

cies and procedures adopted by the agency to honor them; and

(d) ensure that the policies, procedures, and practices of the agency related to copyrights protecting computer software are adequate and fully implement the policies set forth in this order.

SEC. 3. *Chief Information Officers Council.* The Chief Information Officers Council (“Council”) established by section 3 of Executive Order No. 13011 of July 16, 1996 [set out above], shall be the principal interagency forum to improve executive agency practices regarding the acquisition and use of computer software, and monitoring and combating the use of unauthorized computer software. The Council shall provide advice and make recommendations to executive agencies and to the Office of Management and Budget regarding appropriate government-wide measures to carry out this order. The Council shall issue its initial recommendations within 6 months of the date of this order.

SEC. 4. *Office of Management and Budget.* The Director of the Office of Management and Budget, in carrying out responsibilities under the Clinger-Cohen Act [probably means the Clinger-Cohen Act of 1996, div. D (§§4001-4402) and div. E (§§5001-5703) of Pub. L. 104-106, see Tables for classification], shall utilize appropriate oversight mechanisms to foster agency compliance with the policies set forth in this order. In carrying out these responsibilities, the Director shall consider any recommendations made by the Council under section 3 of this order regarding practices and policies to be instituted on a government-wide basis to carry out this order.

SEC. 5. *Definition.* “Executive agency” and “agency” have the meaning given to that term in section 4(1) of the Office of Federal Procurement Policy Act (41 U.S.C. 403(1)).

SEC. 6. *National Security.* In the interest of national security, nothing in this order shall be construed to require the disclosure of intelligence sources or methods or to otherwise impair the authority of those agencies listed at [former] 50 U.S.C. 401a(4) [now 50 U.S.C. 3003(4)] to carry out intelligence activities.

SEC. 7. *Law Enforcement Activities.* Nothing in this order shall be construed to require the disclosure of law enforcement investigative sources or methods or to prohibit or otherwise impair any lawful investigative or protective activity undertaken for or by any officer, agent, or employee of the United States or any person acting pursuant to a contract or other agreement with such entities.

SEC. 8. *Scope.* Nothing in this order shall be construed to limit or otherwise affect the interpretation, application, or operation of 28 U.S.C. 1498.

SEC. 9. *Judicial Review.* 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, 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.

§ 11102. Sense of Congress

It is the sense of Congress that, during the five-year period beginning with 1996, executive agencies should achieve each year through improvements in information resources management by the agency—

(1) at least a five percent decrease in the cost (in constant fiscal year 1996 dollars) incurred by the agency in operating and maintaining information technology; and

(2) a five percent increase in the efficiency of the agency operations.

(Pub. L. 107-217, Aug. 21, 2002, 116 Stat. 1236.)

HISTORICAL AND REVISION NOTES

Revised Section	Source (U.S. Code)	Source (Statutes at Large)
11102	40:1442.	Pub. L. 104-106, div. E, title LI, §5132, Feb. 10, 1996, 110 Stat. 689.

§ 11103. Applicability to national security systems

(a) DEFINITION.—

(1) NATIONAL SECURITY SYSTEM.—In this section, the term “national security system” means a telecommunications or information system operated by the Federal Government, the function, operation, or use of which—

(A) involves intelligence activities;

(B) involves cryptologic activities related to national security;

(C) involves command and control of military forces;

(D) involves equipment that is an integral part of a weapon or weapons system; or

(E) subject to paragraph (2), is critical to the direct fulfillment of military or intelligence missions.

(2) LIMITATION.—Paragraph (1)(E) does not include a system to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

(b) IN GENERAL.—Except as provided in subsection (c), chapter 113 of this title does not apply to national security systems.

(c) EXCEPTIONS.—

(1) IN GENERAL.—Sections 11313, 11315, and 11316 of this title apply to national security systems.

(2) CAPITAL PLANNING AND INVESTMENT CONTROL.—The heads of executive agencies shall apply sections 11302 and 11312 of this title to national security systems to the extent practicable.

(3) APPLICABILITY OF PERFORMANCE-BASED AND RESULTS-BASED MANAGEMENT TO NATIONAL SECURITY SYSTEMS.—

(A) IN GENERAL.—Subject to subparagraph (B), the heads of executive agencies shall apply section 11303 of this title to national security systems to the extent practicable.

(B) EXCEPTION.—National security systems are subject to section 11303(b)(5) of this title, except for subparagraph (B)(iv).

(Pub. L. 107-217, Aug. 21, 2002, 116 Stat. 1236.)

HISTORICAL AND REVISION NOTES

Revised Section	Source (U.S. Code)	Source (Statutes at Large)
11103(a)	40:1452.	Pub. L. 104-106, div. E, title LI, §§5141, 5142, Feb. 10, 1996, 110 Stat. 689.
11103(b)	40:1451(a).	
11103(c)	40:1451(b).	

EXEMPTION FROM REQUIREMENT FOR CAPITAL PLANNING AND INVESTMENT CONTROL FOR INFORMATION TECHNOLOGY EQUIPMENT INCLUDED AS INTEGRAL PART OF A WEAPON OR WEAPON SYSTEM

Pub. L. 114-328, div. A, title VIII, §895, Dec. 23, 2016, 130 Stat. 2326, provided that:

“(a) WAIVER AUTHORITY.—Notwithstanding subsection (c)(2) of section 11103 of title 40, United States

Code, a national security system described in subsection (a)(1)(D) of such section shall not be subject to the requirements of paragraphs (2) through (5) of section 11312(b) of such title unless the milestone decision authority determines in writing that application of such requirements is appropriate and in the best interests of the Department of Defense.

“(b) MILESTONE DECISION AUTHORITY DEFINED.—In this section, the term ‘milestone decision authority’ has the meaning given the term in section 2366a(d)(7) of title 10, United States Code.”

CHAPTER 113—RESPONSIBILITY FOR ACQUISITIONS OF INFORMATION TECHNOLOGY

SUBCHAPTER I—DIRECTOR OF OFFICE OF MANAGEMENT AND BUDGET

Sec.

- 11301. Responsibility of Director.
- 11302. Capital planning and investment control.
- 11303. Performance-based and results-based management.

SUBCHAPTER II—EXECUTIVE AGENCIES

- 11311. Responsibilities.
- 11312. Capital planning and investment control.
- 11313. Performance and results-based management.
- 11314. Authority to acquire and manage information technology.
- 11315. Agency Chief Information Officer.
- 11316. Accountability.
- 11317. Significant deviations.
- 11318. Interagency support.
- 11319. Resources, planning, and portfolio management.

SUBCHAPTER III—OTHER RESPONSIBILITIES

- 11331. Responsibilities for Federal information systems standards.
- [11332. Repealed.]

AMENDMENTS

2014—Pub. L. 113–291, div. A, title VIII, §831(b), Dec. 19, 2014, 128 Stat. 3440, added item 11319.

2002—Pub. L. 107–296, title X, §§1002(b), 1005(a)(2), Nov. 25, 2002, 116 Stat. 2269, 2272, and Pub. L. 107–347, title III, §§302(b), 305(a), Dec. 17, 2002, 116 Stat. 2957, 2960, amended table of sections identically, substituting “Responsibilities for Federal information systems standards” for “Responsibilities regarding efficiency, security, and privacy of federal computer systems” in item 11331 and striking out item 11332 “Federal computer system security training and plan”.

SUBCHAPTER I—DIRECTOR OF OFFICE OF MANAGEMENT AND BUDGET

§ 11301. Responsibility of Director

In fulfilling the responsibility to administer the functions assigned under chapter 35 of title 44, the Director of the Office of Management and Budget shall comply with this chapter with respect to the specific matters covered by this chapter.

(Pub. L. 107–217, Aug. 21, 2002, 116 Stat. 1237.)

HISTORICAL AND REVISION NOTES

<i>Revised Section</i>	<i>Source (U.S. Code)</i>	<i>Source (Statutes at Large)</i>
11301	40:1411.	Pub. L. 104–106, div. E, title LI, §5111, Feb. 10, 1996, 110 Stat. 680.

MODERNIZING GOVERNMENT TECHNOLOGY

Pub. L. 115–91, div. A, title X, subtitle G, Dec. 12, 2017, 131 Stat. 1586, provided that:

“SEC. 1076. DEFINITIONS.

“In this subtitle:

“(1) ADMINISTRATOR.—The term ‘Administrator’ means the Administrator of General Services.

“(2) BOARD.—The term ‘Board’ means the Technology Modernization Board established under section 1094(c)(1).

“(3) CLOUD COMPUTING.—The term ‘cloud computing’ has the meaning given the term by the National Institute of Standards and Technology in NIST Special Publication 800–145 and any amendatory or superseding document thereto.

“(4) DIRECTOR.—The term ‘Director’ means the Director of the Office of Management and Budget.

“(5) FUND.—The term ‘Fund’ means the Technology Modernization Fund established under section 1094(b)(1) [probably should be “1078(b)(1)”].

“(6) INFORMATION TECHNOLOGY.—The term ‘information technology’ has the meaning given the term in section 3502 of title 44, United States Code.

“(7) IT WORKING CAPITAL FUND.—The term ‘IT working capital fund’ means an information technology system modernization and working capital fund established under section 1093(b)(1) [probably should be “1077(b)(1)”].

“(8) LEGACY INFORMATION TECHNOLOGY SYSTEM.—The term ‘legacy information technology system’ means an outdated or obsolete system of information technology.

“SEC. 1077. ESTABLISHMENT OF AGENCY INFORMATION TECHNOLOGY SYSTEMS MODERNIZATION AND WORKING CAPITAL FUNDS.

“(a) DEFINITION.—In this section, the term ‘covered agency’ means each agency listed in section 901(b) of title 31, United States Code.

“(b) INFORMATION TECHNOLOGY SYSTEM MODERNIZATION AND WORKING CAPITAL FUNDS.—

“(1) ESTABLISHMENT.—The head of a covered agency may establish within the covered agency an information technology system modernization and working capital fund for necessary expenses described in paragraph (3).

“(2) SOURCE OF FUNDS.—The following amounts may be deposited into an IT working capital fund:

“(A) Reprogramming and transfer of funds made available in appropriations Acts enacted after the date of enactment of this Act [Dec. 12, 2017], including the transfer of any funds for the operation and maintenance of legacy information technology systems, in compliance with any applicable reprogramming law or guidelines of the Committees on Appropriations of the Senate and the House of Representatives or transfer authority specifically provided in appropriations law.

“(B) Amounts made available to the IT working capital fund through discretionary appropriations made available after the date of enactment of this Act.

“(3) USE OF FUNDS.—An IT working capital fund established under paragraph (1) may only be used—

“(A) to improve, retire, or replace existing information technology systems in the covered agency to enhance cybersecurity and to improve efficiency and effectiveness across the life of a given workload, procured using full and open competition among all commercial items to the greatest extent practicable;

“(B) to transition legacy information technology systems at the covered agency to commercial cloud computing and other innovative commercial platforms and technologies, including those serving more than 1 covered agency with common requirements;

“(C) to assist and support covered agency efforts to provide adequate, risk-based, and cost-effective information technology capabilities that address evolving threats to information security;

“(D) to reimburse funds transferred to the covered agency from the Fund with the approval of the