Federal Register

Thursday,
October 18, 2001

Part VI

The President

Executive Order 13231—Critical Infrastructure Protection in the Information Age

Federal Register
Vol. 66, No. 202
Thursday, October 18, 2001

Presidential Documents

Title 3—

The President

Executive Order 13231 of October 16, 2001

Critical Infrastructure Protection in the Information Age

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to ensure protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems, in the information age, it is hereby ordered as follows:

Section 1. *Policy.*

(a) The information technology revolution has changed the way business is transacted, government operates, and national defense is conducted. Those three functions now depend on an interdependent network of critical information infrastructures. The protection program authorized by this order shall consist of continuous efforts to secure information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems. Protection of these systems is essential to the telecommunications, energy, financial services, manufacturing, water, transportation, health care, and emergency services sectors.

(b) It is the policy of the United States to protect against disruption of the operation of information systems for critical infrastructure and thereby help to protect the people, economy, essential human and government services, and national security of the United States, and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible. The implementation of this policy shall include a voluntary public-private partnership, involving corporate and nongovernmental organizations.

Sec. 2. *Scope.* To achieve this policy, there shall be a senior executive branch board to coordinate and have cognizance of Federal efforts and programs that relate to protection of information systems and involve:

(a) cooperation with and protection of private sector critical infrastructure, State and local governments' critical infrastructure, and supporting programs in corporate and academic organizations;

(b) protection of Federal departments' and agencies' critical infrastructure; and

(c) related national security programs.

Sec. 3. *Establishment.* I hereby establish the ''President's Critical Infrastructure Protection Board'' (the ''Board'').

Sec. 4. *Continuing Authorities.* This order does not alter the existing authorities or roles of United States Government departments and agencies. Authorities set forth in 44 U.S.C. Chapter 35, and other applicable law, provide senior officials with responsibility for the security of Federal Government information systems.

(a) *Executive Branch Information Systems Security.* The Director of the Office of Management and Budget (OMB) has the responsibility to develop and oversee the implementation of government-wide policies, principles, standards, and guidelines for the security of information systems that support the executive branch departments and agencies, except those noted in section 4(b) of this order. The Director of OMB shall advise the President and the appropriate department or agency head when there is a critical deficiency in the security practices within the purview of this section in an executive branch department or agency. The Board shall assist and support the Director

of OMB in this function and shall be reasonably cognizant of programs related to security of department and agency information systems.

(b) *National Security Information Systems.* The Secretary of Defense and the Director of Central Intelligence (DCI) shall have responsibility to oversee, develop, and ensure implementation of policies, principles, standards, and guidelines for the security of information systems that support the operations under their respective control. In consultation with the Assistant to the President for National Security Affairs and the affected departments and agencies, the Secretary of Defense and the DCI shall develop policies, principles, standards, and guidelines for the security of national security information systems that support the operations of other executive branch departments and agencies with national security information.

(i) Policies, principles, standards, and guidelines developed under this subsection may require more stringent protection than those developed in accordance with subsection 4(a) of this order.

(ii) The Assistant to the President for National Security Affairs shall advise the President and the appropriate department or agency head when there is a critical deficiency in the security practices of a department or agency within the purview of this section. The Board, or one of its standing or ad hoc committees, shall be reasonably cognizant of programs to provide security and continuity to national security information systems.

(c) *Additional Responsibilities: The Heads of Executive Branch Departments and Agencies.* The heads of executive branch departments and agencies are responsible and accountable for providing and maintaining adequate levels of security for information systems, including emergency preparedness communications systems, for programs under their control. Heads of such departments and agencies shall ensure the development and, within available appropriations, funding of programs that adequately address these mission areas. Cost-effective security shall be built into and made an integral part of government information systems, especially those critical systems that support the national security and other essential government programs. Additionally, security should enable, and not unnecessarily impede, department and agency business operations.

Sec. 5. *Board Responsibilities.* Consistent with the responsibilities noted in section 4 of this order, the Board shall recommend policies and coordinate programs for protecting information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems. Among its activities to implement these responsibilities, the Board shall:

(a) *Outreach to the Private Sector and State and Local Governments.* In consultation with affected executive branch departments and agencies, coordinate outreach to and consultation with the private sector, including corporations that own, operate, develop, and equip information, telecommunications, transportation, energy, water, health care, and financial services, on protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems; and coordinate outreach to State and local governments, as well as communities and representatives from academia and other relevant elements of society.

(i) When requested to do so, assist in the development of voluntary standards and best practices in a manner consistent with 15 U.S.C. Chapter 7;

(ii) Consult with potentially affected communities, including the legal, auditing, financial, and insurance communities, to the extent permitted by law, to determine areas of mutual concern; and

(iii) Coordinate the activities of senior liaison officers appointed by the Attorney General, the Secretaries of Energy, Commerce, Transportation, the Treasury, and Health and Human Services, and the Director of the Federal Emergency Management Agency for outreach on critical infrastructure protection issues with private sector organizations within the areas of concern to these departments and agencies. In these and other related functions, the Board shall work in coordination with the Critical Infrastructure Assurance Office (CIAO) and the National Institute of Standards and Technology of the Department of Commerce, the National Infrastructure Protection Center (NIPC), and the National Communications System (NCS).

(b) *Information Sharing.* Work with industry, State and local governments, and nongovernmental organizations to ensure that systems are created and well managed to share threat warning, analysis, and recovery information among government network operation centers, information sharing and analysis centers established on a voluntary basis by industry, and other related operations centers. In this and other related functions, the Board shall work in coordination with the NCS, the Federal Computer Incident Response Center, the NIPC, and other departments and agencies, as appropriate.

(c) *Incident Coordination and Crisis Response.* Coordinate programs and policies for responding to information systems security incidents that threaten information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems. In this function, the Department of Justice, through the NIPC and the Manager of the NCS and other departments and agencies, as appropriate, shall work in coordination with the Board.

(d) *Recruitment, Retention, and Training Executive Branch Security Professionals.* In consultation with executive branch departments and agencies, coordinate programs to ensure that government employees with responsibilities for protecting information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems, are adequately trained and evaluated. In this function, the Office of Personnel Management shall work in coordination with the Board, as appropriate.

(e) *Research and Development.* Coordinate with the Director of the Office of Science and Technology Policy (OSTP) on a program of Federal Government research and development for protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems, and ensure coordination of government activities in this field with corporations, universities, Federally funded research centers, and national laboratories. In this function, the Board shall work in coordination with the National Science Foundation, the Defense Advanced Research Projects Agency, and with other departments and agencies, as appropriate.

(f) *Law Enforcement Coordination with National Security Components.* Promote programs against cyber crime and assist Federal law enforcement agencies in gaining necessary cooperation from executive branch departments and agencies. Support Federal law enforcement agencies' investigation of illegal activities involving information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems, and support coordination by these agencies with other departments and agencies with responsibilities to defend the Nation's security. In this function, the Board shall work in coordination with the Department of Justice, through the NIPC, and the Department of the Treasury, through the Secret Service, and with other departments and agencies, as appropriate.

(g) *International Information Infrastructure Protection.* Support the Department of State's coordination of United States Government programs for international cooperation covering international information infrastructure protection issues.

(h) *Legislation.* In accordance with OMB circular A–19, advise departments and agencies, the Director of OMB, and the Assistant to the President for Legislative Affairs on legislation relating to protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems.

(i) *Coordination with Office of Homeland Security.* Carry out those functions relating to protection of and recovery from attacks against information systems for critical infrastructure, including emergency preparedness communications, that were assigned to the Office of Homeland Security by Executive Order 13228 of October 8, 2001. The Assistant to the President for Homeland Security, in coordination with the Assistant to the President for National Security Affairs, shall be responsible for defining the responsibilities of the Board in coordinating efforts to protect physical assets that support information systems.

Sec. 6. *Membership.* (a) Members of the Board shall be drawn from the executive branch departments, agencies, and offices listed below; in addition, concerned Federal departments and agencies may participate in the activities of appropriate committees of the Board. The Board shall be led by a Chair and Vice Chair, designated by the President. Its other members shall be the following senior officials or their designees:

(i) Secretary of State;

(ii) Secretary of the Treasury;

(iii) Secretary of Defense;

(iv) Attorney General;

(v) Secretary of Commerce;

(vi) Secretary of Health and Human Services;

(vii) Secretary of Transportation;

(viii) Secretary of Energy;

(ix) Director of Central Intelligence;

(x) Chairman of the Joint Chiefs of Staff;

(xi) Director of the Federal Emergency Management Agency;

(xii) Administrator of General Services;

(xiii) Director of the Office of Management and Budget;

(xiv) Director of the Office of Science and Technology Policy;

(xv) Chief of Staff to the Vice President;

(xvi) Director of the National Economic Council;

(xvii) Assistant to the President for National Security Affairs;

(xviii) Assistant to the President for Homeland Security;

(xix) Chief of Staff to the President; and

(xx) Such other executive branch officials as the President may designate.

Members of the Board and their designees shall be full-time or permanent part-time officers or employees of the Federal Government.

(b) In addition, the following officials shall serve as members of the Board and shall form the Board's Coordination Committee:

(i) Director, Critical Infrastructure Assurance Office, Department of Commerce;
(ii) Manager, National Communications System;
(iii) Vice Chair, Chief Information Officers' (CIO) Council;
(iv) Information Assurance Director, National Security Agency;
(v) Deputy Director of Central Intelligence for Community Management; and
(vi) Director, National Infrastructure Protection Center, Federal Bureau of Investigation, Department of Justice.

(c) The Chairman of the Federal Communications Commission may appoint a representative to the Board.

Sec. 7. *Chair.* (a) The Chair also shall be the Special Advisor to the President for Cyberspace Security. Executive branch departments and agencies shall make all reasonable efforts to keep the Chair fully informed in a timely manner, and to the greatest extent permitted by law, of all programs and issues within the purview of the Board. The Chair, in consultation with the Board, shall call and preside at meetings of the Board and set the agenda for the Board. The Chair, in consultation with the Board, may propose policies and programs to appropriate officials to ensure the protection of the Nation's information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems. To ensure full coordination between the responsibilities of the National Security Council (NSC) and the Office of Homeland Security, the Chair shall report to both the Assistant to the President for National Security Affairs and to the Assistant to the President for Homeland Security. The Chair shall coordinate with the Assistant to the President for Economic Policy on issues relating to private sector systems and economic effects and with the Director of OMB on issues relating to budgets and the security of computer networks addressed in subsection 4(a) of this order.

(b) The Chair shall be assisted by an appropriately sized staff within the White House Office. In addition, heads of executive branch departments and agencies are authorized, to the extent permitted by law, to detail or assign personnel of such departments and agencies to the Board's staff upon request of the Chair, subject to the approval of the Chief of Staff to the President. Members of the Board's staff with responsibilities relating to national security information systems, communications, and information warfare may, with respect to those responsibilities, also work at the direction of the Assistant to the President for National Security Affairs.

Sec. 8. *Standing Committees.* (a) The Board may establish standing and ad hoc committees as appropriate. Representation on standing committees shall not be limited to those departments and agencies on the Board, but may include representatives of other concerned executive branch departments and agencies.

(b) Chairs of standing and ad hoc committees shall report fully and regularly on the activities of the committees to the Board, which shall ensure that the committees are well coordinated with each other.

(c) There are established the following standing committees:

(i) *Private Sector and State and Local Government Outreach*, chaired by the designee of the Secretary of Commerce, to work in coordination with the designee of the Chairman of the National Economic Council.

(ii) *Executive Branch Information Systems Security*, chaired by the designee of the Director of OMB. The committee shall assist OMB in fulfilling its responsibilities under 44 U.S.C. Chapter 35 and other applicable law.

(iii) *National Security Systems.* The National Security Telecommunications and Information Systems Security Committee, as established by and consistent with NSD–42 and chaired by the Department of Defense, shall serve as a Board standing committee, and be redesignated the Committee on National Security Systems.

(iv) *Incident Response Coordination*, co-chaired by the designees of the Attorney General and the Secretary of Defense.

(v) *Research and Development*, chaired by a designee of the Director of OSTP.

(vi) *National Security and Emergency Preparedness Communications.* The NCS Committee of Principals is renamed the Board's Committee for National Security and Emergency Preparedness Communications. The reporting functions established above for standing committees are in addition to the functions set forth in Executive Order 12472 of April 3, 1984, and do not alter any function or role set forth therein.

(vii) *Physical Security*, co-chaired by the designees of the Secretary of Defense and the Attorney General, to coordinate programs to ensure the physical security of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems. The standing committee shall coordinate its work with the Office of Homeland Security and shall work closely with the Physical Security Working Group of the Records Access and Information Security Policy Coordinating Committee to ensure coordination of efforts.

(viii) *Infrastructure Interdependencies*, co-chaired by the designees of the Secretaries of Transportation and Energy, to coordinate programs to assess the unique risks, threats, and vulnerabilities associated with the interdependency of information systems for critical infrastructures, including the development of effective models, simulations, and other analytic tools and cost-effective technologies in this area.

(ix) *International Affairs*, chaired by a designee of the Secretary of State, to support Department of State coordination of United States Government programs for international cooperation covering international information infrastructure issues.

(x) *Financial and Banking Information Infrastructure*, chaired by a designee of the Secretary of the Treasury and including representatives of the banking and financial institution regulatory agencies.

(xi) *Other Committees*. Such other standing committees as may be established by the Board.

(d) *Subcommittees.* The chair of each standing committee may form necessary subcommittees with organizational representation as determined by the Chair.

(e) *Streamlining.* The Board shall develop procedures that specify the manner in which it or a subordinate committee will perform the responsibilities previously assigned to the Policy Coordinating Committee. The Board, in coordination with the Director of OSTP, shall review the functions of the Joint Telecommunications Resources Board, established under Executive Order 12472, and make recommendations about its future role.

Sec. 9. *Planning and Budget.* (a) The Board, on a periodic basis, shall propose a National Plan or plans for subjects within its purview. The Board, in coordination with the Office of Homeland Security, also shall make recommendations to OMB on those portions of executive branch department and agency budgets that fall within the Board's purview, after review of relevant program requirements and resources.

(b) The Office of Administration within the Executive Office of the President shall provide the Board with such personnel, funding, and administrative support, to the extent permitted by law and subject to the availability of appropriations, as directed by the Chief of Staff to carry out the provisions of this order. Only those funds that are available for the Office of Homeland Security, established by Executive Order 13228, shall be available for such purposes. To the extent permitted by law and as appropriate, agencies represented on the Board also may provide administrative support for the Board. The National Security Agency shall ensure that the Board's information and communications systems are appropriately secured.

(c) The Board may annually request the National Science Foundation, Department of Energy, Department of Transportation, Environmental Protection Agency, Department of Commerce, Department of Defense, and the Intelligence Community, as that term is defined in Executive Order 12333

of December 4, 1981, to include in their budget requests to OMB funding for demonstration projects and research to support the Board's activities.

Sec. 10. *Presidential Advisory Panels.* The Chair shall work closely with panels of senior experts from outside of the government that advise the President, in particular: the President's National Security Telecommunications Advisory Committee (NSTAC) created by Executive Order 12382 of September 13, 1982, as amended, and the National Infrastructure Advisory Council (NIAC or Council) created by this Executive Order. The Chair and Vice Chair of these two panels also may meet with the Board, as appropriate and to the extent permitted by law, to provide a private sector perspective.

(a) *NSTAC.* The NSTAC provides the President advice on the security and continuity of communications systems essential for national security and emergency preparedness.

(b) *NIAC.* There is hereby established the National Infrastructure Advisory Council, which shall provide the President advice on the security of information systems for critical infrastructure supporting other sectors of the economy: banking and finance, transportation, energy, manufacturing, and emergency government services. The NIAC shall be composed of not more than 30 members appointed by the President. The members of the NIAC shall be selected from the private sector, academia, and State and local government. Members of the NIAC shall have expertise relevant to the functions of the NIAC and generally shall be selected from industry Chief Executive Officers (and equivalently ranked leaders in other organizations) with responsibilities for the security of information infrastructure supporting the critical sectors of the economy, including banking and finance, transportation, energy, communications, and emergency government services. Members shall not be full-time officials or employees of the executive branch of the Federal Government.

(i) The President shall designate a Chair and Vice Chair from among the members of the NIAC.

(ii) The Chair of the Board established by this order will serve as the Executive Director of the NIAC.

(c) *NIAC Functions.* The NIAC will meet periodically to:

(i) enhance the partnership of the public and private sectors in protecting information systems for critical infrastructures and provide reports on this issue to the President, as appropriate;

(ii) propose and develop ways to encourage private industry to perform periodic risk assessments of critical information and telecommunications systems;

(iii) monitor the development of private sector Information Sharing and Analysis Centers (ISACs) and provide recommendations to the Board on how these organizations can best foster improved cooperation among the ISACs, the NIPC, and other Federal Government entities;

(iv) report to the President through the Board, which shall ensure appropriate coordination with the Assistant to the President for Economic Policy under the terms of this order; and

(v) advise lead agencies with critical infrastructure responsibilities, sector coordinators, the NIPC, the ISACs, and the Board.

(d) *Administration of the NIAC.*

(i) The NIAC may hold hearings, conduct inquiries, and establish subcommittees, as appropriate.

(ii) Upon the request of the Chair, and to the extent permitted by law, the heads of the executive branch departments and agencies shall provide the Council with information and advice relating to its functions.

(iii) Senior Federal Government officials may participate in the meetings of the NIAC, as appropriate.

(iv) Members shall serve without compensation for their work on the Council. However, members may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in Federal Government service (5 U.S.C. 5701–5707).

(v) To the extent permitted by law, and subject to the availability of appropriations, the Department of Commerce, through the CIAO, shall provide the NIAC with administrative services, staff, and other support services and such funds as may be necessary for the performance of the NIAC's functions.

(e) *General Provisions.*

(i) Insofar as the Federal Advisory Committee Act, as amended (5 U.S.C. App.), may apply to the NIAC, the functions of the President under that Act, except that of reporting to the Congress, shall be performed by the Department of Commerce in accordance with the guidelines and procedures established by the Administrator of General Services.

(ii) The Council shall terminate 2 years from the date of this order, unless extended by the President prior to that date.

(iii) Executive Order 13130 of July 14, 1999, is hereby revoked.

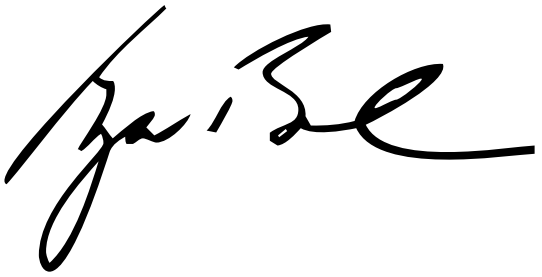
Sec. 11. *National Communications System.* Changes in technology are causing the convergence of much of telephony, data relay, and internet communications networks into an interconnected network of networks. The NCS and its National Coordinating Center shall support use of telephony, converged information, voice networks, and next generation networks for emergency preparedness and national security communications functions assigned to them in Executive Order 12472. All authorities and assignments of responsibilities to departments and agencies in that order, including the role of the Manager of NCS, remain unchanged except as explicitly modified by this order.

Sec. 12. *Counter-intelligence.* The Board shall coordinate its activities with those of the Office of the Counter-intelligence Executive to address the threat to programs within the Board's purview from hostile foreign intelligence services.

Sec. 13. *Classification Authority.* I hereby delegate to the Chair the authority to classify information originally as Top Secret, in accordance with Executive Order 12958 of April 17, 1995, as amended, or any successor Executive Order.

Sec. 14. *General Provisions.* (a) Nothing in this order shall supersede any requirement made by or under law.

(b) This order does not create any right or benefit, substantive or procedural, enforceable at law or equity, against the United States, its departments, agencies or other entities, its officers or employees, or any other person.



THE WHITE HOUSE,
October 16, 2001.

[FR Doc. 01–26509
Filed 10–17–01; 10:32 am]
Billing code 3195–01–P