considered until the new Council membership is determined. On the home front, we do not want action on Security Council reform to jeopardize timely Hill action of UN arrears legislation this Spring.

On the 24 seat debate, the UK is concerned that without progress this year, Germany will join Italy in pushing for one or more rotating seats for the EU—a move that threatens Britain's permanent seat on the Council. UK is pressing us to accept a 24 seat expansion.

On the veto issue, the UK agrees with us on deferring this question until the Council's new members have been determined.

Talking Points:

- I am determined to maintain momentum on Security Council expansion this year. However, early action on Council expansion in New York, especially if it is controversial with Congress, would jeopardize passage of UN arrears legislation this Spring. Nonetheless, I do not intend to allow this initiative to lead to a dead end.

- Therefore, we need to slow down the P3&2 process, giving us time to pass UN arrears legislation this Spring. This must be done without inducing any adverse action on Security Council reform, especially among EU members. The process is manageable, and we will collaborate with you over the coming weeks to orchestrate our efforts.

- Regarding the 21 seat limitation, I recognize we face opposition to our firm stand to preserve the Council's efficiency. However, as we see in the continuing Iraqi-UNSCOM crisis, Security Council efficiency is a decisive factor in responding to threats to international peace and security.

- As long as we focus the international debate on regional representation within the Council, I am confident we can overcome opposition to the 21 seat limitation.

- Regarding extension of the veto, it is premature to consider this critical issue without resolution on the remaining questions.

- The P3&2 Group is making progress toward resolving those remaining questions. Hopefully, we can have a framework resolution passed in the General Assembly in 1998.

UN Arrears

Background: UK has been consistently harsh in its criticism of the U.S. regarding our failure to pay UN arrears. The Brits have taken a tough line on full and unconditional payment of the $1.5 billion we owe the UN.

Talking Points

- I was upset that Congress blocked our plan to pay about $1 billion of our UN arrears because of domestic politics. We had worked long and hard with Senator Helms and other Republicans and I thought we had a deal.

- I intend to get supplemental legislation passed before May. My proposal includes over $1.0 billion in arrears payments and only those conditions that all nations would agree to--most of them involving questions of national sovereignty.

- Congress will demand reductions in our assessment rates, once the arrears legislation is passed. I am seeking less controversial scale reductions of 22% in the Regular Budget and 25% for Peacekeeping at the UN.

- Once we get the legislation passed this Spring, I will need UK's help, especially with the EU, to have the General Assembly take action in June to allow us to pay our arrears.

- UK's influence will be decisive. We've put a tremendous amount of effort into closing the gap between what Congress will provide and what the General Assembly will accept. It will be a contentious debate, but progress can be made if we work together.

TIME OF TRANSMISSION: TIME OF RECEIPT:

WHITE HOUSE SITUATION ROOM

PRECEDENCE: **IMMEDIATE**

CLASSIFICATION: ~~SECRET~~

RELEASER: _____

DATE/TIME: **2/2/98**

MESSAGE #: _____

FROM: **LEONARD HAWLEY** PH: **456-9351** ROOM: **302**

SUBJECT: **UNIKOM ISSUES** PAGES: **2**

PLEASE DELIVER TO:

LOCATION	DELIVER TO	ROOM	PHONE
USUN	**COL RICH ROAN**		**212-415-4363**

SPECIAL DELIVERY INSTRUCTIONS/REMARKS:

Withdrawal/Redaction Marker
Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
003. list	re: UNIKOM Issues - Iraq Pol-Mil Plan (1 page)	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 [12]

2006-0191-F
jp279

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
004a. 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 [12]

2006-0191-F
jp279

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

DISCUSSION PAPER FOR
NSC DEPUTIES COMMITTEE MEETING ON UNCONVENTIONAL THREATS TO THE UNITED STATES (U)

References: (1) Report of President's Commission on Critical Infrastructure Protection; (2) Draft PDD-XX; (3) Draft PDD-YY

This discussion paper addresses how the US Government should be structured to respond to the emerging, unconventional threats to US territory and Americans abroad. The paper is keyed to the latest drafts of PDD-XX and PDD-YY, attached. These drafts have changed from previous versions based upon informal interagency coordination.

1.0 Background

There are increased concerns about our vulnerability to unconventional threats because:

o The margin of U.S. military superiority over potential enemies is so great that it may force such enemies to look for unconventional ways to attack us, such as attacks in the homeland to intimidate us and to degrade our military response;

o Many of our potential enemies have access to unconventional means including terrorism, weapons of mass destruction, and cyber warfare capabilities; they could use these unconventional methods of attack singly or in combination;

o Our potential enemies include non-state actors such as terrorist groups and international organized criminal syndicates, some of which are capable of posing the same level of unconventional threat as nations;

o Federal agencies, state and local governments, and private sector institutions all have significant vulnerabilities to unconventional attacks;

o The increasing interdependence of elements of our government, military, economy, and society on a set of interrelated, interdependent infrastructures could make the scope and effects of unconventional attacks extremely damaging.

Classified by: Glyn T. Davies
Reason: 1.5(d)
Declassified on: 01-24-08

1.1 Expressions of Concern: These concerns have been expressed by the President, the Congress, senior Administration officials, and panels, most notably the Marsh Commission.

The President: Over the last three years the President has repeated his personal concern, as in these examples:

> "New technologies make our borders vulnerable to terrorists and dangerous weapons....Every day millions of people use laptops, modems, CD ROMs, (but) technology can be used for good or evil....these forces make us even more vulnerable to the organized forces of destruction, the forces of terror....The technological revolution can bring more and more problems to our shores....Today the threat to our security is not just in an enemy silo, but in a briefcase or in the car bomb of a terrorist."

> "Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States....Because many of these critical infrastructures are owned and operated by the private sector, it is essential that the government and private sector work together to develop a strategy for protecting them and assuring their continued operation."

And in Tuesday's State of the Union:

> "We must combat an unholy axis of new threats from terrorists, international criminals.... These 21st century predators feed on technology and the free flow of information and ideas and people. And they will be all the more lethal if weapons of mass destruction fall into their hands."

Congress: The Congress has, on several occasions, indicated its interest in the further integration and coordination of these issues.

o The Senate Appropriations Committee required the Administration to submit by the end of 1998 a comprehensive interdepartmental plan for dealing with critical infrastructure protection, terrorism, and weapons of mass destruction vulnerability in the U.S.

o The Intelligence Authorization called for the establishment within the NSC of a new "Committee on Transnational Threats" to be chaired by the APNSA, the primary function of which would be to "coordinate and direct the activities of the USG relating to combating transnational threats."

o The Defense Authorization mandated that the President designate an individual to serve in the Executive Office of the President as the National Coordinator on Proliferation Matters

to advise on non-proliferation of WMD, including issues related to terrorism, arms control, and international organized crime, and to coordinate nonproliferation research efforts.

Senior Administration Officials: The Attorney General, Secretary of Defense, and others have addressed this issue:

> "The front lines are no longer overseas; it can just as well be in any American city."
> William Cohen, 25 November 1997

> "The evolving security environment has significant implications for how the national security apparatus operates. The distinction between foreign and domestic policies are less pronounced than in the past. The United States faces a panoply of threats that require smooth interaction among diplomatic, military, law enforcement, and consequence management organizations. Our national security apparatus must be flexible and responsive to meet the kinds of challenges this nation will face in the foreseeable future." William Cohen, 15 December 1997

> "We will develop an effective capability to detect, prevent, defeat and manage consequences of nuclear, biological and chemical material and weapons used by terrorists. Let me explain briefly some of the means by which we seek to accomplish these objectives....A Presidential Commission on Critical Infrastructure Protection has been created....as part of this effort, an Information Protection Task force has been created. It is a multi-agency effort to identify and coordinate existing expertise and capability, in the government and the private sector, relative to critical infrastructure protection" Janet Reno, 13 May 1997

Panels and Commissions: There have been numerous reports, both within and outside of the government, that have addressed these issues and recommended additional efforts, coordination and integration:

o The December 1997 report of the National Defense Panel which stressed the need for increased emphasis, comprehensive planning, and interagency coordination on homeland defense, focusing on the interrelated dangers of terrorism, weapons of mass destruction and consequence management, and information warfare and attacks on critical infrastructures.

o The October 1997 report of the President's Commission on Critical Infrastructure Protection (Marsh Commission) recommended that the administration coordinate critical infrastructure protection through an office in the NSC, create a interdepartmental support office located in Commerce, formalize a "lead agency" management process, and create a public/private information sharing and analysis center.

o The March 1997 report of the Livermore Study Group on Terrorist Use of Weapons of Mass Destruction (Woolsey-Nye report) called for a National Coordinator reporting to the Vice President and supported by a planning staff.

o The Brown Commission on U.S. Intelligence for the Twenty-First Century recommended the creation of a coordinator on the NSC and a permanent support staff to address terrorism, WMD proliferation, narcotics trafficking, and international organized crime.

o The 1996 report of the Defense Science Board Task Force on Information Warfare-Defense recommended establishing a center for intelligence, indication and warning, and threat assessment within the Defense Department and also recommended possibly establishing an additional public/private center for indications and warning.

o The Commission on the Roles and Missions of the Armed Forces recommended that the office of the Vice President be charged with integrating the nation's response capabilities and that a permanent multiagency planning staff be established.

2.0 Proposed Directives and Structure

2.1 The PDDs: A pair of Presidential Decision Directives have been drafted in response to these concerns and proposals:

o PDD-XX: The purpose of this directive is twofold. First, it is a vehicle for the President to re-emphasize the importance he personally attaches to addressing the unconventional threats to the homeland and to Americans abroad. Second, the directive establishes an improved system for interagency coordination and accountability, by strengthening the Lead Agency approach and specifying ten program areas. There would be clear responsibility for policy development and implementation for each program.

o PDD-YY: This directive elaborates policy on one of the ten program areas, the protection of critical infrastructure. A separate Directive is required because no Administration has ever enunciated a comprehensive and detailed policy and program in this area. The Directive incorporates the work of the Marsh Commission. The central concept incorporated in this PDD is that of a Public/Private Partnership leading to the greatest possible voluntary cooperation between the government and the private sector to reduce vulnerabilities. Two other key

concepts are an outreach program of Education and Awareness and the creation of a National Infrastructure Protection Plan.

2.2 The Structure: The two Directives use an interagency structure to address the unconventional threats by building on the current interagency system and by adding specific, new Critical Infrastructure organizations.

o IWGs: The existing IWGs for Counter-terrorism, Critical Infrastructure Protection and WMD Counter-terrorism Consequence Management would be the core of the interagency system. These IWGs would each meet at the Assistant Secretary-level or above and be chaired by a Special Assistant to the President (NSC) with the designation National Coordinator for Security, Critical Infrastructure and Counter-Terrorism. A new IWG, Security of Essential Government Operations, will also be created and chaired by the National Coordinator, as a complement to the existing IWG on Continuity of Government Operations. The National Coordinator, as the chair of the groups, may convene joint meetings as appropriate. When the DC or PC meets to consider counter-terrorism, security or infrastructure protection issues, the National Coordinator would join the meeting as a full member.

o IPC: An Infrastructure Protection Center would be created in the Department of Justice, FBI. The Center would provide a warning, assessment, and crisis management focus for infrastructure and, particularly, cyber attacks.

o ISAC: The USG would encourage the private sector to create an Information Sharing and Analysis Center to address cyber and other critical infrastructure issues. The USG would facilitate and, as appropriate, participate in the ISAC. The rationale for a private sector entity is that (a) infrastructures are largely owned and operated by the private sector, (b) infrastructures are increasingly interdependent requiring a means of sharing and assessing vulnerabilities and other protection information across sectors, (c) the private sector needs a locus for its own activities in support of the Government effort, and (d) the private sector may be reluctant, at least initially, to share vulnerability and competitive information with the Government.

In addition, the PDD carries forward the Commission recommendations for an Advisory Council and a small interagency National Plan Coordination staff (NPC). The NPC staff would coordinate the integration of the various components of the

National Infrastructure Protection Plan, which will be developed by the various Lead Agencies. The NPC staff would also coordinate the government-wide outreach and Education and Awareness efforts. The NPC staff in the directive is, however, half the size of the current Transition Office and has a sunset provision following the creation of the National Infrastructure Protection Plan.

3.0 Issues for Discussion

3.1 Integration of Unconventional Threat Responses: As noted in sections 1.0 and 2.0 above, the President, Congress, and expert panels have seen a commonality among the unconventional threats to the homeland and Americans abroad. Currently the USG structure does not integrate these threats for policy development, implementation, or crisis management below the Deputy Secretary level in most agencies. The National Coordinator, in his role as the chair of the related IWGs, would be responsible for ensuring such coordination, and for raising these issues for consideration by the Deputies or Principals, as appropriate.

These Directives do not create a structure similar to the "Drug Czar," which is a separate organization in the Executive Office of the President, has a staff of 200, and is headed by a Cabinet Rank officer subject to Senate confirmation. Instead, the directives employ and strengthen the Lead Agency approach, and designate a senior officer within the NSC staff system to coordinate the work of the IWGs.

Alternatives to the PDDs would be to:

o Have the IWGs report to a new senior coordinating group on these issues which would report directly to the Principals Committee

o Merge the existing four IWGs into the terrorism IWG

o Create a new agency within the Executive Office of the President, similar to the "Drug Czar"

-- or, conversely, have separate several senior NSC Staff officers, each with one or two assistants, to serve as the White House point of contact for each of the types of Unconventional Threats.

3.2 Single Lead Agency for Critical Infrastructure: The two draft directives assign specific Lead Agency functions to several departments. There is not a single Lead Agency. Coordination among the departments is facilitated by an interagency National Plan Coordination Support Staff, for which the Commerce Department would serve as Executive Agent.

An Alternative Approach to this distributed approach would be to place a single department, specifically the Justice Department, in the role of Lead Agency. Justice has objected to an approach which does not designate a single Lead Agency. Justice is creating a large, well-funded Infrastructure Protection Center (IPC) within the FBI, as one of the offices reporting to a Deputy Assistant Director of the Bureau.

In the Alternative Approach, the IPC could perform the role of two other components in PDD-YY, the National Plan Coordination staff and the Information Sharing and Analysis Center.

3.2.1 The Information Sharing and Analysis Center: Based on the work of the Commission and the IWG, draft PDD-YY proposes that the USG work with the private sector to develop a complementary analysis entity to the proposed Justice Department Information Protection Center (IPC). The proposed private sector counter-part could be called the Information Sharing and Analysis Center (ISAC).

While the USG can not create the ISAC, the PDD would have the USG urge and facilitate its creation and make suggestions about how it might work. The rationale for the ISAC would be:

o The various sectors of the commercial, private infrastructures each have their own industry/trade groups that could address infrastructure issues, but there is no such group that serves as a venue for all sectors to develop education and awareness programs, fund research, or develop policies;

o Some parts of the private sector have demonstrated a reluctance to share proprietary information with the Justice Department and FBI; these companies might be more willing to participate in vulnerability analyses and report on problems if the reports were going to an industry owned and operated institute which could filter the information provided to DOJ/FBI.

The Alternative Approach would rely upon the FBI's IPC to perform this liaison with the private sector. This approach

would avoid the USG giving the appearance of condoning a non-governmental entity as the locus for reporting crimes. The private sector could develop some entity on its own, but the USG would not actively encourage or facilitate it.

3.2.2 The National Plan Coordination (NPC) support staff: The draft PDD-YY directs that the Commission Transition Office be reduced in size by roughly half to 20 professionals, be redesignated the National Plan Coordination support staff, and be given a "sunset clause" or limited duration of 36 months (the period during which the National Infrastructure Protection Plan would be under development). The draft PDD assigns the staff office to the Commerce Department as Executive Agent beginning in FY99 (until then it would continue in DOD).

The rationale for the Office is that this new and complex issue spills over any one department and requires full time coordination of the work of many departments and agencies. The tasks of the office would be:

o Coordinate the development of the sector plans and their integration into the National Infrastructure Protection Plan;

o Coordinate the development of a U.S. Government Protection Plan from the submissions of the CIOs of each department and agency;

o Coordinate outreach to the public and the sectors; implement the Education & Awareness recommendations of the Commission;

o Serve as Executive Secretary of the Interagency Working Group on Critical Infrastructure Protection;

o Conclude the classification, publication, and disposition of the Commission's documentation.

The draft PDD places the Office in the Department of Commerce as Executive Agent. The rationale for that assignment is the belief that the private sector reaction to the PDD implementing the Commission's recommendations would be more favorable if the organization demonstrates USG appreciation for the private sector's role in critical infrastructure protection, the need for effective business rationale for USG's expectations of private sector protection efforts, and to further encourage understanding of the breadth of the issues involved (business, defense, law enforcement, intelligence, etc.). Without that

assignment, the PDD would seem to treat the Critical Infrastructure issue exclusively as a national security/law enforcement problem.

The Alternative Approach would rely upon the only large infrastructure staff in the USG to perform these roles for the rest of the government, i.e. the FBI's IPC. In addition 3-4 NSC staffers would be reassigned from their current duties to work with the IPC and the Interagency Working Group. The IPC would:

o Coordinate the portions of the National Plan initially drafted by each of the Departments with a Lead Sector liaison function;

o Review the individual department and agency's cyber security and protection plans for there own internal operations.

3.3 Extension of Executive Order: Whether the NPC support staff is created or the FBI's IPC takes on that role, there is the separate issue of whether to extend the Commission Transition Office and the current Advisory Committee while the new PDDs are coming into effect. The Staff Director has proposed that the Executive Order creating these organizations be amended to have an end date of September 30. This amendment would permit the staff to conclude the classification and distribution of their voluminous files and report, finalize on-going contract research, and respond to the numerous requests for information and briefings on the Commission. It would also extend the Advisory Committee until new appointments could be completed.

Withdrawal/Redaction Marker
Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
004c. memo	For VPOTUS et al - Presidential Decision Directive; 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 [12]

2006-0191-F
jp279

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