

FOIA MARKER

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

Collection/Record Group: Clinton Presidential Records
Subgroup/Office of Origin: Office of Science and Technology
Series/Staff Member:
Subseries:

OA/ID Number: 43311
FolderID:

Folder Title:
Executive Orders 13010 of 15 July 1996 and 13011 of 17 July 1996

Stack:	Row:	Section:	Shelf:	Position:
S	1	1	7	3

EXECUTIVE ORDER 13010 of July 15, 1996
(As amended by Executive Order 13025 of November 13, 1996;
Executive Order 13041 of April 3, 1997; and
Executive Order 13064 of October 11, 1997)

Critical Infrastructure Protection

Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government. Threats to these critical infrastructures fall into two categories: physical threats to tangible property ("physical threats"), and threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures ("cyber threats"). Because many of these critical infrastructures are owned and operated by the private sector, it is essential that the government and private sector work together to develop a strategy for protecting them and assuring their continued operation.

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

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

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

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

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

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

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

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

Sec. 3. *The Steering Committee of the President's Commission on Critical Infrastructure Protection.* A Steering Committee ("Steering Committee") shall oversee the work of the Commission on behalf of the Principals Committee. The Steering Committee shall comprise five members. Four of the members shall be appointed by the President, and the fifth member shall be the Chair of the Commission. Two of the members of the Committee shall be employees of the Executive Office of the President. The Steering Committee will receive regular reports on the progress of the Commission's work and approve the submission of reports to the Principals Committee.

Sec. 4. *Mission.* The Commission shall:

- (a) within 30 days of this order, produce a statement of its mission objectives, which will elaborate the general objectives set forth in this order, and a detailed schedule for addressing each mission objective, for approval by the Steering Committee;
- (b) identify and consult with: (i) elements of the public and private sectors that conduct, support, or contribute to infrastructure assurance; (ii) owners and operators of the critical infrastructures; and (iii) other elements of the public and private sectors, including the Congress, that have an interest in critical infrastructure assurance issues and that may have differing perspectives on these issues;
- (c) assess the scope and nature of the vulnerabilities of, and threats to, critical infrastructures;
- (d) determine what legal and policy issues are raised by efforts to protect critical infrastructures and assess how these issues should be addressed;

- (e) recommend a comprehensive national policy and implementation strategy for protecting critical infrastructures from physical and cyber threats and assuring their continued operation;
- (f) propose any statutory or regulatory changes necessary to effect its recommendations; and
- (g) produce reports and recommendations to the Steering Committee as they become available; it shall not limit itself to producing one final report.

Sec. 5. *Advisory Committee to the President's Commission on Critical Infrastructure Protection.*

- (a) The Commission shall receive advice from an advisory committee ("Advisory Committee") composed of no more than 20 individuals appointed by the President from the private and public sectors who are knowledgeable about critical infrastructures. The Advisory Committee shall advise the Commission on the subjects of the Commission's mission in whatever manner the Advisory Committee, the Commission Chair, and the Steering Committee deem appropriate.
- (b) A Chair or Co-Chairs shall be designated by the President from among the members of the Advisory Committee.
- (c) The Advisory Committee shall be established in compliance with the Federal Advisory Committee Act, as amended (5 U.S.C. App.). The Department of Defense shall perform the functions of the President under the Federal Advisory Committee Act for the Advisory Committee, except that of reporting to the Congress, in accordance with the guidelines and procedures established by the Administrator of General Services.

Sec. 6. *Administration.*

- (a) All executive departments and agencies shall cooperate with the Commission and provide such assistance, information, and advice to the Commission as it may request, to the extent permitted by law.
- (b) The Commission and the Advisory Committee may hold open and closed hearings, conduct inquiries, and establish subcommittees, as necessary.
- (c) Members of the Advisory Committee shall serve without compensation for their work on the Advisory Committee. While engaged in the work of the Advisory Committee, members may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in the government service.
- (d) To the extent permitted by law, and subject to the availability of appropriations, the Department of Defense shall provide the Commission and the Advisory Committee with administrative services, staff, other support services, and such funds as may be necessary for the performance of its functions and shall reimburse the executive branch components that provide representatives to the Commission for the compensation of those representatives.

(e) In order to augment the expertise of the Commission, the Department of Defense may, at the Commission's request, contract for the services of nongovernmental consultants who may prepare analyses, reports, background papers, and other materials for consideration by the Commission. In addition, at the Commission's request, executive departments and agencies shall request that existing Federal advisory committees consider and provide advice on issues of critical infrastructure protection, to the extent permitted by law.

(f) The Commission shall terminate 1 year and 90 days from the date of this order, unless extended by the President prior to that date. The Principals Committee, the Steering Committee, and the Advisory Committee shall terminate no later than March 15, 1998, and, upon submission of the Commission's report, shall review the report and prepare appropriate recommendations to the President.

(g) The person who served as Chair of the Commission may continue to be a member of the Steering Committee after termination of the Commission.

Sec. 7. *Review of Commission's Report.*

(a) Upon the termination of the Commission as set out in section 6(f) of this order, certain of the Commission's staff may be retained no later than March 15, 1998, solely to assist the Principals, Steering, and Advisory Committees in reviewing the Commission's report and preparing recommendations to the President. They shall act under the direction of the Steering Committee or its designated agent. The Department of Defense shall continue to provide funding and administrative support for the retained Commission staff.

(b) Pursuant to Executive Order 12958, I hereby designate the Executive Secretary of the National Security Council to exercise the authority to classify information originally as "Top Secret" with respect to the work of the Commission staff, the Principals Committee, the Steering Committee, the Advisory Committee, and the Infrastructure Protection Task Force.

Sec. 8. *Interim Coordinating Mission.*

(a) While the Commission is conducting its analysis and until the President has an opportunity to consider and act on its recommendations, there is a need to increase coordination of existing infrastructure protection efforts in order to better address, and prevent, crises that would have a debilitating regional or national impact. There is hereby established an Infrastructure Protection Task Force ("IPTF") within the Department of Justice, chaired by the Federal Bureau of Investigation, to undertake this interim coordinating mission.

(b) The IPTF will not supplant any existing programs or organizations.

(c) The Steering Committee shall oversee the work of the IPTF.

(d) The IPTF shall include at least one full-time member each from the Federal Bureau of Investigation, the Department of Defense, and the National Security Agency. It shall also receive part-time assistance from other executive branch departments and agencies. Members shall be

designated by their departments or agencies on the basis of their expertise in the protection of critical infrastructures. IPTF members' compensation shall be paid by their parent agency or department.

(e) The IPTF's function is to identify and coordinate existing expertise, inside and outside of the Federal Government, to:

- (i) provide, or facilitate and coordinate the provision of, expert guidance to critical infrastructures to detect, prevent, halt, or confine an attack and to recover and restore service;
- (ii) issue threat and warning notices in the event advance information is obtained about a threat;
- (iii) provide training and education on methods of reducing vulnerabilities and responding to attacks on critical infrastructures;
- (iv) conduct after-action analysis to determine possible future threats, targets, or methods of attack; and
- (v) coordinate with the pertinent law enforcement authorities during or after an attack to facilitate any resulting criminal investigation.

(f) All executive departments and agencies shall cooperate with the IPTF and provide such assistance, information, and advice as the IPTF may request, to the extent permitted by law.

(g) All executive departments and agencies shall share with the IPTF information about threats and warning of attacks, and about actual attacks on critical infrastructures, to the extent permitted by law.

(h) The IPTF shall terminate no later than 180 days after the termination of the Commission, unless extended by the President prior to that date.

Sec. 9. General.

(a) This order is not intended to change any existing statutes or Executive orders.

(b) This order is not intended to create any right, benefit, trust, or responsibility, substantive or procedural, enforceable at law or equity by a party against the United States, its agencies, its officers, or any person.

/s/ William J. Clinton

THE WHITE HOUSE,
July 15, 1996.

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release

July 17, 1996

EXECUTIVE ORDER 13011

- - - - -

FEDERAL INFORMATION TECHNOLOGY

A Government that works better and costs less requires efficient and effective information systems. The Paperwork Reduction Act of 1995 and the Information Technology Management Reform Act of 1996 provide the opportunity to improve significantly the way the Federal Government acquires and manages information technology. Agencies now have the clear authority and responsibility to make measurable improvements in mission performance and service delivery to the public through the strategic application of information technology. A coordinated approach that builds on existing structures and successful practices is needed to provide maximum benefit across the Federal Government from this technology.

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

Section 1. Policy. It shall be the policy of the United States Government that executive agencies shall: (a) significantly improve the management of their information systems, including the acquisition of information technology, by implementing the relevant provisions of the Paperwork Reduction Act of 1995 (Public Law 104-13), the Information Technology Management Reform Act of 1996 (Division E of Public Law 104-106) ("Information Technology Act"), and the Government Performance and Results Act of 1993 (Public Law 103-62);

(b) refocus information technology management to support directly their strategic missions, implement an investment review process that drives budget formulation and execution for information systems, and rethink and restructure the way they perform their functions before investing in information technology to support that work;

(c) establish clear accountability for information resources management activities by creating agency Chief Information Officers (CIOs) with the visibility and management responsibilities necessary to advise the agency head on the design, development, and implementation of those information systems. These responsibilities include: (1) participating in the investment review process for information systems; (2) monitoring and evaluating the performance of those information systems on the basis of applicable performance measures; and, (3) as necessary, advising the agency head to modify or terminate those systems;

(d) cooperate in the use of information technology to improve the productivity of Federal programs and to promote a coordinated, interoperable, secure, and shared Governmentwide infrastructure that is provided and supported by a diversity of private sector suppliers and a well-trained corps of information technology professionals; and

(e) establish an interagency support structure that builds on existing successful interagency efforts and shall provide expertise and advice to agencies; expand the skill and career development opportunities of information technology professionals; improve the management and use of information technology within and among agencies by developing information technology procedures and standards and by identifying and sharing experiences, ideas, and promising practices; and provide innovative, multi-disciplinary, project-specific support to agencies to enhance interoperability, minimize unnecessary duplication of effort, and capitalize on agency successes.

Sec. 2. Responsibilities of Agency Heads. The head of each executive agency shall: (a) effectively use information technology to improve mission performance and service to the public;

(b) strengthen the quality of decisions about the employment of information resources to meet mission needs through integrated analysis, planning, budgeting, and evaluation processes, including:

(1) determining, before making investments in new information systems, whether the Government should be performing the function, if the private sector or another agency should support the function, and if the function needs to be or has been appropriately redesigned to improve its efficiency;

(2) establishing mission-based performance measures for information systems investments, aligned with agency performance plans prepared pursuant to the Government Performance and Results Act of 1993 (Public Law 103-62);

(3) establishing agency-wide and project-level management structures and processes responsible and accountable for managing, selecting, controlling, and evaluating investments in information systems, with authority for terminating information systems when appropriate;

(4) supporting appropriate training of personnel; and

(5) seeking the advice of, participating in, and supporting the interagency support structure set forth in this order;

(c) select CIOs with the experience and skills necessary to accomplish the duties set out in law and policy, including this order, and involve the CIO at the highest level of the agency in the processes and decisions set out in this section;

(d) ensure that the information security policies, procedures, and practices of the executive agency are adequate;

(e) where appropriate, and in accordance with the Federal Acquisition Regulation and guidance to be issued by the Office of Management and Budget (OMB), structure major information systems investments into manageable projects as narrow in scope and brief in duration as practicable, consistent with the Information Technology Act, to reduce risk, promote flexibility and interoperability, increase accountability, and better correlate mission need with current technology and market conditions; and

(f) to the extent permitted by law, enter into a contract that provides for multiagency acquisitions of information technology as an executive agent for the Government, if and in the manner that the Director of OMB considers it advantageous to do so.

Sec. 3. Chief Information Officers Council. (a) Purpose and

Functions. A Chief Information Officers Council ("CIO Council") is established as the principal interagency forum to improve agency practices on such matters as the design, modernization, use, sharing, and performance of agency information resources. The Council shall:

- (1) develop recommendations for overall Federal information technology management policy, procedures, and standards;
- (2) share experiences, ideas, and promising practices, including work process redesign and the development of performance measures, to improve the management of information resources;
- (3) identify opportunities, make recommendations for, and sponsor cooperation in using information resources;
- (4) assess and address the hiring, training, classification, and professional development needs of the Federal Government with respect to information resources management;
- (5) make recommendations and provide advice to appropriate executive agencies and organizations, including advice to OMB on the Governmentwide strategic plan required by the Paperwork Reduction Act of 1995; and
- (6) seek the views of the Chief Financial Officers Council, Government Information Technology Services Board, Information Technology Resources Board, Federal Procurement Council, industry, academia, and State and local governments on matters of concern to the Council as appropriate.

(b) Membership. The CIO Council shall be composed of the CIOs and Deputy CIOs of the following executive agencies plus two representatives from other agencies:

1. Department of State;
2. Department of the Treasury;
3. Department of Defense;
4. Department of Justice;
5. Department of the Interior;
6. Department of Agriculture;
7. Department of Commerce;
8. Department of Labor;
9. Department of Health and Human Services;
10. Department of Housing and Urban Development;
11. Department of Transportation;
12. Department of Energy;
13. Department of Education;
14. Department of Veterans Affairs;
15. Environmental Protection Agency;

16. Federal Emergency Management Agency;
17. Central Intelligence Agency;
18. Small Business Administration;
19. Social Security Administration;
20. Department of the Army;
21. Department of the Navy;
22. Department of the Air Force;
23. National Aeronautics and Space Administration;
24. Agency for International Development;
25. General Services Administration;
26. National Science Foundation;
27. Nuclear Regulatory Commission; and
28. Office of Personnel Management.

The Administrator of the Office of Information and Regulatory Affairs of OMB, the Controller of the Office of Federal Financial Management of OMB, the Administrator of the Office of Federal Procurement Policy of OMB, a Senior Representative of the Office of Science and Technology Policy, the Chair of the Government Information Technology Services Board, and the Chair of the Information Technology Resources Board shall also be members. The CIO Council shall be chaired by the Deputy Director for Management of OMB. The Vice Chair, elected by the CIO Council on a rotating basis, shall be an agency CIO.

Sec. 4. Government Information Technology Services Board.

(a) Purpose and Functions. A Government Information Technology Services Board ("Services Board") is established to ensure continued implementation of the information technology recommendations of the National Performance Review and to identify and promote the development of innovative technologies, standards, and practices among agencies and State and local governments and the private sector. It shall seek the views of experts from industry, academia, and State and local governments on matters of concern to the Services Board as appropriate. The Services Board shall also make recommendations to the agencies, the CIO Council, OMB, and others as appropriate, and assist in the following:

(1) creating opportunities for cross-agency cooperation and intergovernmental approaches in using information resources to support common operational areas and to develop and provide shared governmentwide infrastructure services;

(2) developing shared governmentwide information infrastructure services to be used for innovative, multiagency information technology projects;

(3) creating and utilizing affinity groups for particular business or technology areas; and

(4) developing with the National Institute of Standards and Technology and with established standards bodies, standards and

guidelines pertaining to Federal information systems, consistent with the limitations contained in the Computer Security Act of 1987 (40 U.S.C. 759 note), as amended by the Information Technology Act.

(b) Membership. The Services Board shall be composed of individuals from agencies based on their proven expertise or accomplishments in fields necessary to achieve its goals. Major government mission areas such as electronic benefits, electronic commerce, law enforcement, environmental protection, national defense, and health care may be represented on the Services Board to provide a program operations perspective. Initial selection of members will be made by OMB in consultation with other agencies as appropriate. The CIO Council may nominate two members. The Services Board shall recommend new members to OMB for consideration. The Chair will be elected by the Services Board.

Sec. 5. Information Technology Resources Board.

(a) Purpose and Functions. An Information Technology Resources Board ("Resources Board") is established to provide independent assessments to assist in the development, acquisition, and management of selected major information systems and to provide recommendations to agency heads and OMB as appropriate. The Resources Board shall:

(1) review, at the request of an agency and OMB, specific information systems proposed or under development and make recommendations to the agency and OMB regarding the status of systems or next steps;

(2) publicize lessons learned and promising practices based on information systems reviewed by the Board; and

(3) seek the views of experts from industry, academia, and State and local governments on matters of concern to the Resources Board, as appropriate.

(b) Membership. The Resources Board shall be composed of individuals from executive branch agencies based on their knowledge of information technology, program, or acquisition management within Federal agencies. Selection of members shall be made by OMB in consultation with other agencies as appropriate. The Chair will be elected by the Resources Board. The Resources Board may call upon the department or agency whose project is being reviewed, or any other department or agency to provide knowledgeable representative(s) to the Board whose guidance and expertise will assist in focusing on the primary issue(s) presented by a specific system.

Sec. 6. Office of Management and Budget. The Director of OMB shall:

(1) evaluate agency information resources management practices and, as part of the budget process, analyze, track and evaluate the risks and results of all major capital investments for information systems;

(2) notify an agency if it believes that a major information system requires outside assistance;

(3) provide guidance on the implementation of this order and on the management of information resources to the executive agencies and to the Boards established by this order; and

(4) evaluate the effectiveness of the management structure set out in this order after 3 years and make recommendations for any appropriate changes.

Sec. 7. General Services Administration. Under the direction of OMB, the Administrator of General Services shall:

(1) continue to manage the FTS2000 program and coordinate the follow-on to that program, on behalf of and with the advice of customer agencies;

(2) develop, maintain, and disseminate for the use of the Federal community, as requested by OMB or the agencies, recommended methods and strategies for the development and acquisition of information technology;

(3) conduct and manage outreach programs in cooperation with agency managers;

(4) be a focal point for liaison on information resources management, including Federal information technology, with State and local governments, and with nongovernmental international organizations subject to prior consultation with the Secretary of State to ensure such liaison would be consistent with and support overall United States foreign policy objectives;

(5) support the activities of the Secretary of State for liaison, consultation, and negotiation with intergovernmental organizations in information resources management matters;

(6) assist OMB, as requested, in evaluating agencies' performance-based management tracking systems and agencies' achievement of cost, schedule, and performance goals; and

(7) provide support and assistance to the interagency groups established in this order.

Sec. 8. Department of Commerce. The Secretary of Commerce shall carry out the standards responsibilities under the Computer Security Act of 1987, as amended by the Information Technology Act, taking into consideration the recommendations of the agencies, the CIO Council, and the Services Board.

Sec. 9. Department of State. (a) The Secretary of State shall be responsible for liaison, consultation, and negotiation with foreign governments and intergovernmental organizations on all matters related to information resources management, including Federal information technology. The Secretary shall further ensure, in consultation with the Secretary of Commerce, that the United States is represented in the development of international standards and recommendations affecting information technology. In the exercise of these responsibilities, the Secretary shall consult, as appropriate, with affected domestic agencies, organizations, and other members of the public.

(b) The Secretary of State shall advise the Director on the development of United States positions and policies on international information policy and technology issues affecting Federal Government activities and the development of international information technology standards.

Sec. 10. Definitions. (a) "Executive agency" has the meaning given to that term in section 4(1) of the Office of Federal Procurement Policy Act (41 U.S.C. 403(1)).

(b) "Information Technology" has the meaning given that term in section 5002 of the Information Technology Act.

(c) "Information resources" has the meaning given that term in section 3502(6) of title 44, United States Code.

(d) "Information resources management" has the meaning given that term in section 3502(7) of title 44, United States Code.

(e) "Information system" has the meaning given that term in section 3502(8) of title 44, United States Code.

(f) "Affinity group" means any interagency group focussed on a business or technology area with common information technology or customer requirements. The functions of an affinity group can include identifying common program goals and requirements; identifying opportunities for sharing information to improve quality and effectiveness; reducing costs and burden on the public; and recommending protocols and other standards, including security standards, to the National Institute of Standards and Technology for Governmentwide applicability, for action in accordance with the Computer Security Act of 1987, as amended by the Information Technology Act.

(g) "National security system" means any telecommunications or information system operated by the United States Government, the function, operation, or use of which (1) involves intelligence activities; (2) involves cryptologic activities related to national security; (3) involves command and control of military forces; (4) involves equipment that is an integral part of a weapon or weapons system; or (5) is critical to the direct fulfillment of military or intelligence missions, but excluding any system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

Sec. 11. Applicability to National Security Systems.

The heads of executive agencies shall apply the policies and procedures established in this order to national security systems in a manner consistent with the applicability and related limitations regarding such systems set out in the Information Technology Act.

Sec. 12. Judicial Review. Nothing in this Executive order shall affect any otherwise available judicial review of agency action. This Executive order is intended only to improve the internal management of the executive branch and does not create any right or benefit, substantive or procedural, enforceable at law or equity by a party against the United States, its agencies or instrumentalities, its officers or employees, or any other person.

WILLIAM J. CLINTON

THE WHITE HOUSE,
July 16, 1996.

#