

1 The Office of Management and Budget (OMB) is proposing to revise Circular No, A-130,  
2 Management of Federal Information Resources, (hereinafter, Circular A-130, or the Circular) in  
3 light of changes that have taken place in statute for information policy and information  
4 technology (including privacy and security) since the Circular was last revised in November  
5 2000.

6 It has been the policy of the United States Government to support the development and use of  
7 efficient and effective information technology and information policy approaches that, when  
8 adopted by Federal agencies, can address important regulatory, procurement, or policy  
9 objectives. OMB is revising Circular A-130 to provide guidance that is timely and relevant to  
10 agency operations in a current, interconnected, ever-changing information resources  
11 environment. This revision is being conducted to incorporate revised and new statutory policy,  
12 technological advancements and enhanced technological capabilities, as well as current and  
13 evolving technical and personnel security threats. Agencies are asked to incorporate this  
14 guidance into their policies, understanding that the subject nature of this document will demand  
15 agencies continually reassess, reexamine, and reevaluate their information resources  
16 management policies and strategies.

17 This Circular establishes general policy for the acquisition and management of information  
18 technology personnel, equipment, funds, and other resources. It also includes a discussion of  
19 agency responsibilities for managing personally identifiable information, provides guidance on  
20 use of electronic transactions and related electronic documentation statutes, and discusses policy  
21 on protecting Federal information resources as appendices. Although this Circular touches on  
22 many specific issues such as privacy, confidentiality, information quality, dissemination, and  
23 statistical policy, those topics are covered more fully in other OMB policies, which are available  
24 on the OMB website at <https://www.whitehouse.gov/omb/>.

25 In this notice, OMB is seeking comment on proposed revisions to this Circular. These revisions  
26 reflect the experience gained by OMB and agencies in implementing the Circular since 2000.  
27 The revisions were undertaken by examining the Circular in its current form, and attempting to  
28 highlight any areas where either the guidance was duplicative, accepted as common practice as  
29 to no longer need specific instruction, or failed to address a specific issue area that had  
30 developed since previous publication. The Circular was examined concurrent with its appendices  
31 to ensure the broader direction of the Circular was complimented by the specificity of the  
32 appendices. The document's language is designed for the guidance to maintain a timeless  
33 characteristic, not immediately becoming outdated or irrelevant.

34 In the main body of the Circular, OMB proposes additional language on the purpose of the  
35 Circular and amends the authorities section to more fully cover existing statutes and Executive  
36 Orders.

37 In the Applicability section of the main body, OMB has simplified the reference to national  
38 security systems by removing "Information classified for national security purposes should also  
39 be handled in accordance with the appropriate national security directives. National security  
40 emergency preparedness activities should be conducted in accordance with Executive Order No.

41 12472” and replacing it with “For national security systems, agencies should follow applicable  
42 laws, Executive Orders, and directives.”

43 OMB has revised the background section of the main body to better articulate agency  
44 responsibilities in this area.

45 In the Definitions Section, OMB has proposed several changes.

46 OMB is proposing to delete the following definitions – “audiovisual production”, “full costs”,  
47 “Information Technology Resources Board”, “information processing services organization”,  
48 “major information system” and “service recipient”, as they are no longer needed for the  
49 purposes of this Circular.

50 The term “government information” has been removed because it is not used in this Circular.  
51 The term “Federal information” has been added to the Definitions section because it is a  
52 commonly used term in statute and is used throughout this Circular.

53 Several new definitions are proposed for inclusion in the Circular including – “confidentiality”,  
54 “digital services”, “enterprise architecture”, “Federal information system”, “information  
55 security”, “information technology resources”, “interagency agreement”, “major information  
56 technology investment”, “open data”, “personally identifiable information” and “senior agency  
57 official for privacy”.

58 The Circular also proposes to modify the definitions for “agency”, “capital planning and  
59 investment control process”, “information resources”, “information resources management”,  
60 “information system”, “information system life cycle”, “information technology”, “the CIO  
61 Council”, and “dissemination”, to be consistent with current guidance and statute.

62 Section 6, Basic Considerations and Assumptions and Section 7, Policy have been revised to  
63 incorporate both policy and statute changes since the Circular was last revised.

64 Section 8 of the Circular designates responsibilities first, government-wide and then specifically  
65 agency-by-agency. The section incorporates additional statutory requirements enacted since the  
66 last revision of the Circular in 2000.

67 Appendix I, previously titled Federal Agency Responsibilities for Maintaining Records About  
68 Individuals, is being revised to provide guidance to Federal agencies on their responsibilities for  
69 managing information resources that involve personally identifiable information (PII). The  
70 previous version of Appendix I described agency responsibilities for implementing the reporting  
71 and publication requirements of the Privacy Act of 1974, as amended (5 U.S.C. § 552a). This  
72 information is being revised and reconstituted as OMB Circular No. A-108, Federal Agency  
73 Responsibilities for Review, Reporting, and Publication under the Privacy Act. The revised  
74 Appendix I, titled Responsibilities for Management of Personally Identifiable Information,  
75 provides guidance on Federal agencies’ responsibilities for protecting PII – including PII  
76 collected for statistical purposes under a pledge of confidentiality – and describes a set of fair  
77 information practice principles (FIPPs) that Federal agencies should consult when managing

78 information resources that involve PII. Finally, Appendix I requires Federal agencies to  
79 implement the privacy controls in National Institute of Standards and Technology (NIST)  
80 Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and  
81 Organizations. Additional guidance on implementing the NIST SP 800-53 privacy controls is  
82 provided in Circular No. A-130, Appendix III, Responsibilities for Protecting Federal  
83 Information Resources.

84 Appendix II, previously titled Implementation of the Government Paperwork Elimination Act, is  
85 being revised to reference requirements of the Electronic Signatures in Global and National  
86 Commerce Act (E-Sign Act). The Government Paperwork Elimination Act (GPEA) and E-Sign  
87 Act are both important tools to improve customer service and governmental efficiency through  
88 the use of information technology. In addition to providing reference to the E-Sign Act and more  
89 recent guidance, such as the “Federal Chief Information Officers’ Council, Use of Electronic  
90 Signatures in Federal Organization Transactions” (dated January 2013), this appendix has been  
91 significantly pared down. For example, OMB M-00-10 attachment entitled “OMB Procedures  
92 and Guidance on Implementing the Government Paperwork Elimination Act” has been removed  
93 and included as a reference. The Background section has been revised to make the information  
94 more current and remove historical information not relevant to the current update. For example,  
95 summaries of public comments received on OMB’s draft GPEA guidance of 2000 have been  
96 removed, as well as outdated references to GAO and NIST publications.

97 Appendix III, previously titled Security of Federal Automated Information Resources, is being  
98 revised to establish new requirements for information security and privacy management, to  
99 incorporate new mandates in the Federal Information Security Modernization Act of 2014, and to  
100 ensure consistency with OMB policies and NIST Federal Information Processing Standards and  
101 800-series publications. In short, the revised Appendix III provides guidance on how agencies  
102 should take a coordinated approach to information security and privacy when protecting Federal  
103 information resources. As a result, the title of the Appendix has been changed to Responsibilities  
104 for Protecting Federal Information Resources. The proposed revisions provide guidance on  
105 agency information security and privacy management, including the transition from the current  
106 static, point-in-time authorization process to a more dynamic continuous monitoring and ongoing  
107 authorization process for information systems and common controls. Examples of additional  
108 requirements included in the revised Appendix III focus on incident response, encryption,  
109 inclusion of security requirements in contracts, oversight of contractors, protecting against  
110 insider threats, protecting against supply chain risks, prohibiting unsupported software and  
111 system components, and holding personnel accountable.

112 In addition, the revised Appendix III clarifies the role of the senior agency official for privacy  
113 (SAOP) in the NIST Risk Management Framework. In accordance with existing OMB policies,  
114 the Appendix explains that the SAOP has overall responsibility and accountability for  
115 implementing privacy protections and ensuring that all privacy requirements are met.  
116 Accordingly, the SAOP is responsible for developing and implementing a privacy continuous  
117 monitoring strategy, reviewing and approving the categorization of information systems,  
118 designating privacy controls, reviewing and approving the privacy plan, conducting privacy  
119 control assessments, and reviewing authorization packages for information systems.

120 **CIRCULAR NO. A-130**

121 **Proposed**

122 **TO THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES**

123 **SUBJECT:** Management of Federal Information Resources

- 124 1. Purpose
- 125 2. Authorities
- 126 3. Applicability
- 127 4. Background
- 128 5. Definitions
- 129 6. Basic Considerations and Assumptions
- 130 7. Policy
- 131 8. Assignment of Responsibilities
- 132 9. Effectiveness
- 133 10. Oversight
- 134 11. Inquiries

135 Appendix I, Responsibilities for Management of Personally Identifiable Information

136 Appendix II, Guidance on Electronic Transactions

137 Appendix III, Responsibilities for Protecting Federal Information Resources

138 **1. Purpose**

139 This Circular establishes general policy for the acquisition and management of personnel,  
140 equipment, funds, and information technology resources that support the quality, design,  
141 collection, processing, editing, compilation, storage, transmission, analysis, release,  
142 dissemination, accessibility, maintenance, information security, cataloguing, sharing, and  
143 disposition of Federal information. It also includes responsibilities for managing personally  
144 identifiable information, requirements for implementing the Government Paperwork Elimination  
145 Act and related electronic documentation statutes, and policy on protecting Federal resources as  
146 appendices. Although this Circular touches on many specific issues such as privacy,  
147 confidentiality, information quality, dissemination, and statistical policy, those topics are covered  
148 more fully in other Office of Management and Budget (OMB) policies, which are available on  
149 the OMB website.

150 **2. Authorities**

151 OMB issues this Circular pursuant to the following statutes and Executive Orders:

- 152 a. Budget and Accounting Procedures Act of 1950, as amended (31 U.S.C. Chapter 11);
- 153 b. Chief Financial Officers Act (31 U.S.C. 3512 et seq.);
- 154 c. Clinger-Cohen Act (also known as the "Information Technology Management Reform Act of  
155 1996") (Pub. L. 104-106, Division E);
- 156 d. Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA);
- 157 e. Digital Accountability and Transparency Act of 2014;
- 158 f. E-Government Act of 2002 (Pub. L. 107-347);
- 159 g. Federal Acquisition Streamlining Act of 1994;
- 160 h. Federal Information Security Modernization Act of 2014;
- 161 i. Federal Information Technology Acquisition Reform Act (FITARA);
- 162 j. Federal Property and Administrative Services Act of 1940, as amended (40 U.S.C. 487);
- 163 k. Federal Records Act of 1950, as amended, codified (44 U.S.C. Chapter 29, 31, 33);
- 164 l. Freedom of Information Act;
- 165 m. Government Paperwork Elimination Act of 1998 (Pub. L. 105-277, Title XVII);
- 166 n. Government Performance and Results Act (GPRA) of 1993, as amended by the Government  
167 Performance and Results Modernization Act (GPRM) of 2010 (Pub. L. 111-352);
- 168 o. Information Quality Act;
- 169 p. Office of Federal Procurement Policy Act (41 U.S.C. Chapter 7);
- 170 q. Paperwork Reduction Act (PRA) of 1980, as amended by the Paperwork Reduction Act of  
171 1995 (44 U.S.C. Chapter 35);
- 172 r. Privacy Act of 1974, as amended (5 U.S.C. 552a);

- 173 s. Section 508 of the Rehabilitation Act of 1973 (as amended (Pub. L. 105-220, 29 U.S.C.  
174 794d);
- 175 t. Executive Order No. 12046, Relating to the Transfer of Telecommunications Functions, of  
176 March 27, 1978;
- 177 u. Executive Order No. 12472, Assignment of National Security and Emergency Preparedness  
178 Telecommunications Functions, of April 3, 1984; and
- 179 v. Other relevant statutes and Executive Orders.

### 180 **3. Applicability**

- 181 a. The requirements of this Circular apply to the information resources management activities  
182 of all agencies of the Executive Branch of the Federal Government; and
- 183 b. The requirements of this Circular do not apply to national security systems. For national  
184 security systems, agencies should follow applicable laws, Executive Orders, and directives.

### 185 **4. Background**

186 The Paperwork Reduction Act, Government Paperwork Elimination Act, Clinger-Cohen Act, E-  
187 Government Act of 2002, and Federal Information Technology Acquisition Reform Act establish  
188 a comprehensive approach for executive agencies to improve the acquisition and management of  
189 their information resources, by:

- 190 a. Establishing a broad mandate for agencies to perform their information resources  
191 management activities in an efficient, effective, economical, secure, and privacy-enhancing  
192 manner;
- 193 b. Focusing information resources planning to support their strategic missions;
- 194 c. Implementing a Capital Planning and Investment Control (CPIC) process that links to and  
195 supports budget formulation and execution; and
- 196 d. Rethinking and restructuring the way agencies do their work before investing in information  
197 systems.

### 198 **5. Definitions**

- 199 a. ‘Agency’ means any executive department, military department, Government corporation,  
200 Government-controlled corporation, or other establishment in the Executive Branch of the  
201 Government (including the Executive Office of the President), or any independent regulatory  
202 agency, but does not include: (i) the Government Accountability Office; (ii) the Federal  
203 Election Commission; (iii) the governments of the District of Columbia and of the territories  
204 and possessions of the United States, and their various subdivisions; or (iv) Government-  
205 owned, contractor-operated facilities, including laboratories engaged in national defense  
206 research and production activities (44 U.S.C., Sec. 3502).
- 207 b. ‘Capital Planning and Investment Control Process’ (CPIC) means a decision-making process  
208 that ensures that IT investments integrate strategic planning, budgeting, procurement, and  
209 management of IT in support of agency missions and business needs. The CPIC process has  
210 three distinct phases: Select, Control, and Evaluate. See 40 U.S.C 11302 and the Clinger-  
211 Cohen Act of 1996 for statutory requirements.

- 212 c. ‘Chief Information Officer’ (CIO) means the senior official that, pursuant to the Clinger-  
213 Cohen Act, provides advice and other assistance to the head of the executive agency and  
214 other senior management personnel of the executive agency to ensure that information  
215 technology is acquired and information resources are managed for the executive agency in a  
216 manner that achieves the agency’s strategic goals and information resources management  
217 goals (40 USC 11315).
- 218 d. ‘Chief Information Officers Council’ (CIO Council) means the Council codified in the E-  
219 Government Act of 2002 (Pub. L. 107-347).
- 220 e. ‘Confidentiality’ means preserving authorized restrictions on access and disclosure, including  
221 means for protecting personal privacy and proprietary information (44 U.S.C. § 3542(b)(B)).
- 222 f. ‘Digital services’ means the software and related technology the Federal Government  
223 provides for the public to access a service of the Federal Government, or software and  
224 technology that is custom-built on behalf of the Federal Government to directly support the  
225 delivery of a service of the Federal Government to the public.
- 226 g. ‘Dissemination’ means the government-initiated distribution of information to a  
227 nongovernment entity, including the public. Not considered dissemination within the  
228 meaning of this Circular is distribution limited to government employees, intra- or  
229 interagency use or sharing of government information, and responses to requests for agency  
230 records under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act (5 U.S.C.  
231 552a). (Note: For purposes of the Privacy Act and other privacy requirements, the term  
232 “dissemination” has a different meaning.)
- 233 h. ‘Enterprise architecture’ (a) means – (i) a strategic information asset base, which defines the  
234 mission; (ii) the information necessary to perform the mission; (iii) the technologies  
235 necessary to perform the mission; and (iv) the transitional processes for implementing new  
236 technologies in response to changing mission needs; and (b) includes – (i) a baseline  
237 architecture; (ii) a target architecture; and (iii) a sequencing plan.
- 238 i. ‘Executive agency’ has the meaning defined in Title 41, Public Contracts section 133 (41  
239 U.S.C. 133).
- 240 j. ‘Federal Information’ means information created, collected, processed, maintained, used,  
241 disseminated, or disposed of by or for the Federal Government, in any medium or form.
- 242 k. ‘Federal information system’ means an information system used or operated by an executive  
243 agency, by a contractor of an executive agency, or by another organization on behalf of an  
244 executive agency (40 U.S.C., Sec. 11331).
- 245 l. ‘Government publication’ means information that is published as an individual document at  
246 government expense, or as required by law, in any medium or form (44 U.S.C. 1901).
- 247 m. ‘Information’ means any communication or representation of knowledge such as facts, data,  
248 or opinions in any medium or form, including textual, numerical, graphic, cartographic,  
249 narrative, electronic, or audiovisual forms.
- 250 n. ‘Information dissemination product’ means any book, paper, map, machine-readable  
251 material, electronic file, audiovisual production, or other documentary material, regardless of  
252 form or characteristic, disseminated by an agency to the public.

- 253 o. ‘Information life cycle’ means the stages through which information passes, typically  
254 characterized as creation or collection, processing, dissemination, use, storage, and  
255 disposition, to include destruction and deletion.
- 256 p. ‘Information management’ means the planning, budgeting, manipulating, controlling, and  
257 processing of information throughout its life cycle.
- 258 q. ‘Information resources’ means information and related resources, such as personnel,  
259 equipment, funds, and information technology (44 U.S.C. 3502).
- 260 r. ‘Information resources management’ means the process of managing information resources  
261 to accomplish agency missions. The term encompasses both information itself and the related  
262 resources, such as personnel, equipment, funds, and information technology (44 U.S.C.  
263 3502).
- 264 s. ‘Information security’ means the protection of information and information systems from  
265 unauthorized access, use, disclosure, disruption, modification, or destruction in order to  
266 provide --
- 267 1) Integrity, which means guarding against improper information modification or  
268 destruction, and includes ensuring information nonrepudiation and authenticity;
- 269 2) Confidentiality, which means preserving authorized restrictions on access and  
270 disclosure, including means for protecting personal privacy and proprietary information;  
271 and
- 272 3) Availability, which means ensuring timely and reliable access to and use of information  
273 (44 U.S.C. 3542).
- 274 t. ‘Information system’ means a discrete set of information resources organized for the  
275 collection, processing, maintenance, use, sharing, dissemination, or disposition of  
276 information (44 U.S.C. 3502).
- 277 u. ‘Information system life cycle’ means all phases in the useful life of an information system,  
278 including planning, acquiring, operating, maintaining, and disposing. See also OMB A-11  
279 Part 7 “Capital Programming Guide” and OMB Circular A-131 “Value Engineering” for  
280 more information regarding the costs and management of assets through their complete life  
281 cycle.
- 282 v. ‘Information technology’ means any services or equipment, or interconnected system(s) or  
283 subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis,  
284 evaluation, manipulation, management, movement, control, display, switching, interchange,  
285 transmission, or reception of data or information by the agency. For purposes of this  
286 definition, such services or equipment is used by an agency if used by the agency directly or  
287 is used by a contractor under a contract with the agency that requires its use; or to a  
288 significant extent, its use in the performance of a service or the furnishing of a product. The  
289 term “information technology” includes computers, ancillary equipment (including imaging  
290 peripherals, input, output, and storage devices necessary for security and surveillance),  
291 peripheral equipment designed to be controlled by the central processing unit of a computer,  
292 software, firmware and similar procedures, services (including cloud computing and help-  
293 desk services or other professional services which support any point of the life cycle of the  
294 equipment or service), and related resources. The term “information technology” does not

295 include any equipment that is acquired by a contractor incidental to a contract which does not  
296 require its use (40 U.S.C. 11101).

297 w. ‘Information technology resources’ means all agency budgetary resources, personnel,  
298 equipment, facilities, or services that are primarily used in the management, operation,  
299 acquisition, or other activity related to the life cycle of information technology; acquisitions  
300 or interagency agreements which include information technology and the services or  
301 equipment provided by such acquisitions or interagency agreements; but does not include  
302 grants which establish or support information technology not operated directly by the Federal  
303 Government.

304 x. ‘Interagency agreement’ means, for the purposes of this document, a written agreement  
305 entered into between two Federal agencies that specifies the goods to be furnished or tasks to  
306 be accomplished by one agency (the servicing agency) in support of the other (the requesting  
307 agency), including assisted acquisitions as described in OMB Memorandum: *Improving the*  
308 *Management and Use of Interagency Acquisitions* and other cases described in FAR Part 17.

309 y. ‘Major information technology investment’ means an investment that requires special  
310 management attention as defined in OMB guidance and agency policies, a “major automated  
311 information system” as defined in 10 U.S.C. 2445, or a major acquisition as defined in the  
312 OMB Circular A-11 Capital Programming Guide consisting of information resources.

313 z. ‘National security system’ means any information system (including any telecommunications  
314 system) used or operated by an agency or by a contractor of an agency, or other organization  
315 on behalf of an agency: (i) the function, operation, or use of which involves intelligence  
316 activities; involves cryptologic activities related to national security; involves command and  
317 control of military forces; involves equipment that is an integral part of a weapon or  
318 weapons system; or is critical to the direct fulfillment of military or intelligence missions  
319 (excluding a system that is to be used for routine administrative and business applications,  
320 for example, payroll, finance, logistics, and personnel management applications); or (ii) is  
321 protected at all times by procedures established for information that have been specifically  
322 authorized under criteria established by an Executive Order or an Act of Congress to be kept  
323 classified in the interest of national defense or foreign policy (44 U.S.C. 3542).

324 aa. ‘Open data’ means publicly available data structured in a way that enables the data to be fully  
325 discoverable and usable by end users. Generally, open data are public, accessible, machine-  
326 readable, described, reusable, complete, timely, and managed in manners consistent with  
327 OMB guidance defining these terms, including relevant privacy, confidentiality, security,  
328 and other valid restrictions.

329 bb. ‘Personally identifiable information’ (PII) means information that can be used to distinguish  
330 or trace an individual’s identity, either alone or when combined with other personal or  
331 identifying information that is linked or linkable to a specific individual. To determine  
332 whether information is PII, agencies must perform an assessment of the specific risk that an  
333 individual can be identified. In performing this assessment, it is important to recognize that  
334 non-identifiable information can become PII whenever additional information becomes  
335 available – in any medium and from any source – that would make it possible to identify an  
336 individual.

- 337 cc. ‘Records’ means all books, papers, maps, photographs, machine-readable materials, or other  
338 documentary materials, regardless of physical form or characteristics, made or received by  
339 an agency of the United States Government under Federal law or in connection with the  
340 transaction of public business and preserved or appropriate for preservation by that agency  
341 or its legitimate successor as evidence of the organization, functions, policies, decisions,  
342 procedures, operations, or other activities of the Government or because of the informational  
343 value of the data in them. Library and museum material made or acquired and preserved  
344 solely for reference or exhibition purposes, extra copies of documents preserved only for  
345 convenience of reference, and stocks of publications and of processed documents are not  
346 included (44 U.S.C. 3301). (Note: For purposes of the Privacy Act, the term ‘Record’ has a  
347 different meaning.)
- 348 dd. ‘Records management’ means the planning, controlling, directing, organizing, training,  
349 promoting, and other managerial activities involved with respect to records creation, records  
350 maintenance and use, and records disposition in order to achieve adequate and proper  
351 documentation of the policies and transactions of the Federal Government and effective and  
352 economical management of agency operations (44 U.S.C. 2901(2)).
- 353 ee. ‘Senior Agency Official for Privacy’ (SAOP) means the senior official, designated by the  
354 head of each agency, who has overall agency-wide responsibility for information privacy,  
355 including implementation of information privacy protections, compliance with Federal laws,  
356 regulations, and policies relating to information privacy, and a central policy-making role in  
357 the agency’s development and evaluation of legislative, regulatory, and other policy  
358 proposals.

## 359 **6. Basic Considerations and Assumptions**

- 360 a. Government information is both a strategic asset and a valuable national resource. It enables  
361 the performance of effective government missions and programs and provides the public with  
362 knowledge of the government, society, and economy – past, present, and future. It is a means  
363 to ensure the accountability of government, to manage the government's operations, to  
364 maintain and enhance the healthy performance of the economy, and is itself a commodity in  
365 the marketplace.
- 366 b. Information technology is not an end in itself. Its role is in support of agency missions and  
367 programs and cannot be planned or managed independently from agency missions, priorities,  
368 and program needs.
- 369 c. The Federal Government’s success in achieving the overall goals of its missions and  
370 programs depends on effective and efficient support by information resources, information  
371 technology, digital services, and related resources.
- 372 d. Openness in government strengthens our democracy. Government agencies have a  
373 responsibility to be open, transparent, and accountable to the public.
- 374 e. Managing government information as an asset to promote openness and interoperability,  
375 subject to applicable restrictions, increases operational efficiencies, reduces costs, improves  
376 services, supports mission needs, safeguards personally identifiable information, and  
377 increases public access to valuable government information.

- 378 f. Agencies must have information security programs that consider the risks and range of  
379 threats to their data and implement controls to mitigate those risks to acceptable levels.
- 380 g. The individual's right to privacy must be considered and protected throughout the  
381 information life cycle in Federal Government information activities involving personally  
382 identifiable information.
- 383 h. Making information resources easy to find, accessible, and usable can fuel entrepreneurship,  
384 innovation, and scientific discovery that improves the lives of Americans and contributes  
385 significantly to job creation.
- 386 i. Agencies must make information accessible to employees and members of the public with  
387 disabilities in compliance with Section 508 of the Rehabilitation Act of 1973, as amended.
- 388 j. The open and efficient exchange of scientific and technical government information, subject  
389 to applicable security and privacy controls and the proprietary rights of others, fosters  
390 excellence in scientific research and effective use of Federal research and development  
391 funds.
- 392 k. The Government must balance the utility of information against the burden imposed on the  
393 public and the cost of its collection.
- 394 l. Information quality is a key parameter of information utility. The rigor of information  
395 collection design should be consistent with the likely use of the information. Quality  
396 standards provide established means to evaluate rigor.
- 397 m. Federal Government collection and dissemination of information must be done pursuant to  
398 applicable statutory requirements and conform to information quality standards established  
399 by the Federal Government. These standards include, among others, statistical directives,  
400 policy guidelines, and best practices. The degree to which the information collection must  
401 conform to Federal standards should be consistent with the likely use of the information.
- 402 n. When the Federal Government disseminates information, it must be done pursuant to  
403 applicable statutory requirements and accompanied with sufficient detail about the collection  
404 design and resulting quality parameters (e.g., response rates) for the public to determine the  
405 fitness of the information for a given use.
- 406 o. The Nation can benefit from Government information disseminated by diverse nonfederal  
407 parties, including State and local government agencies, educational and other not-for-profit  
408 institutions, and for-profit organizations.
- 409 p. The protection of confidential statistical or trade secret information as required by statute  
410 must be upheld in Federal Government information activities throughout the information life  
411 cycle.
- 412 q. Systematic attention to the management of Government records from creation to disposition  
413 is an essential component of sound information resources management that ensures public  
414 accountability. Together with records preservation, it protects the Government's historical  
415 record and safeguards the legal and financial rights of the Government and the public.
- 416 r. Because State, local, tribal, and territorial governments are important producers of  
417 government information for many areas such as health, social welfare, labor, transportation,  
418 and education, the Federal Government should cooperate with these governments in the

419 management of information resources. Federal Government information resources  
420 management policies and activities can affect, and be affected by, the information policies  
421 and activities of other nations.

422 s. Effective information management practices in times of limited budgetary resources depend  
423 on the strategic management of personnel, equipment, and information technology.

## 424 7. Policy

425 a. Ensuring Effective Information Resources Planning and Management

426 1) When planning, budgeting, and executing Government programs and services, agencies  
427 shall take explicit account of information resources and information technology (IT)  
428 assets, personnel, and policies.

429 2) Agencies shall manage information throughout its life cycle, including information  
430 collection, processing, maintenance, storage, use, sharing, dissemination, and  
431 disposition. In doing so, agencies shall:

432 a) Collect or create and disseminate information in a way that is open and supports  
433 downstream interoperability among information systems and dissemination of  
434 information to the public, as appropriate, without the need for costly retrofitting, to  
435 the extent permitted by law and subject to privacy, confidentiality, security, and  
436 other valid restrictions;

437 b) Protect the individual's right to privacy, ensure confidentiality, and have information  
438 security and privacy programs that consider the risks and range of threats to their  
439 data;

440 c) Consider target audiences of Government information when determining format,  
441 frequency of update, and other information management decisions;

442 d) Consider the impact of decisions and actions in each stage of the information life  
443 cycle on other stages;

444 e) Consider the effects of information management actions on members of the public  
445 and State, local, tribal and territorial governments and their access to Government  
446 information and ensure consultation with the public and those governments as  
447 appropriate;

448 f) Seek to satisfy new information needs through interagency or intergovernmental  
449 sharing of information, or through nongovernmental sources, where lawful and  
450 appropriate, before creating or collecting new information;

451 g) Provide training to personnel involved in information resources management;

452 h) Protect Government information commensurate with the risk that could result from  
453 unauthorized access, use, disclosure, disruption, modification, or destruction of such  
454 information;

455 i) Consult National Institute of Standards and Technology (NIST) Federal Information  
456 Processing Standards (FIPS), and NIST Special Publications (SPs) (e.g., 500 and 800  
457 series guidelines);

- 458 j) Collect, record, preserve, and make accessible sufficient information to ensure the  
459 management and accountability of agency programs, and to protect the legal and  
460 financial rights of the Federal Government;
- 461 k) Consider the effects of their actions on accessibility of technology for Federal  
462 employees and members of the public with disabilities and comply with Section 508  
463 of the Rehabilitation Act of 1973, as amended (Pub. L. 105-220, 29 U.S.C. 794d);
- 464 l) Make their information publicly accessible to the extent permitted by law and subject  
465 to privacy, confidentiality, security, and other valid restrictions, and maintain a  
466 public inventory of their information to provide the public an efficient way to  
467 discover and access agencies' publicly available information;
- 468 m) Collect or create only that information necessary for the proper performance of  
469 authorized agency functions and that has practical utility;
- 470 n) Comply with the Privacy Act of 1974, the privacy provisions of the E-Government  
471 Act of 2002, other applicable laws, and all OMB policies on privacy;
- 472 o) Comply with the Confidential Information Protection provisions of Title IV of the E-  
473 Government Act of 2002 and OMB guidance on implementing the Confidential  
474 Information Protection provisions of the E-Government Act of 2002;
- 475 p) Comply with the Information Quality Act and OMB implementing guidance;
- 476 q) Comply with OMB Statistical Policy Directives issued under Section 3504 of the  
477 PRA; and
- 478 r) Executive agencies under Sections 1703 and 1705 of the Government Paperwork  
479 Elimination Act (GPEA), P. L. 105-277, Title XVII, are required to provide:
- 480 (i) The option of the electronic maintenance, submission, or disclosure of  
481 information, when practicable as a substitute for paper; and
- 482 (ii) The use and acceptance of electronic signatures, when practicable. Agencies  
483 shall follow the provisions in OMB memoranda on implementing requirements  
484 of the Government Paperwork Elimination Act.

485 b. Information Resources Management (IRM) Strategic Plan

486 In support of agency missions and business needs, as part of the agency's overall strategic  
487 and performance planning processes, agencies shall have an IRM Strategic Plan that  
488 describes the agency's technology and information resources goals, including but not limited  
489 to the processes described in c.-i. below. The IRM Strategic Plan shall show how these goals  
490 map to the agency's mission and organizational priorities. These goals should be specific,  
491 verifiable, and quantitatively measurable, so that progress against these goals can be tracked.  
492 The agency should review its IRM Strategic Plan annually alongside the Annual Performance  
493 Plan reviews to determine if there are any performance gaps or changes to mission needs,  
494 priorities or goals. The IRM Strategic Plan should be updated each year to incorporate  
495 necessary changes, and any annual updates should be publicly posted on the agency's  
496 website in conjunction with the Agency Strategic Plan. The associated materials shall be  
497 provided to OMB upon request.

498 c. Implementing Records Management

- 499 1) Agencies shall ensure that records management programs provide adequate and proper  
500 documentation of agency activities.
- 501 2) Agencies shall ensure the ability to access and retrieve records throughout their life cycle  
502 regardless of form or medium.
- 503 3) Agencies shall, in a timely fashion, establish, and obtain the approval of the Archivist of  
504 the United States for retention schedules for Federal records.
- 505 4) Agencies shall provide training and guidance as appropriate to all agency officials and  
506 employees and contractors regarding their Federal records management responsibilities.
- 507 d. Providing Information to the Public
- 508 1) Agencies shall make information resources accessible, discoverable, and usable by the  
509 public to the extent permitted by law and subject to privacy, confidentiality, security and  
510 other valid restrictions.
- 511 2) Agencies have a responsibility to provide information to the public that is consistent  
512 with their missions.
- 513 3) Agencies shall address this responsibility by:
- 514 a) Managing information as an asset throughout its life cycle to promote openness and  
515 interoperability, and properly safeguarding systems and information;
- 516 b) Maintaining a public data listing and an enterprise data inventory describing agency  
517 information resources in accordance with guidance from OMB;
- 518 c) Ensuring that the public has timely and equitable access to the agency's public  
519 information;
- 520 d) Providing information, as required by law, describing agency organization, activities,  
521 programs, meetings, record series and systems, and other information holdings, and  
522 how the public may gain access to agency information;
- 523 e) Providing access to agency records under provisions of the Freedom of Information  
524 Act, the Privacy Act of 1974, the Information Quality Act, the Federal Records Act,  
525 the E-Government Act of 2002, the Federal Information Security Modernization Act  
526 of 2014, and other relevant statutes subject to the protections and limitations  
527 provided for in these Acts;
- 528 f) Providing notice of Federal agency privacy practices for the collection, use,  
529 maintenance, and dissemination of personally identifiable information;
- 530 g) Providing any other information that is necessary or appropriate for the proper  
531 performance of agency functions and to ensure the transparency and accountability  
532 of government;
- 533 h) Providing such information proactively rather than waiting for it to be requested;
- 534 i) Providing such information in a format(s) accessible to employees and members of  
535 the public with disabilities in compliance with Section 508 of the Rehabilitation Act  
536 of 1973, as amended (29 U.S.C. 794d);

- 537 j) Considering whether information disseminated from other Federal or nonfederal  
538 sources is equivalent to agency information and reasonably fulfills the dissemination  
539 responsibilities of the agency;
- 540 k) Establishing and maintaining inventories of all agency information dissemination  
541 products;
- 542 l) Developing other aids as necessary to assist the public in locating agency  
543 information including catalogs and directories, site maps, search functions, and other  
544 means;
- 545 m) Identifying the source of the information disseminated to the public, if from outside  
546 the agency;
- 547 n) Ensuring that government publications are made available to depository libraries  
548 through the Government Publishing Office, as required by law (44 U.S.C. Part 19);
- 549 o) Establishing and maintaining communications with members of the public and with  
550 State, local, tribal, and territorial governments so that the agency publishes  
551 information that meets their respective needs;
- 552 p) Providing adequate notice when initiating, substantially modifying, or terminating  
553 dissemination of significant information that the public may be using; and
- 554 q) Ensuring that, to the extent existing information dissemination policies or practices  
555 are inconsistent with the requirements of this Circular, a prompt and orderly  
556 transition to compliance with the requirements of this Circular is made.

557 e. Conforming with Open Data Standards

558 Agencies shall adopt a presumption in favor of openness to the extent permitted by law and  
559 subject to privacy, confidentiality, security, and other valid restrictions. Additionally,  
560 agencies shall:

- 561 1) Whenever possible, plan for IT solutions or services that incorporate capabilities to  
562 release data online in open, machine-readable formats;
- 563 2) Disseminate information in a manner that best achieves a balance between the usefulness  
564 of the information and the cost to the government and the public;
- 565 3) Disseminate information on equitable and timely terms;
- 566 4) Take advantage of all dissemination channels, including Federal, State, local, tribal,  
567 territorial governments, libraries, nonprofit, and private sector entities, in discharging  
568 agency information dissemination responsibilities;
- 569 5) Help the public locate government information maintained by or for the agency and help  
570 make information already disseminated easy to find and locate;
- 571 6) Comply with all applicable laws governing the disclosure of information, including  
572 those related to the quality, privacy, confidentiality, security, and other valid restrictions;  
573 and
- 574 7) To the extent practicable and subject to valid restrictions, publish information online (in  
575 addition to any other planned or mandated publication methods) in an open, machine-  
576 readable format that can be retrieved, downloaded, indexed, and searched by commonly

577 used web search applications and is public, accessible, described, reusable, complete,  
578 timely, and managed in manners consistent with OMB guidance regarding open data.  
579 This includes providing such information in a format(s) accessible to employees and  
580 members of the public with disabilities in compliance with Section 508 of the  
581 Rehabilitation Act of 1973, as amended (Pub. L. 105-220, 29 U.S.C. 794d).

582 f. Avoiding Improperly Restrictive Practices

583 To avoid improperly restrictive practices, agencies shall:

- 584 1) Avoid establishing, or permitting others to establish on their behalf, exclusive, restricted,  
585 or other distribution arrangements that interfere with allowing the agency to disseminate  
586 its information on a timely and equitable basis. Exceptions to this policy are time-limited  
587 restrictions or exclusivity in cases where the agency, due to resource constraints, would  
588 normally be unable to provide the information to the public on its own;
- 589 2) Avoid establishing unnecessary restrictions, including charging of fees or royalties, on  
590 the reuse, resale, or re-dissemination of Federal information by the public; and
- 591 3) Recover only the cost of dissemination if fee and user charges are necessary. They must  
592 exclude from calculation the costs associated with original collection and processing of  
593 the information. Exceptions to this policy are:
  - 594 a) Where statutory requirements are at variance with the policy;
  - 595 b) Where the agency collects, processes, and disseminates the information for the  
596 benefit of a specific identifiable group beyond the benefit to the general public;
  - 597 c) Where the agency plans to establish user charges at less than cost of dissemination  
598 because of a determination that higher charges would constitute a significant barrier  
599 to properly performing the agency's functions, including reaching members of the  
600 public whom the agency has a responsibility to inform; or
  - 601 d) Where the Director of OMB determines an exception is warranted.

602 g. Implementing Information Safeguards

603 To ensure proper safeguards, agencies shall:

- 604 1) Ensure that information is protected commensurate with the risk that would result from  
605 unauthorized access, use, disclosure, disruption, modification, or destruction of such  
606 information;
- 607 2) Limit the collection of personally identifiable information to that which is legally  
608 authorized and necessary for the proper performance of agency functions;
- 609 3) Only maintain personally identifiable information for as long as is necessary to  
610 accomplish a legally authorized purpose;
- 611 4) Limit the sharing of personally identifiable information or proprietary information to that  
612 which is legally authorized, and impose appropriate conditions on use where a  
613 continuing obligation to ensure the confidentiality of the information exists; and
- 614 5) Provide individuals, upon request, access to records about them maintained in Privacy  
615 Act systems of records, and permit them to amend such records consistent with the  
616 provisions of the Privacy Act.

617 h. IT Resources Portfolio Management

618 In support of agency missions and business needs and in coordination with program  
619 managers, the agency shall define, implement, and maintain processes, standards, and  
620 policies applied to all ‘information technology resources’ at the agency, in accordance with  
621 OMB guidance. Specifically, agencies shall ensure that department/headquarters chief  
622 information officers lead and oversee, in coordination with program managers, the following  
623 agency-wide and investment-level management processes, in accordance with OMB  
624 guidance:

- 625 1) Define the development processes, milestones, review gates, and the overall policies for  
626 all capital planning and project management and reporting for IT resources;
- 627 2) Perform planning, programming, budgeting, and execution decisions, related reporting  
628 requirements, and reports related to IT resources, and the management, governance, and  
629 oversight processes related to IT resources;
- 630 3) Establish and maintain a process to regularly engage with program managers to evaluate  
631 IT resources supporting each agency strategic objective. Work with program managers  
632 to ensure that legacy and ongoing IT investments are appropriately delivering customer  
633 value and meeting the business objectives of programs;
- 634 4) Establish a portfolio-wide acquisition strategy that avoids duplication by considering  
635 existing solutions first and adopt the contracting vehicles necessary to build a robust  
636 technology infrastructure in coordination with program managers;
- 637 5) Ensure that the workforce related to IT resources has the appropriate knowledge and  
638 skill for facilitating the achievement of the performance goals established for the  
639 portfolio of IT resources and evaluate the extent to which the executive-level workforce  
640 of the agency has appropriate IT-related knowledge and skills;
- 641 6) Develop an enterprise architecture that describes the baseline architecture, the target  
642 architecture, and a plan to get to the target architecture;
- 643 7) Ensure that IT resources across the portfolio use appropriate measurements to evaluate  
644 the cost variance, schedule variance, and overall performance of their activities as a part  
645 of portfolio-wide processes such as capital planning and investment control, enterprise  
646 architecture, and other agency information technology or performance management  
647 processes. When an Earned Value Management System (EVMS) is required, the  
648 standard definitions of cost variance and schedule variance will be used to measure  
649 progress;
- 650 8) Establish agency-wide policies and procedures for conducting investment reviews,  
651 operational analyses, or other applicable performance reviews to evaluate the following  
652 aspects of IT resources, including projects in development and ongoing activities:  
653 determine whether there is a continuing need for the activity as planned; for high-risk  
654 activities whether the root causes of risk in the investment have been addressed, whether  
655 there is sufficient capability to deliver the remaining planned increments within the  
656 planned cost and schedule, and what corrective actions, including termination, should be  
657 taken;

- 658 9) Establish an overall portfolio of IT resources that achieve program and business  
659 objectives efficiently and effectively by:
- 660 a) Weighing potential and ongoing investments and their underlying capabilities against  
661 other proposed and ongoing investments in the portfolio;
- 662 b) Implementing an EVMS and conducting an Integrated Baseline Review (IBR) as  
663 required by Federal Acquisition Regulation Subpart 34.2 or, when an EVMS is not  
664 required, implementing a baseline validation process as part of an overall investment  
665 risk management strategy consistent with OMB guidance; and
- 666 c) Identifying gaps between planned and actual cost, schedule, and performance goals  
667 for information technology investments and identifying strategies and time frames to  
668 close such gaps;
- 669 10) Recommend to the agency head the modification, pause, or termination of any  
670 acquisition, investment, or activity that includes a significant IT component based on the  
671 CIO's judgment—including but not limited to the results of the processes described in 1)  
672 through 9) above—within the terms of the relevant contracts and applicable regulations;  
673 and
- 674 11) Maintain the following, as required by the Paperwork Reduction Act (44 U.S.C.  
675 3506(b)(4) and 3511), Freedom of Information Act (5 U.S.C. 552(g)), and Federal  
676 Information Security Modernization Act of 2014: an inventory of the agency's major  
677 information systems, holdings, and dissemination products; a description of the agency's  
678 major information and record locator systems; an inventory of the agency's other  
679 information resources, such as personnel and funding (at the level of detail that the  
680 agency determines is most appropriate for its use in managing the agency's information  
681 resources); and an online resource for persons to obtain public information from the  
682 agency pursuant to these Acts.

683 i. IT Investment Management

684 IT investment decisions must also be consistent with policies and processes defined by the  
685 agency as described above. Agency chief information officers shall establish criteria  
686 identifying which of the following investment management aspects require the direct  
687 involvement of the chief information officer in accordance with the below requirements.  
688 Agencies shall ensure that policies and processes approved by the department/headquarters  
689 chief information officer are applied to all IT investment decisions and processes below.

690 1) Acquisition of Information Technology

691 Agencies shall:

- 692 a) Consistent with applicable Federal acquisition requirements, make use of adequate  
693 competition, allocate risk between government and contractor, and maximize return  
694 on investment (ROI) when acquiring information technology;
- 695 b) Conduct definitive technical, cost, and risk analyses of alternative design  
696 implementations, including consideration of migration and retraining costs, scaled to  
697 the size and complexity of individual requirements (definitive acquisition planning  
698 provisions are set forth in Federal Acquisition Regulation [FAR] subparts 7.1,  
699 Acquisition Plans, and 10, Market Research);

- 700 c) Consider existing Federal contract solutions available to meet agency needs to avoid  
701 duplicative investments;
- 702 d) Structure acquisitions for major IT investments into useful segments with a narrow  
703 scope and brief duration. This should reduce risk, promote flexibility and  
704 interoperability, increase accountability, and better match mission need with current  
705 technology and market conditions;
- 706 e) Not approve an acquisition strategy or acquisition plan (as described in FAR Part 7)  
707 or interagency agreement (such as those used to support purchases through another  
708 agency) that includes IT without review and approval by the agency CIO. The CIO  
709 shall consider the following factors when reviewing acquisition strategies and  
710 acquisition plans:
- 711 (i) Alignment with mission and program objectives in coordination with program  
712 leadership;
- 713 (ii) Appropriateness with respect to the mission and business objectives supported  
714 by the IT strategic plan;
- 715 (iii) Appropriateness of contract type for IT-related resources; and
- 716 (iv) Appropriateness of IT-related portions of statement of needs or statement of  
717 work.

718 2) IT Capital Planning and Investment Control

719 IT Capital Planning and Investment Control (CPIC) is the process by which agencies  
720 establish the need and goals to plan, acquire or develop, and evaluate the results of  
721 investments in information systems, technologies, and capabilities in support of agency  
722 missions, organizational and performance requirements, strategies, and goals. Agencies  
723 must designate IT investments as major investments or non-major investments according  
724 to relevant statute, regulations and guidance in OMB Circular A-11, and perform CPIC  
725 processes commensurate with the size, scope, duration, and delivery risk of the  
726 investment. The CPIC process consists of all stages of capital programming, including  
727 planning, budgeting, procurement, management, and assessment. For further guidance  
728 on capital programming, refer to OMB Circular A-11, including the Capital  
729 Programming Guide. IT CPIC comprises portfolio-level planning and management, and  
730 investment-specific planning and management. Agency CPIC processes must be  
731 consistent with OMB guidance defining the steps, standards, reporting artifacts,  
732 responsibilities, and other aspects of CPIC. The actions, policies, and artifacts of the  
733 CPIC process's evaluation, selection, and control phases shall ensure that the following  
734 requirements are appropriately met by all IT resources:

- 735 a) All IT resources are included in IT portfolio and capital planning documents or  
736 artifacts;
- 737 b) In coordination with program managers, significant decisions related to major IT  
738 investments are supported by business cases with appropriate evidence;
- 739 c) All IT resources appropriately implement incremental development and modular  
740 approaches as defined in OMB guidance;

- 741 d) IT investments support and enable core mission and operational functions and  
742 processes that support the agency’s missions and business requirements;
- 743 e) Decisions to improve, enhance, or modernize existing information technology  
744 investments or to develop new information technology investments are made only  
745 after conducting an alternatives analysis that includes both government-provided  
746 (internal, interagency, and intra-agency where applicable) and commercially  
747 provided options and the most advantageous option to the government has been  
748 selected;
- 749 f) Preference must first be given to using available and suitable Federal information  
750 systems, technologies, and shared services or information processing facilities, or to  
751 acquiring commercially available off-the-shelf software and technologies over  
752 developing or acquiring custom or duplicative solutions. Decisions to acquire custom  
753 or duplicative solutions must be justified based on overall life-cycle cost-  
754 effectiveness or ability to meet specific and high-priority mission or operational  
755 requirements;
- 756 g) Information technology needs are met through scalable, provisioned services when it  
757 is cost-effective to do so rather than acquiring or developing new information  
758 systems or equipment;
- 759 h) New acquisitions which include information technology must evaluate open source  
760 software and off-the-shelf technology as options;
- 761 i) Information systems security levels are commensurate with the risk that may result  
762 from unauthorized access, use, disclosure, disruption, modification, or destruction of  
763 such information;
- 764 j) Information technology investments must facilitate interoperability, application  
765 portability, and scalability across networks of heterogeneous hardware, software, and  
766 telecommunications platforms;
- 767 k) Information systems and processes must support interoperability and information  
768 accessibility, maximize the usefulness of information, minimize the burden on the  
769 public, and preserve the appropriate integrity, usability, availability, confidentiality,  
770 and disposition of information throughout the life cycle of the information, in  
771 accordance with the PRA, FISMA, Privacy Act (as amended) and the Federal  
772 Records Act (as amended);
- 773 l) Information systems and processes must facilitate accessibility under the  
774 Rehabilitation Act of 1973, as amended; in particular, see specific electronic and  
775 information technology accessibility requirements commonly known as “section  
776 508” requirements (29 U.S.C. § 794d); and
- 777 m) Agencies must incorporate records management functions and retention  
778 requirements into the design, development, and implementation of information  
779 systems, particularly Internet resources to include storage solutions and cloud-based  
780 services such as software as a service, platform as a service, and infrastructure as a  
781 service.

782

783 **8. Assignment of Responsibilities**

- 784 a. For all Federal agencies, the head of each agency shall:
- 785 1) Have primary responsibility for managing agency information resources to support  
786 agency missions and business requirements;
- 787 2) Ensure that the digital services provided by the agency work well and are continually  
788 improved to better meet the needs of the public;
- 789 3) Ensure that the agency implements the information policies, principles, directives,  
790 standards, guidelines, rules, and regulations promulgated by OMB, as appropriate;
- 791 4) Develop agency policies and procedures that provide for timely acquisition of required  
792 information technology;
- 793 5) Implement and enforce applicable records management policies and procedures,  
794 including requirements for archiving information maintained in electronic format,  
795 particularly in the planning, design, and operation of information systems;
- 796 6) Identify to the Director of OMB any statutory, regulatory, and other impediments to  
797 efficient management of Federal information resources, and recommend to the Director  
798 legislation, policies, procedures, and other guidance to improve such management;
- 799 7) Assist OMB in the performance of its functions under the PRA, including making  
800 services, personnel, and facilities available to OMB for this purpose to the extent  
801 practicable;
- 802 8) Ensure that the agency:
- 803 a) Cooperates with other agencies in the use of information technology to improve the  
804 productivity, effectiveness, and efficiency of Federal programs; and
- 805 b) Promotes a coordinated, interoperable, secure, and shared governmentwide  
806 infrastructure that is provided and supported by a diversity of private sector  
807 suppliers;
- 808 9) Develop a well-trained corps of information resources management professionals;
- 809 10) Develop an effective and experienced corps of digital services experts;
- 810 11) Use the guidance provided in OMB Circular A-11, "Planning, Budgeting, Acquisition  
811 and Management of Capital Assets," and other relevant OMB guidance for IT CPIC to  
812 promote effective and efficient capital planning within the organization;
- 813 12) Ensure that the agency provides budget data pertaining to information resources to  
814 OMB, consistent with the requirements of OMB Circular A-11 and related OMB  
815 guidance, and ensure, to the extent reasonable, that in the design of information systems  
816 with the purpose of disseminating information to the public, an index of information  
817 disseminated by the system shall be included in the directory created by the  
818 Superintendent of Documents pursuant to 41 U.S.C. 4101. (Nothing in this paragraph  
819 authorizes the dissemination of information to the public unless otherwise authorized.);
- 820 13) Permit, to the extent practicable, the use of one agency's contract by another agency or  
821 the award of multiagency contracts, provided the action is within the scope of the  
822 contract and consistent with OMB guidance;

- 823 14) As designated by the Director of OMB, act as executive agent for the governmentwide  
824 acquisition of information technology;
- 825 15) Ensure compliance with Federal information privacy and security requirements, to  
826 include statistical confidentiality;
- 827 16) Designate a senior agency official for privacy (SAOP) who has overall agency-wide  
828 responsibility for information privacy; and
- 829 17) Appoint a Chief Information Officer, as required by 44 U.S.C. 3506(a).
- 830 a) The CIO shall report directly to the agency head as required by the Clinger-Cohen  
831 Act (40 U.S.C. 1425(b) & (c)). Agencies that have implemented legislation that  
832 requires the CIO and other management officials to report to a Chief Operating  
833 Officer (COO), Undersecretary for Management, Assistant Secretary for  
834 Administration, or similar management executive shall ensure that the CIO has direct  
835 access to the agency head (i.e., the Secretary, or Deputy Secretary serving on the  
836 Secretary's behalf) for their information technology responsibilities to remain  
837 consistent with the Clinger-Cohen requirement.
- 838 b) The CIO shall carry out the responsibilities of the agencies listed in the Paperwork  
839 Reduction Act (44 U.S.C. 3506), the Clinger-Cohen Act (40 U.S.C. 1425(b) & (c)),  
840 the E-Government Act of 2002 (Pub. L. 107-347), the Privacy Act of 1974 (as  
841 amended (5 U.S.C. 552a)), the Government Performance and Results Modernization  
842 Act of 2010 (Pub. L. 111-352), the Government Paperwork Elimination Act of 1998  
843 (Pub. L. 105-277, Title XVII), the Federal Records Act of 1950 (as amended,  
844 codified (44 U.S.C. Chapter 29, 31, 33)), the Federal Acquisition Streamlining Act  
845 V, Section 508 of the Rehabilitation Act of 1973 (as amended (Pub. L. 105-220, 29  
846 U.S.C. 794d)); the Digital Accountability and Transparency Act of 2014; the Federal  
847 Information Security Modernization Act of 2014; and other related statutes.
- 848 c) The head of the agency must consult with the Director of OMB prior to appointing a  
849 Chief Information Officer, and shall advise the Director on matters regarding the  
850 authority, responsibilities, and organizational resources of the Chief Information  
851 Officer.

852 For purposes of this paragraph (17), military departments and the Office of the Secretary  
853 of Defense may each appoint one official.

- 854 b. The Chief Information Officer, in coordination with other agency senior officials and  
855 program managers, must, among other things:
- 856 1) Develop internal agency information policies and procedures and oversee, evaluate, and  
857 otherwise periodically review agency information resources management activities  
858 (including the management of information technology resources) for conformity with the  
859 policies set forth in this Circular;
- 860 2) Advise the agency head on information resources implications of strategic planning  
861 decisions;
- 862 3) Advise the agency head on the design, development, and implementation of information  
863 resources;

- 864 4) Advise the agency head on budgetary implications of decision affecting information  
865 resources and information technology resources;
- 866 5) Be an active participant throughout the annual agency budget process in establishing  
867 investment priorities for agency information technology resources;
- 868 6) Review and approve all reprogramming of funds related to information technology  
869 resources;
- 870 7) Advise and support the teams responsible for creating and maintaining the agency's  
871 digital services, including by coordinating with such teams to ensure that digital services  
872 activities support the overall program and business objectives of the information  
873 technology resources portfolio as well as the agency's missions and programs;
- 874 8) Define, maintain, and oversee policies and standards governing all strategic-level and  
875 investment-level information technology management processes described in Section 8.  
876 Identify incomplete or inconsistent application of these policies and standards within the  
877 agency and report these to the agency head and OMB as appropriate. In consultation  
878 with OMB, describe the effectiveness of these agency processes as a part of portfolio  
879 reviews or other reporting;
- 880 9) Be an active participant during all agency strategic management activities, including the  
881 development, implementation, and maintenance of agency strategic and operational  
882 plans;
- 883 10) Designate an official within the office of the CIO to serve as a liaison to help coordinate  
884 agency actions and policies with the agency's SAOP, unless the agency's CIO is  
885 designated as the SAOP;
- 886 11) Collaborate with heads of Federal principal statistical agencies and recognized statistical  
887 units to support their conformance with Statistical Policy Directives governing the  
888 design, scope, collection, processing, calculation, production, and dissemination of  
889 official Federal statistics;
- 890 12) Monitor and evaluate the performance of information technology investments through a  
891 CPIC process, and advise the agency head on whether to continue, modify, or terminate  
892 a program or project;
- 893 13) Be responsible for ensuring that the agency workforce has the information resources  
894 management skills it needs by playing a material role in the selection of staff with  
895 significant information technology resource management responsibilities; continuously  
896 assessing and improving the requirements established for agency personnel regarding  
897 knowledge and skills; determining the extent to which the positions and personnel at the  
898 agency meet those requirements; and developing strategies and specific plans for hiring,  
899 training, and professional development to rectify any deficiency in meeting those  
900 requirements;
- 901 14) Report to the agency head on the effectiveness of the agency information security  
902 program;
- 903 15) Maintain regular participation with the Chief Information Officers Council which serves  
904 as the principal interagency forum for CIOs to share best practices, seek out assistance

905 from other Federal CIOs and to collaborate on improving the management of Federal IT;  
906 and

907 16) Oversee agency compliance with the prompt, efficient, and effective implementation of  
908 the information policies and information resources management responsibilities  
909 established under the Paperwork Reduction Act, which include reducing the information  
910 collection burdens on the public and increasing the utility of information created,  
911 collected, maintained, used, shared, and disseminated by the agency. Specific  
912 responsibilities include:

913 a) Establishing an independent (independent of program responsibility) review process  
914 for information collections;

915 b) Seeking and obtaining OMB approval before undertaking a collection of information  
916 directed to 10 or more persons;

917 c) Publishing a 60-day notice in the *Federal Register* requesting public comment on the  
918 proposed collection of information;

919 d) Reviewing and considering public comments received on the proposed collection of  
920 information;

921 e) Publishing a 30-day notice in the *Federal Register* notifying the public of the  
922 agency's request for comments and submission to OMB for review of the proposed  
923 collection of information; and

924 f) Fulfilling all other duties and responsibilities assigned to the Chief Information  
925 Officer per 5 C.F.R. 1320.

926 c. Department of State

927 The Secretary of State shall:

928 1) Consult with and advise the Director of OMB on the development of United States  
929 positions and policies on international information policy and technology issues  
930 affecting Federal Government activities and the development of international  
931 information technology standards; and

932 2) Be responsible for liaison, consultation, and negotiation with foreign governments and  
933 intergovernmental organizations on all matters related to information resources  
934 management, including Federal information technology. The Secretary must also ensure,  
935 in consultation with the Secretary of Commerce, that the United States is robustly  
936 represented in the development of international standards and recommendations  
937 affecting information technology. These responsibilities may also require the Secretary  
938 to consult, as appropriate, with affected domestic agencies, organizations, and other  
939 members of the public.

940 d. Department of Commerce

941 The Secretary of Commerce shall:

942 1) Develop and issue Federal Information Processing Standards (FIPS) and guidelines  
943 necessary to ensure the efficient and effective acquisition, management, security, and

- 944 use of information technology, while taking into consideration the recommendations of  
945 the agencies and the CIO Council;
- 946 2) Provide OMB and the agencies with scientific and technical advisory services relating to  
947 the development and use of information technology;
- 948 3) Conduct studies and evaluations concerning telecommunications technology, and the  
949 improvement, expansion, testing, operation, and use of Federal telecommunications  
950 systems, and advise the Director of OMB and appropriate agencies of the  
951 recommendations that result from such studies;
- 952 4) Develop, in consultation with the Secretary of State and the Director of OMB, plans,  
953 policies, and programs relating to international telecommunications issues affecting  
954 Government information activities;
- 955 5) Identify needs for standardization of telecommunications and information processing  
956 technology, and develop standards, in consultation with the Secretary of Defense and the  
957 Administrator of General Services, to ensure efficient application of such technology;  
958 and
- 959 6) Ensure that the Federal Government is represented in the development of national and,  
960 in consultation with the Secretary of State, international information technology  
961 standards, and advise the Director of OMB on such activities.
- 962 e. Department of Defense
- 963 The Secretary of Defense shall develop, in consultation with the Administrator of General  
964 Services, uniform Federal telecommunications standards and guidelines to ensure national  
965 security, emergency preparedness, and continuity of government.
- 966 f. Department of Homeland Security
- 967 The Department of Homeland Security shall:
- 968 1) Assist agencies with the implementation of information security policies and practices  
969 for information systems;
- 970 2) Assist the Office of Management and Budget in carrying out its information security  
971 oversight and policy responsibilities;
- 972 3) In consultation with OMB, develop and oversee the implementation of binding  
973 operational directives to agencies. Such directives shall be consistent with OMB policies  
974 and NIST standards and guidelines. The directives may be revised or repealed by OMB  
975 if the direction issued on behalf of OMB is not in accordance with policies developed by  
976 OMB. The binding operational directives shall focus on:
- 977 a) Requirements for the mitigation of exigent risks to information systems;
- 978 b) Requirements for reporting incidents to the Federal information security incident  
979 center; and
- 980 c) Other operational requirements, as deemed necessary by OMB or DHS, in  
981 consultation with OMB;
- 982 4) Consult with the Director of NIST regarding any binding operational directives that  
983 implement standards and guidelines developed by NIST;

- 984 5) Convene meetings with senior agency officials to help ensure effective implementation  
985 of information security policies and procedures;
- 986 6) Coordinate governmentwide efforts on information security policies and practices,  
987 including consultation with the Chief Information Officers Council and the National  
988 Institute of Standards of Technology;
- 989 7) Provide and operate Federal information security shared services as directed by OMB;
- 990 8) Provide operational and technical assistance to agencies in implementing policies,  
991 principles, standards, and guidelines on information security. This includes:
  - 992 a) Operating the Federal information security incident center;
  - 993 b) Deploying technology to assist agencies to continuously diagnose and mitigate cyber  
994 threats and vulnerabilities, with or without reimbursement and at the request of the  
995 agency;
  - 996 c) Compiling and analyzing data on agency information security; and
  - 997 d) Developing and conducting targeted operational evaluations, including threat and  
998 vulnerability assessments, on information systems;
- 999 9) Provide agencies with intelligence about cyber threats, vulnerabilities, and incidents for  
1000 risk assessments;
- 1001 10) Consult with OMB to determine what other actions may be necessary to support  
1002 implementation of effective governmentwide information security programs; and
- 1003 11) Provide the public with timely notice and opportunities for comment on proposed  
1004 information security directives and procedures to the extent that such directives and  
1005 procedures affect communication with the public.

1006 g. General Services Administration

1007 The Administrator of General Services shall:

- 1008 1) Continue to manage a governmentwide network contract program and coordinate the  
1009 follow-up to that program, on behalf of and with the advice of agencies;
- 1010 2) Develop, maintain, and disseminate for the use of the Federal community (as requested  
1011 by OMB or agencies) recommended methods and strategies for the development and  
1012 acquisition of information technology;
- 1013 3) Conduct and manage outreach programs in cooperation with agency managers;
- 1014 4) Serve as a liaison on information resources management (including Federal information  
1015 technology) with State, local, tribal, and territorial governments. GSA must also be a  
1016 liaison with nongovernmental international organizations, subject to prior consultation  
1017 with the Secretary of State to ensure consistency with the overall United States foreign  
1018 policy objectives;
- 1019 5) Provide support and assistance to the CIO Council; and
- 1020 6) Manage the Acquisition Services Fund in accordance with Public L. 109-313.

1021 h. Office of Personnel Management

- 1022 The Director, Office of Personnel Management shall:
- 1023 1) Analyze on an ongoing basis, the personnel needs of the Federal Government related to  
1024 information technology and information resources management;
  - 1025 2) Identify where current information technology and information resources management  
1026 training do not satisfy the needs of the Federal Government related to information  
1027 technology;
  - 1028 3) Oversee the development of curricula, training methods, and training priorities that  
1029 correspond to the projected personnel needs related to information technology and  
1030 information resources management; and
  - 1031 4) Assess the training of employees in information technology disciplines in order to ensure  
1032 that information resources management needs are addressed.

1033 i. National Archives and Records Administration

1034 The Archivist of the United States shall:

- 1035 1) Administer the Federal records management program in accordance with the Federal  
1036 Records Act and National Archives and Records Administration (NARA) requirements  
1037 (36 CFR Subchapter B – Records Management);
- 1038 2) Assist the Director of OMB in developing standards and guidelines relating to the  
1039 records management program; and
- 1040 3) Create records management policies, ensure agency compliance with records  
1041 management requirements and provide training as needed, and coordinate with OMB  
1042 and other agencies, to provide public access to high-value government records.

1043 **9. Effectiveness**

1044 This Circular is effective upon issuance. This Circular is not intended to, and does not, create any  
1045 right or benefit, substantive or procedural, enforceable at law or in equity by any party against  
1046 the United States, its departments, agencies, or entities, its officers, employees, or agents, or any  
1047 other person.

1048 **10. Oversight**

1049 The Director of OMB shall use information technology planning reviews, fiscal budget reviews,  
1050 information collection budget reviews, management reviews, and such other measures as the  
1051 Director deems necessary to evaluate the adequacy and efficiency of each agency's information  
1052 resources management and compliance with this Circular.

1053 **11. Inquiries**

1054 All questions or inquiries regarding information resources management, Government paperwork  
1055 elimination, privacy, and confidentiality should be addressed to the Office of Information and  
1056 Regulatory Affairs, Office of Management and Budget, Washington, D.C. 20503. Telephone:  
1057 (202) 395-3785 or Email: [infopolicy-oira@omb.eop.gov](mailto:infopolicy-oira@omb.eop.gov) or [privacy-oira@omb.eop.gov](mailto:privacy-oira@omb.eop.gov).  
1058 Questions or inquiries regarding information systems and technology or the security of Federal  
1059 information resources should be addressed to the Office of Electronic Government and

1060 Information Technology, Office of Management and Budget, Washington, D.C. 20503.  
1061 Telephone: (202) 395-0379 or Email: [egov@omb.eop.gov](mailto:egov@omb.eop.gov).

1062 **Appendix I to OMB Circular No. A-130**  
1063 **Responsibilities for Management of Personally Identifiable Information**  
1064

1065 **1. Purpose**

1066 This Appendix outlines some of the general responsibilities for Federal agencies managing  
1067 information resources that involve personally identifiable information (PII). For more specific  
1068 requirements, agencies should consult specific OMB guidance documents, which are available  
1069 on the OMB website.

1070 Previous versions of this Appendix included information about the reporting and publication  
1071 requirements of the Privacy Act of 1974 (5 U.S.C. § 552a) and additional OMB guidance. This  
1072 information has been revised and reconstituted as OMB Circular No. A-108, *Federal Agency*  
1073 *Responsibilities for Review, Reporting, and Publication under the Privacy Act*, which is also  
1074 available on the OMB website.

1075 **2. Responsibilities for Protecting PII**

1076 The Federal Government necessarily collects, uses, disseminates, and maintains PII to carry out  
1077 the missions mandated by the Constitution and laws of the United States. The term PII, as  
1078 defined in the main body of this Circular, refers to information that can be used to distinguish or  
1079 trace an individual's identity, either alone or when combined with other personal or identifying  
1080 information that is linked or linkable to a specific individual. To determine whether information  
1081 is PII, agencies must perform an assessment of the specific risk that an individual can be  
1082 identified. In performing this assessment, it is important to recognize that non-identifiable  
1083 information can become PII whenever additional information becomes available – in any  
1084 medium and from any source – that would make it possible to identify an individual.

1085 When Federal agencies manage information resources that involve PII, the individual's privacy  
1086 must be considered and appropriately protected. Agencies are required to designate a senior  
1087 agency official for privacy (SAOP) who has overall agency-wide responsibility and  
1088 accountability for ensuring the agency's implementation of all privacy requirements. The SAOP  
1089 should have a central policy-making role and should ensure that the agency considers the privacy  
1090 impact of all agency actions and policies that involve PII. The SAOP's review of privacy  
1091 implications should begin at the earliest planning and development stages of agency actions and  
1092 policies that involve PII, and should continue through the life cycle of the information.

1093 The SAOP must ensure that the agency complies with all applicable requirements in law,  
1094 regulation, and policy. Relevant authorities include, but are not limited to, the Privacy Act of  
1095 1974 (5 U.S.C. § 552a), the Paperwork Reduction Act of 1995 (44 U.S.C. chapter 35), the E-  
1096 Government Act of 2002 (44 U.S.C. § 3501 note), *Privacy Act Implementation: Guidelines and*  
1097 *Responsibilities* (40 Fed. Reg. 28,948, July 9, 1975), *Final Guidance Interpreting the Provisions*  
1098 *of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988* (54 Fed.  
1099 Reg. 25,818, June 19, 1989), and *OMB Guidance for Implementing the Privacy Provisions of the*  
1100 *E-Government Act of 2002* (OMB Memorandum M-03-22, Sept. 26, 2003).

1101

1102 **3. Responsibilities for Protecting PII Collected for Statistical Purposes under a Pledge of**  
1103 **Confidentiality**

1104 The Nation relies on the flow of credible statistics to support the decisions of individuals,  
1105 households, governments, businesses, and other organizations. Any loss of trust in the relevance,  
1106 accuracy, objectivity, or integrity of the Federal statistical system and its products can foster  
1107 uncertainty about the validity of measures our Nation uses to monitor and assess performance,  
1108 progress, and needs.

1109 Given the importance of robust and objective official Federal statistics, agencies and components  
1110 charged with the production of these statistics are assigned particular responsibility.  
1111 Specifically, information acquired by an agency or component under a pledge of confidentiality  
1112 and for exclusively statistical purposes cannot be used for any regulatory or enforcement  
1113 purpose. As defined in the Confidential Information Protection and Statistical Efficiency Act  
1114 (Pub. L. 107–347, title V; 116 Stat. 2962), statistical purpose refers to the description,  
1115 estimation, or analysis of the characteristics of groups, without identifying the individuals or  
1116 organizations that compose such groups; it includes the development, implementation, or  
1117 maintenance of methods, technical or administrative procedures, or information resources that  
1118 support such purposes. These agencies and components must protect the integrity and  
1119 confidentiality of this information against unauthorized access, use, modification, or deletion  
1120 throughout the life cycle of the information. Further, these agencies and components must adhere  
1121 to legal requirements and follow best practices for protecting the confidentiality of data,  
1122 including training their employees and agents, and ensuring the physical and information system  
1123 security of confidential information.

1124 Relevant authorities include, but are not limited to, Title V of the E-Government Act of 2002, the  
1125 Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA) (Pub. L.  
1126 107–347, title V; 116 Stat. 2962) and *Implementation Guidance for Title V of the E-Government*  
1127 *Act, Confidential Information Protection and Statistical Efficiency Act of 2002* (CIPSEA  
1128 *Implementation Guidance*) (72 Fed. Reg. 33362, 33368, June 15, 2007); and *Fundamental*  
1129 *Responsibilities of Federal Statistical Agencies and Recognized Statistical Units* (79 Fed. Reg.  
1130 71610, Dec. 2, 2014).

1131 **4. Fair Information Practice Principles**

1132 In addition to the requirements in law, regulation, and policy, agencies should consult the Fair  
1133 Information Practice Principles (FIPPs) when managing information resources that involve PII.  
1134 The FIPPs are a collection of widely accepted principles that agencies should use when  
1135 evaluating systems, processes, programs, and activities that affect individual privacy. Rooted in a  
1136 1973 Federal Government report, the FIPPs are at the core of the Privacy Act of 1974, and are  
1137 reflected in the laws of many U.S. states and foreign nations, as well as incorporated in the  
1138 policies of many organizations around the world.

1139 The precise expression of the FIPPs has varied over time and in different contexts. However, the  
1140 FIPPs retain a consistent set of core principles that are broadly relevant to agencies' information  
1141 management practices. The FIPPs are as follows:

- 1142 a. *Individual Participation.* Agencies should involve the individual in the decision-making  
1143 process regarding the collection, use, dissemination, and maintenance of PII and, to the  
1144 extent practicable, seek individual consent for these activities.
- 1145 b. *Transparency.* Agencies should be transparent about information policies and practices with  
1146 respect to PII, and should provide clear and accessible notice regarding collection, use,  
1147 dissemination, and maintenance of PII.
- 1148 c. *Authority.* Agencies should only collect, use, disseminate, or maintain PII if they have  
1149 specific authority to do so, and should identify this authority in the appropriate notice.
- 1150 d. *Purpose Specification and Use Limitation.* Agencies should provide notice of the specific  
1151 purpose for which PII is collected and should only use, disseminate, or maintain PII for a  
1152 purpose that is explained in the notice and is compatible with the purpose for which the PII  
1153 was collected.
- 1154 e. *Minimization.* Agencies should only collect and maintain PII that is directly relevant and  
1155 necessary to accomplish a legally authorized purpose, and should only maintain PII for as  
1156 long as is necessary to accomplish the purpose.
- 1157 f. *Access and Amendment.* Agencies should provide individuals with appropriate access to PII  
1158 and appropriate opportunity to correct or amend PII.
- 1159 g. *Redress.* Agencies should provide individuals with appropriate opportunity for redress  
1160 regarding unauthorized use and dissemination of PII, and should establish procedures to  
1161 receive and address individuals' privacy-related complaints.
- 1162 h. *Quality and Integrity.* Agencies should collect, use, disseminate, and maintain PII with such  
1163 accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure  
1164 fairness to the individual.
- 1165 i. *Security.* Agencies should establish administrative, technical, and physical safeguards to  
1166 protect PII commensurate with the risk and magnitude of the harm that would result from its  
1167 unauthorized access, use, modification, loss, destruction, or dissemination.
- 1168 j. *Training.* Agencies should clearly define the roles and responsibilities with respect to PII for  
1169 all employees and contractors, and should provide appropriate training to all employees and  
1170 contractors who have access to PII.
- 1171 k. *Integration.* Agencies should begin to consider the effect on individual privacy during the  
1172 earliest planning and development stages of any actions and policies, and should continue to  
1173 account for privacy implications during each stage of the life cycle of PII.
- 1174 l. *Accountability.* Agencies should be accountable for complying with these principles and all  
1175 applicable privacy requirements, and should appropriately monitor, audit, and document  
1176 compliance.

## 1177 **5. Privacy Controls for Federal Information Systems and Organizations**

1178 Agencies cannot protect privacy without considering information security. Therefore, it is  
1179 essential for agencies to take a coordinated approach to identifying and addressing privacy and  
1180 security requirements. A coordinated approach allows agencies to more effectively consider

1181 privacy and security requirements that may overlap in concept and in implementation within  
1182 Federal information systems, programs, and organizations.

1183 Agencies are expected to implement the security and privacy controls in National Institute of  
1184 Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy*  
1185 *Controls for Federal Information Systems and Organizations*. NIST SP 800-53 establishes  
1186 privacy controls that are designed to help agencies satisfy statutory privacy requirements and  
1187 privacy-related OMB policies. The privacy controls are based on the FIPPs and outline the  
1188 administrative, technical, and physical safeguards that agencies should apply to protect and  
1189 ensure proper handling of PII. Agencies should implement the privacy controls in a manner that  
1190 is consistent with their authorities, missions, and operational needs.

1191 The requirement to implement security and privacy controls is described in more detail in  
1192 Appendix III to this Memorandum, *Responsibilities for Protecting Federal Information*  
1193 *Resources*.

**Appendix II to OMB Circular No. A-130  
Guidance on Electronic Transactions**

1194  
1195  
1196  
1197  
1198  
1199  
  
1200  
1201  
1202  
1203  
1204  
1205  
  
1206  
1207  
  
1208  
1209  
  
1210  
1211  
1212  
1213  
  
1214  
1215  
1216  
  
1217  
  
1218  
1219  
1220  
1221  
1222  
1223  
  
1224  
1225  
1226  
1227  
1228  
1229  
1230  
  
1231  
1232

**1. Summary**

The Office of Management and Budget (OMB) provides procedures and guidance to implement the Government Paperwork Elimination Act (GPEA) and the Electronic Signatures in Global and National Commerce Act (E-SIGN).

GPEA required Federal agencies to allow individuals or entities that deal with the agencies the option to submit information or transact with the agency electronically, when practicable, and to maintain records electronically, when practicable. GPEA specifically states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form, and encourages Federal Government use of a range of electronic signature alternatives.

E-SIGN promotes the use of electronic contract formation, signatures, and recordkeeping in private commerce by establishing legal equivalence between:

- a. Contracts written on paper and contracts in electronic form;
- b. Pen-and-ink signatures and electronic signatures; and
- c. Other legally required written documents (termed “records”) and the same information in electronic form.

E-SIGN applies broadly to commercial, consumer, and business transactions affecting interstate or foreign commerce, and to transactions regulated by both Federal and State Government.

In support of GPEA and E-SIGN, the General Services Administration, in coordination with the Federal Chief Information Officers’ Council, maintains guidance on use of Electronic Signatures (E-Signatures) in Federal organization transactions which expands upon OMB guidance.

**2. Background**

This document provides agencies the guidance required under Sections 1703 and 1705 of the Government Paperwork Elimination Act (GPEA), Public L. 105-277, Title XVII, signed into law on October 21, 1998, and the Electronic Signatures in Global and National Commerce Act (E-SIGN), Public L. 106-229, signed into law on June 30, 2000. GPEA and E-SIGN are important tools to improve customer service and governmental efficiency through the use of information technology.

As public awareness of electronic communications and Internet usage has increased, demand for on-line interactions with the Federal agencies has also increased. Moving to electronic transactions and electronic signatures can reduce transaction costs for the agency and its partners. Transactions are quicker and information access can be more easily tailored to the specific questions that need to be answered. As a result, data analysis by Federal agencies would be easier. In addition, reengineering the work process associated with transactions may improve efficiency of agency operations.

Public confidence in the security of the government's electronic information processes is essential as agencies make this transition. Electronic commerce, electronic mail, and electronic

1233 benefits transfer can require the exchange of sensitive information within government, between  
1234 the government and private industry or individuals, and among governments. Electronic systems  
1235 must be able to protect the confidentiality and privacy of information, authenticate the identity of  
1236 the transacting parties to the degree required by the transaction, guarantee that the information is  
1237 not altered in an unauthorized way, and provide access when needed. A corresponding policy  
1238 and management structure must support the infrastructure that delivers these services.

1239 GPEA seeks to “preclude agencies or courts from systematically treating electronic documents  
1240 and signatures less favorably than their paper counterparts,” so that citizens can interact with the  
1241 Federal Government electronically (S. Rep. 105-335). It required Federal agencies to provide  
1242 individuals or entities that deal with agencies the option to submit information or transact with  
1243 the agency electronically, and to maintain records electronically, when practicable. It also  
1244 addresses the matter of private employers being able to use electronic means to store, and file  
1245 with Federal agencies, information pertaining to their employees. GPEA states that electronic  
1246 records and their related electronic signatures are not to be denied legal effect, validity, or  
1247 enforceability merely because they are in electronic form. It also encourages Federal  
1248 Government use of a range of electronic signature alternatives. This guidance implements GPEA  
1249 and supports the continued transition to electronic government.

1250 E-SIGN also eliminates barriers to electronic commerce, while also providing consumers with  
1251 protections equivalent to those available in the world of paper-based transactions. The Act makes  
1252 clear that no person is required to use electronic records, signatures, or contracts. E-SIGN  
1253 requires that a consumer affirmatively consent to the use of electronic notices and records. Prior  
1254 to consenting, the consumer must receive notice of their rights. Moreover, the consumer must  
1255 provide the affirmative consent electronically, in a manner that reasonably demonstrates that the  
1256 consumer can access the electronic records that are the subject of the consent.

1257 E-SIGN applies broadly to Federal and State statutes and regulations governing private sector  
1258 (including business-to-business and business-to-consumer) activities. It generally covers legal  
1259 requirements that information be disclosed in private transactions. It also requires that agencies  
1260 generally permit private parties to retain records electronically. The government may establish  
1261 appropriate performance standards for the accuracy, integrity, and accessibility of records  
1262 retained electronically, to ensure compliance with applicable laws and to guard against fraud.

1263 Agency activities and requirements that involve information, but do not relate to business,  
1264 commercial, or consumer transactions, are not within the scope of E-SIGN. Instead they are  
1265 addressed by the Government Paperwork Elimination Act (GPEA). Certain laws and regulations  
1266 involve both GPEA and E-SIGN, especially with respect to record retention requirements in  
1267 agency regulations that relate to business, consumer, and commercial transactions. Additionally,  
1268 GPEA and E-SIGN guidance builds on the requirements and scope of the Paperwork Reduction  
1269 Act (PRA) of 1995. All transactions that involve Federal information collections covered under  
1270 the PRA are also covered under GPEA and E-SIGN. Guidance on implementing the  
1271 requirements of these Acts is referenced below.

### 1272 **3. Guidance**

1273 Guidance and procedures on implementing the Government Paperwork Elimination Act are set  
1274 forth in the documents referenced below:

- 1275 a. OMB Memoranda M-00-10, *Procedures and Guidance on Implementing the Government*  
1276 *Paperwork Elimination Act*, April 25, 2000.  
1277 [https://www.whitehouse.gov/omb/memoranda\\_m00-10](https://www.whitehouse.gov/omb/memoranda_m00-10)
- 1278 b. OMB Memoranda M-00-15, *OMB Guidance on Implementing the Electronic Signatures*,  
1279 September 25, 2000. [https://www.whitehouse.gov/omb/memoranda\\_m00-15](https://www.whitehouse.gov/omb/memoranda_m00-15)
- 1280 c. Guidance on Implementing the Electronic Signatures in Global and National Commerce Act  
1281 (E-SIGN). [https://www.whitehouse.gov/sites/default/files/omb/memoranda/esign-](https://www.whitehouse.gov/sites/default/files/omb/memoranda/esign-guidance.pdf)  
1282 [guidance.pdf](https://www.whitehouse.gov/sites/default/files/omb/memoranda/esign-guidance.pdf)
- 1283 d. Department of Justice, *Legal Considerations in Designing and Implementing Electronic*  
1284 *Processes: A Guide for Federal Agencies*, November 2000. <http://www.idmanagement.gov/>
- 1285 e. Federal Chief Information Council, *Use of Electronic Signatures in Federal Organization*  
1286 *Transactions*, January 2013. <http://www.idmanagement.gov/>

1287  
1288

**Appendix III to OMB Circular No. A-130**  
**Responsibilities for Protecting Federal Information Resources**

1289 **Requirements**

1290 **1. Introduction**

1291 Agencies<sup>1</sup> of the Federal Government depend on the secure acquisition, processing, storage,  
1292 transmission, and disposition of information to carry out their core missions and business  
1293 functions. This allows diverse information resources ranging from large enterprise information  
1294 systems (or systems of systems) to small mobile computing devices to collect, process, store,  
1295 maintain, transmit, and disseminate this information. The information relied upon is subject to a  
1296 range of threats that could potentially harm or adversely affect organizational operations (i.e.,  
1297 mission, functions, image, or reputation), organizational assets, individuals, other organizations,  
1298 or the Nation. These threats include environmental disruptions, purposeful attacks, structural  
1299 failures, human errors, and other threats that can compromise the confidentiality, integrity, or  
1300 availability of information. Leaders at all levels of the Federal Government must understand their  
1301 responsibilities and be held accountable for managing information security and protecting  
1302 privacy.

1303 Federal agencies must implement information security programs and privacy programs with the  
1304 flexibility to meet current and future information management needs and the sufficiency to  
1305 comply with applicable requirements. Emerging technologies and services will continue to shift  
1306 the ways in which agencies acquire, develop, manage, and use information and technology. As  
1307 technologies and services continue to change, so will the threat environment. Agency programs  
1308 must have the capability to address current threats while protecting their information resources  
1309 and privacy. The programs must also have the capability to address new and emerging threats.  
1310 To be effective, information security and privacy must be part of the day-to-day operations of  
1311 agencies. This is best accomplished by planning for the requisite security and privacy capabilities  
1312 as an integral part of the agency strategic planning and risk management processes, not as a  
1313 separate activity. This includes, but is not limited to, the integration of information security and  
1314 privacy requirements (and associated security and privacy controls) into the enterprise  
1315 architecture, system development life cycle activities, systems engineering processes, and  
1316 acquisition processes.

1317 As Federal agencies take advantage of emerging information technologies and services to obtain  
1318 more effective mission and operational capabilities, achieve greater efficiencies, and reduce  
1319 costs, they must also apply the principles and practices of risk management, information security,  
1320 and privacy, to the acquisition and use of those technologies and services. OMB requires  
1321 agencies to take a risk-based approach to information security to ensure that appropriate  
1322 safeguards and countermeasures are selected and implemented in a prioritized manner for current  
1323 missions and business operations. Such risk-based approaches involve framing, assessing,

---

<sup>1</sup> The terms *agency* and *organization* are interspersed throughout the document. However, these terms have similar meaning depending on the original sources of reference. The term *agency* is used in this publication in lieu of the more general term *organization* only in those circumstances where its usage is directly related to other source documents such as Federal statute or policy. The term *organization* is used in this publication to describe an entity of any size, complexity, or positioning within an organizational structure (e.g., a Federal agency or, as appropriate, any of its operational elements).

1324 responding to, and monitoring security risks on an ongoing basis. Risk-based approaches can  
1325 also support potential performance improvements and cost savings when agencies make  
1326 decisions about maintaining, modernizing, or replacing existing information technologies and  
1327 services or implementing new technologies and services that leverage internal, other  
1328 government, or private sector innovative and market-driven solutions. These responsibilities  
1329 extend to the creation, collection, processing, storage, transmission, dissemination, and disposal  
1330 of Federal information when such information is hosted by nonfederal entities on behalf of the  
1331 Federal Government. Ultimately, agency heads remain responsible and accountable for ensuring  
1332 that information management practices comply with all applicable requirements, and that Federal  
1333 information is adequately protected commensurate with the risk resulting from the unauthorized  
1334 access, use disclosure, disruption, modification, or destruction of such information.

1335 While it is essential for agencies to take a coordinated approach to identifying and addressing  
1336 security and privacy requirements, it is also important to recognize that security and privacy are  
1337 different and may require different approaches. For example, privacy laws and policies often  
1338 establish clear rules and requirements that agencies must comply with when collecting, using,  
1339 maintaining, or disseminating personally identifiable information (PII). When agencies are  
1340 taking steps to meet these specific requirements, a purely risk-based approach is not taken since  
1341 the requirements must be satisfied in full. However, once the baseline privacy requirements are  
1342 met, agencies are expected to use privacy impact assessments and other tools to further analyze  
1343 privacy risks and consider the implementation of additional privacy control enhancements to  
1344 protect PII. For more information about privacy requirements, consult Appendix I to this  
1345 Memorandum, *Responsibilities for Management of Personally Identifiable Information*.

## 1346 **2. Purpose**

1347 This Appendix establishes minimum requirements for Federal information security programs,  
1348 assigns Federal agency responsibilities for the security of information and information systems,  
1349 and links agency information security programs and agency management control systems  
1350 established in accordance with OMB Circular No. A-123, *Management's Responsibility for*  
1351 *Internal Control*. This Appendix also establishes requirements for Federal privacy programs,  
1352 assigns responsibilities for privacy program management, and describes how agencies should  
1353 take a coordinated approach to implementing information security and privacy controls.<sup>2</sup> This  
1354 Appendix revises requirements contained in previous versions of Appendix III to OMB Circular  
1355 No. A-130, and incorporates requirements of the Federal Information Security Modernization  
1356 Act of 2014 (P.L. 113-283), the E-Government Act of 2002 (P.L. 107-347), and responsibilities  
1357 assigned in Executive Orders and Presidential Directives.

## 1358 **3. Definitions**

- 1359 a. The terms ‘Confidentiality,’ ‘Federal information,’ ‘Federal information system,’  
1360 ‘information security,’ ‘personally identifiable information,’ and ‘senior agency official for  
1361 privacy’ are defined in the main body of this Circular.
- 1362 b. ‘Adequate security’ means security protections commensurate with the risk resulting from  
1363 the unauthorized access, use, disclosure, disruption, modification, or destruction of

---

<sup>2</sup> Agencies should consult OMB policies on privacy, including Appendix I to this Memorandum and OMB Circular No. A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*.

- 1364 information. This includes ensuring that information hosted on behalf of an agency and  
1365 information systems and applications used by the agency operate effectively and provide  
1366 appropriate confidentiality, integrity, and availability protections through the application of  
1367 cost-effective security controls.
- 1368 c. ‘Authorization’ means the official management decision given by a senior Federal official to  
1369 authorize operation of an information system and to explicitly accept the risk to  
1370 organizational operations (including mission, functions, image, or reputation), organizational  
1371 assets, individuals, other organizations, and the Nation based on the implementation of an  
1372 agreed-upon set of security and privacy controls. Authorization also applies to common  
1373 controls inherited by organizational information systems.
- 1374 d. ‘Authorization boundary’ means all components of an information system to be authorized  
1375 for operation by an authorizing official and excludes separately authorized systems, to which  
1376 the information system is connected.<sup>3</sup>
- 1377 e. ‘Authorization official’ means a senior Federal official or executive with the authority to  
1378 authorize (i.e., assume responsibility for) the operation of an information system or the use of a  
1379 designated set of common controls at an acceptable level of risk to organizational operations  
1380 (including mission, functions, image, or reputation), organizational assets, individuals, other  
1381 organizations, and the Nation.
- 1382 f. ‘Authorization package’ means the essential information that an authorizing official uses to  
1383 determine whether or not to authorize the operation of an information system or the use of a  
1384 designated set of common controls. At a minimum, the authorization package includes the  
1385 security plan, the privacy plan, the security control assessment, the privacy control  
1386 assessment, and the security plan of action and milestones.
- 1387 g. ‘Breach’ means the loss of control, compromise, unauthorized disclosure, unauthorized  
1388 acquisition, unauthorized access, or any similar term referring to situations where persons  
1389 other than authorized users and for an other than authorized purpose have access or potential  
1390 access to personally identifiable information, whether physical or electronic.
- 1391 h. ‘Common control’ means a security or privacy control that is inherited by multiple  
1392 information systems.
- 1393 i. ‘Control inheritance’ means a situation in which an information system or application  
1394 receives protection from security and privacy controls (or portions of controls) that are  
1395 developed, implemented, assessed, authorized, and monitored by entities other than those  
1396 responsible for the system or application; entities either internal and external to the  
1397 organization where the system or application resides.
- 1398 j. ‘Controlled unclassified information’ means information that requires safeguarding or  
1399 dissemination controls pursuant to and consistent with law, regulations, and governmentwide  
1400 policies, excluding information that is classified under Executive Order 13526, Classified  
1401 National Security Information, December 29, 2009, or any predecessor or successor order, or  
1402 the Atomic Energy Act of 1954, as amended.

---

<sup>3</sup> Organizations have significant flexibility in determining what constitutes an information system and its associated boundary.

- 1403 k. ‘Critical infrastructure’ means systems and assets, whether physical or virtual, so vital to the  
1404 United States that the incapacity or destruction of such systems and assets would have a  
1405 debilitating impact on security, national economic security, national public health safety, or  
1406 any combination of those matters (42 U.S.C., § 5195c(e)).
- 1407 l. ‘Environment of operation’ means the physical, technical, and organizational setting in  
1408 which an information system operates.
- 1409 m. ‘Hybrid control’ means a control that is implemented in an information system in part as a  
1410 common control and in part as a system-specific control.
- 1411 n. ‘Information security architecture’ means an embedded, integral part of the enterprise  
1412 architecture that describes the structure and behavior of the enterprise security processes,  
1413 information security systems, personnel, and organizational subunits, showing their  
1414 alignment with the enterprise’s mission and strategic plans.
- 1415 o. ‘Information security continuous monitoring’ means maintaining ongoing awareness of  
1416 information security, vulnerabilities, and threats to support organizational risk management  
1417 decisions.<sup>4</sup>
- 1418 p. ‘Information system resilience’ means the ability of an information system to continue to: (i)  
1419 operate under adverse conditions or stress, even if in a degraded or debilitated state, while  
1420 maintaining essential operational capabilities; and (ii) recover to an effective operational  
1421 posture in a time frame consistent with mission needs.
- 1422 q. ‘Initial authorization’ means the initial (start-up) risk determination and risk acceptance  
1423 decision based on a zero-base review of the information system conducted prior to its  
1424 entering the operations/maintenance phase of the system development life cycle. The zero-  
1425 base review includes an assessment of all security and privacy controls (i.e., system-specific,  
1426 hybrid, and common controls) contained in a security plan or in a privacy plan and  
1427 implemented within an information system or the environment in which the system operates.
- 1428 r. ‘National security system’ means any information system (including any telecommunications  
1429 system) used or operated by an agency or by a contractor of an agency, or other organization  
1430 on behalf of an agency: (i) the function, operation, or use of which involves intelligence  
1431 activities; involves cryptologic activities related to national security; involves command and  
1432 control of military forces; involves equipment that is an integral part of a weapon or weapons  
1433 system; or is critical to the direct fulfillment of military or intelligence missions (excluding a  
1434 system that is to be used for routine administrative and business applications, for example,  
1435 payroll, finance, logistics, and personnel management applications); or (ii) is protected at all  
1436 times by procedures established for information that have been specifically authorized under  
1437 criteria established by an Executive Order or an Act of Congress to be kept classified in the  
1438 interest of national defense or foreign policy (44 U.S.C. § 3552).
- 1439 s. ‘Ongoing authorization’ means the risk determinations and risk acceptance decisions  
1440 subsequent to the initial authorization, taken at agreed-upon and documented frequencies in  
1441 accordance with the organization’s mission/business requirements and organizational risk

---

<sup>4</sup> The terms *continuous* and *ongoing* in this context mean that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organizational information.

- 1442 tolerance. Ongoing authorization is a time-driven or event-driven authorization process  
1443 whereby the authorizing official is provided with the necessary and sufficient information  
1444 regarding the security and privacy state of the information system to determine whether or  
1445 not the mission/business risk of continued system operation is acceptable.
- 1446 t. ‘Overlay’ means a specification of security and/or privacy controls, control enhancements,  
1447 supplemental guidance, and other supporting information employed during the tailoring  
1448 process, that is intended to complement (and further refine) security control baselines. The  
1449 overlay specification may be more stringent or less stringent than the original security control  
1450 baseline specification and can be applied to multiple information systems.
- 1451 u. ‘Privacy continuous monitoring’ means maintaining ongoing awareness of privacy risks and  
1452 assessing privacy controls at a frequency sufficient to ensure compliance with applicable  
1453 requirements and to adequately protect personally identifiable information.
- 1454 v. ‘Privacy control’ means the administrative, technical, and physical safeguards employed  
1455 within organizations to protect and ensure the proper handling of personally identifiable  
1456 information or prevent activities that create privacy risk.
- 1457 w. ‘Privacy control assessment’ means the testing or evaluation of privacy controls to determine  
1458 the extent to which the controls are implemented correctly, operating as intended, and  
1459 producing the desired outcome with respect to meeting the privacy requirements for an  
1460 information system or organization.
- 1461 x. ‘Privacy program plan’ means a formal document that provides an overview of the privacy  
1462 requirements for an organization-wide privacy program and describes the program  
1463 management controls and common controls in place or planned for meeting those  
1464 requirements. The privacy program plan and the information security program plan may be  
1465 integrated into one consolidated document.
- 1466 y. ‘Privacy plan’ means a formal document that provides an overview of the privacy  
1467 requirements for an information system or program and describes the privacy controls in  
1468 place or planned for meeting those requirements. The privacy plan and the security plan may  
1469 be integrated into one consolidated document.
- 1470 z. ‘Reauthorization’ means the static, single point-in-time risk determination and risk  
1471 acceptance decision that occurs after initial authorization. In general, reauthorization actions  
1472 may be time-driven or event-driven; however, under ongoing authorization, reauthorization is  
1473 typically an event-driven action initiated by the authorizing official or directed by the Risk  
1474 Executive (function) in response to an event that drives information security or privacy risk  
1475 above the previously agreed-upon organizational risk tolerance.
- 1476 aa. ‘Risk’ means a measure of the extent to which an entity is threatened by a potential  
1477 circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude  
1478 of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of  
1479 occurrence.
- 1480 bb. ‘Risk management’ means the program and supporting processes to manage information  
1481 security and privacy risk to organizational operations (including mission, functions, image,  
1482 reputation), organizational assets, individuals, other organizations, and the Nation, and  
1483 includes: establishing the context for risk-related activities; assessing risk; responding to  
1484 risk once determined; and monitoring risk over time.

- 1485 cc. 'Risk response' means accepting, avoiding, mitigating, sharing, or transferring risk to  
1486 organizational operations, organizational assets, individuals, other organizations, or the  
1487 Nation.
- 1488 dd. 'Security category' means the characterization of information or an information system  
1489 based on an assessment of the potential impact that a loss of confidentiality, integrity, or  
1490 availability of such information or information system would have on organizational  
1491 operations, organizational assets, individuals, other organizations, and the Nation.
- 1492 ee. 'Security control' means the safeguards or countermeasures prescribed for an information  
1493 system or an organization to protect the confidentiality, integrity, and availability of the  
1494 system and its information.
- 1495 ff. 'Security control assessment' means the testing or evaluation of security controls to  
1496 determine the extent to which the controls are implemented correctly, operating as  
1497 intended, and producing the desired outcome with respect to meeting the security  
1498 requirements for an information system or organization.
- 1499 gg. 'Security control baseline' means the set of minimum security controls defined for a low-  
1500 impact, moderate-impact, or high-impact information system.
- 1501 hh. 'Security program plan' means a formal document that provides an overview of the  
1502 security requirements for an organization-wide information security program and describes  
1503 the program management controls and common controls in place or planned for meeting  
1504 those requirements. The security program plan and the security program plan may be  
1505 integrated into one consolidated document.
- 1506 ii. 'Security plan' means a formal document that provides an overview of the security  
1507 requirements for an information system or an information security program and describes  
1508 the security controls in place or planned for meeting those requirements. The security plan  
1509 and the privacy plan may be integrated into one consolidated document.
- 1510 jj. 'Supply chain' means a linked set of resources and processes between multiple tiers of  
1511 developers that begins with the sourcing of products and services and extends through the  
1512 design, development, manufacturing, processing, handling, and delivery of products and  
1513 services to the acquirer.
- 1514 kk. 'System-specific control' means a control for an information system that has not been  
1515 designated as a common control or the portion of a hybrid control that is to be  
1516 implemented within an information system.
- 1517 ll. 'Tailoring' means the process by which security control baselines are modified by  
1518 identifying and designating common controls; applying scoping considerations; selecting  
1519 compensating controls; assigning specific values to organization-defined control  
1520 parameters; supplementing baselines with additional controls or control enhancements; and  
1521 providing additional specification information for control implementation. The tailoring  
1522 process may also be applied to privacy controls.
- 1523 mm. 'Trustworthiness' means the degree to which an information system can be expected to  
1524 preserve the confidentiality, integrity, and availability of the information being processed,  
1525 stored, or transmitted by the system across a full range of threats.

1526 nn. ‘Trustworthy information system’ means a system that is believed to be capable of  
1527 operating within defined levels of risk despite the environmental disruptions, human errors,  
1528 structural failures, and purposeful attacks that are expected to occur in its environment of  
1529 operation.

#### 1530 4. General Requirements

- 1531 a. Agencies must develop, implement, document, maintain, and oversee agency-wide  
1532 information security and privacy programs including people, processes, and technologies to:
- 1533 1) Provide for appropriate agency information security and privacy policies, planning,  
1534 budgeting, management, implementation, and oversight;
  - 1535 2) Cost-effectively manage information security risk, which includes reducing such risk to  
1536 an acceptable level;
  - 1537 3) Ensure compliance with all applicable privacy requirements in law, regulation, and  
1538 policy, and use privacy impact assessments and other tools to analyze and address  
1539 privacy risks;
  - 1540 4) Protect information and information systems from unauthorized access, use, disclosure,  
1541 disruption, modification, or destruction in order to provide for their confidentiality,  
1542 integrity, and availability;
  - 1543 5) Provide adequate security for all information, including PII, created, collected,  
1544 processed, stored, transmitted/disseminated, or disposed of by or on behalf of the Federal  
1545 Government, to include Federal information residing in contractor information systems  
1546 and networks;
  - 1547 6) Provide information security safeguards and countermeasures commensurate with the  
1548 risk from unauthorized access, use, disclosure, disruption, modification, or destruction of  
1549 information collected or maintained by or on behalf of the agency and information  
1550 systems used or operated by an agency, or by a contractor of an agency or other  
1551 organization on behalf of an agency;
  - 1552 7) Implement an agency-wide risk management approach that frames, assesses, responds  
1553 to, and monitors information security risk across three organizational tiers (i.e.,  
1554 organization level, mission/business process level, and information system level);<sup>5</sup>
  - 1555 8) Implement a risk management framework to guide and inform the categorization of  
1556 Federal information and information systems; the selection, implementation, and  
1557 assessment of security and privacy controls; the authorization of information systems  
1558 and common controls; and the continuous monitoring of information systems and  
1559 environments of operation;
  - 1560 9) Ensure, for information systems and the environments in which those systems operate,  
1561 that security and privacy controls are implemented correctly, operating as intended, and  
1562 continually monitored and assessed; that procedures are in place to ensure that security  
1563 and privacy controls remain effective over time; and that steps are taken to maintain risk  
1564 at an acceptable level within organizational risk tolerance;

---

<sup>5</sup> Refer to NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, for additional information.

- 1565 10) Implement policies and procedures to ensure that all personnel are held accountable for  
1566 complying with agency-wide information security and privacy programs; and
- 1567 11) Ensure that performance plans for all Federal employees include an element addressing  
1568 the need to adhere to Federal and agency-specific requirements for the protection of  
1569 information and information systems; and for individuals with significant security and  
1570 privacy responsibilities, include requirements regarding their role in protecting  
1571 information and information systems.
- 1572 b. Agencies must protect Controlled Unclassified Information (CUI) in accordance with  
1573 requirements set forth by the National Archives and Records Administration.
- 1574 c. Agencies must implement security and privacy policies, standards, and procedures that are  
1575 consistent and compliant with statutory and governmentwide requirements as well as  
1576 applicable security- and privacy-related policies, standards, and procedures issued by the  
1577 Office of Management and Budget (OMB), the Department of Commerce (DOC), the  
1578 Department of Homeland Security (DHS), the General Services Administration (GSA), and  
1579 the Office of Personnel Management (OPM). This includes following the standards and  
1580 guidelines contained in Federal Information Processing Standards (FIPS) and NIST (800-  
1581 series) Special Publications.

1582 **5. Specific Requirements<sup>6</sup>**

1583 a. Security Categorization

1584 Agencies must:

- 1585 1) Identify appropriate authorization boundaries for information systems; and
- 1586 2) Categorize information and information systems, in accordance with FIPS Publication  
1587 199 and NIST Special Publication 800-60, considering potential adverse security and  
1588 privacy impacts to organizational operations and assets, individuals, other organizations,  
1589 and the Nation.

1590 b. Planning and Budgeting, Capital Planning, and Enterprise Architecture

1591 Agencies must:

- 1592 1) Identify and plan for the resources needed to implement information security and  
1593 privacy programs;
- 1594 2) Ensure that information security and privacy is addressed throughout the life cycle of  
1595 each agency information system, and that security and privacy activities and costs are  
1596 explicitly identified and included in IT investment capital plans and budgetary requests;
- 1597 3) Ensure that capital investment plans submitted to OMB as part of the budget process  
1598 meet the information security and privacy requirements appropriate for the life cycle  
1599 stage of the investment; and

---

<sup>6</sup> The requirements in this section represent those areas deemed to be of fundamental importance to the achievement of effective agency information security programs and those areas deemed to require specific emphasis by OMB. The security programs developed and executed by agencies need not be limited to the aforementioned areas but can employ a comprehensive set of safeguards and countermeasures based on the principles, concepts, and methodologies defined in the suite of NIST standards and guidelines.

1600 4) Incorporate information security and privacy requirements into the organization's  
1601 enterprise architecture to ensure that information systems and the environments in which  
1602 those systems operate, achieve the necessary levels of trustworthiness, protection, and  
1603 resilience.

1604 c. Plans, Controls, and Assessments

1605 Agencies must:

1606 1) Develop information security program and privacy program plans that provide an  
1607 overview of the organization-wide information security and privacy requirements and  
1608 describe the program management controls and common controls in place or planned for  
1609 meeting those requirements;

1610 2) Implement a risk-based security control selection process for information systems and  
1611 environments of operation that satisfies the minimum information security requirements  
1612 in FIPS Publication 200 and security control baselines in NIST Special Publication 800-  
1613 53, tailored as appropriate;

1614 3) Implement a privacy control selection process for information systems and environments  
1615 of operation that satisfies the privacy requirements in OMB guidance, including, but not  
1616 limited to, Appendix I to this Memorandum, OMB Circular No. A-108, *Federal Agency  
1617 Responsibilities for Review, Reporting, and Publication under the Privacy Act*, and  
1618 NIST Special Publication 800-53;

1619 4) Develop security and privacy plans for information systems and environments of  
1620 operation to record security and privacy controls and appropriate implementation details;

1621 5) Designate common controls in order to provide cost-effective security and privacy  
1622 capabilities that can be inherited by multiple organizational information systems;

1623 6) Implement security controls and privacy controls in information systems and  
1624 environments of operation using architectural and systems/security engineering  
1625 principles, practices, and techniques;

1626 7) Deploy effective security controls to provide Federal employees and contractors with  
1627 multifactor authentication, digital signature, and encryption capabilities that provide  
1628 assurance of identity and are interoperable and accepted across all Executive Branch  
1629 agencies;

1630 8) Assess all selected and implemented security and privacy controls in organizational  
1631 information systems (and environments in which those systems operate) prior to  
1632 operation, and periodically thereafter, consistent with the frequency defined in the  
1633 organizational information security continuous monitoring (ISCM) and privacy  
1634 continuous monitoring (PCM) strategies and the organizational risk tolerance;

1635 9) Conduct and record the results of security control assessments and privacy control  
1636 assessments in security and privacy assessment reports, respectively;

1637 10) Use agency Plans of Action and Milestones (POA&Ms), and make available or provide  
1638 access to OMB, DHS, Inspectors General, and the Government Accountability Office,  
1639 upon request, to record and manage the mitigation and remediation of identified

- 1640 weaknesses and deficiencies, not associated with accepted risks, in organizational  
1641 information systems and environments of operation; and
- 1642 11) Obtain approval from the authorizing official for connections from the information  
1643 system, as defined by its authorization boundary, to other information systems based on  
1644 the risk to the organization's operations and assets, individuals, other organizations, and  
1645 the Nation.
- 1646 d. Authorization and Continuous Monitoring
- 1647 Agencies must:
- 1648 1) Designate senior Federal officials to formally: (i) authorize an information system to  
1649 operate; and (ii) authorize organization-designated common controls for use based on a  
1650 determination of, and explicit acceptance of, the information security risk to  
1651 organizational operations and assets, individuals, other organizations, and the Nation, and  
1652 prior to operational status;
- 1653 2) Complete an initial authorization for each information system and all organization-  
1654 designated common controls;
- 1655 3) Transition information systems and common controls to an ongoing authorization  
1656 process when eligible for such a process and with the formal approval of the respective  
1657 authorizing officials;
- 1658 4) Reauthorize information systems and common controls as needed, on a time- or event-  
1659 driven basis in accordance with organizational risk tolerance;
- 1660 5) Develop an ISCM strategy and PCM strategy to address information security and  
1661 privacy risks and requirements across the organizational risk management tiers (i.e.,  
1662 organization/governance tier, mission/business process tier, and/or information system  
1663 tier);<sup>7</sup>
- 1664 6) Implement and periodically update the ISCM strategy and PCM strategy to reflect: (i)  
1665 the effectiveness of deployed controls; (ii) significant changes to information systems  
1666 and environments of operations; and (iii) adherence to Federal statutes, policies,  
1667 directives, instructions, regulations, standards, and guidelines;
- 1668 7) Ensure that all selected and implemented controls are addressed in the ISCM strategy  
1669 and PCM strategy and are effectively monitored on an ongoing basis, as determined by  
1670 the agency's ISCM and PCM programs;<sup>8</sup>
- 1671 8) Establish and maintain an ISCM program that:
- 1672 a) Provides an understanding of organizational risk tolerance and helps officials set  
1673 priorities and manage information security risk consistently throughout the  
1674 organization;
- 1675 b) Includes metrics that provide meaningful indications of security status at all  
1676 organizational tiers;

---

<sup>7</sup> The ISCM strategy and PCM strategy may be integrated into one consolidated continuous monitoring strategy.

<sup>8</sup> The ISCM program and PCM program may be integrated into one consolidated continuous monitoring program.

- 1677 c) Ensures the continued effectiveness of all security controls selected and implemented  
1678 by monitoring controls with the frequencies specified in the ISCM strategy;
- 1679 d) Verifies compliance with information security requirements derived from  
1680 missions/business functions, Federal statutes, directives, instructions, regulations,  
1681 policies, and standards/guidelines;
- 1682 e) Is informed by all applicable organizational IT assets to help maintain visibility into  
1683 the security of the assets;
- 1684 f) Ensures knowledge and control of changes to information systems and environments  
1685 of operation; and
- 1686 g) Maintains awareness of threats and vulnerabilities;
- 1687 9) Establish and maintain a PCM program that:
- 1688 a) Ensures continued compliance with all applicable privacy requirements;
- 1689 b) Verifies the continued effectiveness of all privacy controls selected and implemented  
1690 across all organizational tiers;
- 1691 c) Includes appropriate metrics to monitor the effective implementation of privacy  
1692 requirements and privacy controls across all organizational tiers;
- 1693 d) Monitors changes to information systems and environments of operation that collect,  
1694 process, store, maintain, use, or disseminate PII; and
- 1695 e) Maintains adequate awareness of any threats and vulnerabilities that may affect PII  
1696 and impact individual privacy;
- 1697 10) Ensure that a robust ISCM program and PCM program are in place before organizational  
1698 information systems or common controls are eligible for ongoing authorization; and
- 1699 11) Leverage available Federal shared services, where practicable and appropriate.
- 1700 e. Privacy Controls for Federal Information Systems and Organizations
- 1701 The senior agency official for privacy (SAOP) has overall agency-wide responsibility and  
1702 accountability for developing, implementing, and maintaining an organization-wide  
1703 governance and privacy program to ensure compliance with all applicable laws, regulations,  
1704 and policies regarding the collection, use, maintenance, dissemination, and disposal of PII by  
1705 programs and information systems. The SAOP must:
- 1706 1) Develop a PCM strategy to address privacy risks and requirements across the  
1707 organizational risk management tiers (i.e., organization/governance tier,  
1708 mission/business process tier, and/or information system tier);
- 1709 2) Establish and maintain a PCM program to maintain ongoing awareness of privacy risks  
1710 and assess privacy controls at a frequency sufficient to ensure compliance with  
1711 applicable requirements and to adequately protect PII;
- 1712 3) Review IT capital investment plans and budgetary requests to ensure that privacy  
1713 requirements (and associated privacy controls), as well as any associated costs, are  
1714 explicitly identified and included;

- 1715 4) Review and approve, in accordance with NIST FIPS Publication 199 and Special  
1716 Publication 800-60, the categories of information systems that collect, process, store,  
1717 maintain, or disseminate PII;
- 1718 5) Designate system-specific, hybrid, and common privacy controls;
- 1719 6) Review and approve the privacy plans for organizational information systems prior to  
1720 authorization, reauthorization, or ongoing authorization;
- 1721 7) Conduct privacy control assessments to ensure that privacy controls are implemented  
1722 correctly, operating as intended, and effective in satisfying privacy requirements; and
- 1723 8) Review authorization packages and determine that all applicable privacy requirements  
1724 are met and the risk to PII is sufficiently addressed prior to authorizing officials making  
1725 risk determination and acceptance decisions.

1726 f. Incident Response

1727 Agencies must:

- 1728 1) Maintain formal security and privacy incident response capabilities and mechanisms to  
1729 include breach notification and adequate training and awareness for employees and  
1730 contractors on how to report and respond to security and privacy incidents;
- 1731 2) Report security and privacy incidents to DHS, the SAOP, their respective Inspectors  
1732 General and General Counsel, and law enforcement in accordance with procedures  
1733 issued by OMB;
- 1734 3) Implement formal security and privacy incident policies to include definitions, detection  
1735 and analysis, containment, internal and external notification and reporting requirements,  
1736 incident reporting methods, post-incident procedures, roles and responsibilities, and  
1737 guidance on how to mitigate impacts to the agency and its respondents following an  
1738 incident;
- 1739 4) Establish clear roles and responsibilities to ensure the oversight and coordination of  
1740 incident response activities and that incidents are appropriately reported, investigated  
1741 and handled;
- 1742 5) Periodically test incident response procedures to ensure effectiveness of such  
1743 procedures;
- 1744 6) Document lessons learned for incident response and update procedures as necessary; and
- 1745 7) Provide reports on incidents as required by FISMA, OMB policy, and DHS binding  
1746 operational directives.

1747 g. Awareness and Training

1748 Agencies must:

- 1749 1) Develop and maintain agency-wide information security and privacy awareness and  
1750 training programs;
- 1751 2) Ensure that the security and privacy awareness and training programs are consistent with  
1752 applicable standards and guidelines issued by OMB, NIST, and OPM;

- 1753 3) Apprise agency personnel about available assistance and technical security and privacy  
1754 products and techniques;
- 1755 4) Provide foundational as well as more advanced levels of security and privacy awareness  
1756 training to information system users (including managers, senior executives, and  
1757 contractors) and ensure that measures are in place to test the knowledge level of  
1758 information system users;
- 1759 5) Provide role-based security and privacy training to personnel with assigned security and  
1760 privacy roles and responsibilities before authorizing access to the information system or  
1761 performing assigned duties;
- 1762 6) Establish rules of behavior, that include consequences for violating rules of behavior, for  
1763 personnel having access to organizational information and information systems;
- 1764 7) Ensure that agency personnel have read and agreed to abide by the rules of behavior for  
1765 the information systems for which they require access prior to being granted access; and
- 1766 8) Consider consequences of violating rules of behavior to include reprimand, suspension,  
1767 removal, or other actions in accordance with applicable law and agency policy.
- 1768 h. Additional Measures to Protect the Confidentiality, Integrity, and Availability of Federal  
1769 Information and Information Systems
- 1770 Agencies must:
- 1771 1) Implement a policy of least functionality by only permitting the use of programs,  
1772 applications, functions, ports, protocols, and/or services that are necessary in meeting  
1773 mission or business needs;
- 1774 2) Implement a policy of least privilege by minimizing the number of information system  
1775 privileges that are needed to perform functions;
- 1776 3) Implement a policy of separation of duties to address the potential for abuse of  
1777 authorized privileges and help to reduce the risk of malevolent activity without  
1778 collusion;
- 1779 4) Audit the execution of information system functions by privileged users to detect misuse  
1780 and to help mitigate the risk from insider threats;
- 1781 5) Prohibit the use of unsupported information system components<sup>9</sup> unless there is an  
1782 overriding mission necessity validated by the Deputy Secretary or equivalent;
- 1783 6) Implement and maintain current updates for all software and firmware components of  
1784 information systems;<sup>10</sup>
- 1785 7) For systems that promote public access, ensure that identity proofing, registration, and  
1786 authentication processes provide assurance of identity consistent with security and

---

<sup>9</sup> Includes hardware, software, or firmware components no longer supported by developers, vendors, or manufacturers through the availability of software patches, firmware updates, replacement parts, and maintenance contracts. NIST Special Publication 800-53 provides additional guidance on unsupported software components.

<sup>10</sup> Security-relevant software and firmware updates include, for example, patches, service packs, hot fixes, device drivers, basic input output system (BIOS), and antivirus signatures.

- 1787 privacy requirements, in accordance with Executive Order 13681,<sup>11</sup> OMB policy, and  
 1788 NIST standards and guidelines;
- 1789 8) Require use of multifactor authentication for employees and contractors in accordance  
 1790 with governmentwide identification standards;
- 1791 9) Encrypt all moderate- and high-impact information at rest or in transit, unless the ability  
 1792 to do so is technically infeasible and the risk of not encrypting is accepted by the  
 1793 authorizing official;
- 1794 10) Implement the current encryption algorithms in accordance with NIST standards and  
 1795 guidelines;
- 1796 11) Develop and implement policies and procedures to support employees and contractors in  
 1797 uniformly applying digital signatures to secure documents and communications;
- 1798 12) Implement attribute-based access security controls to control and monitor access to  
 1799 Federal information;
- 1800 13) Implement digital rights management capabilities to control the distribution and prevent  
 1801 the unauthorized alteration or disclosure of Federal information;
- 1802 14) Implement measures to protect against supply chain threats to information systems,  
 1803 system components, or information system services by employing agency-defined  
 1804 security safeguards as part of a comprehensive, defense-in-breadth information security  
 1805 strategy; and
- 1806 15) Employ contingency planning and resiliency concepts and methodologies to ensure the  
 1807 confidentiality, integrity, and availability of Federal information and information  
 1808 systems supporting agency missions and business operations.
- 1809 i. Contracts and Grants
- 1810 Agencies must ensure that terms and conditions in contracts and grants involving the  
 1811 processing, storage, transmission, and destruction of Federal information are sufficient to  
 1812 enable agencies to meet necessary mitigation, oversight, and law enforcement requirements  
 1813 concerning Federal information, including but not limited to, sufficient provisions for  
 1814 government notification and access, as well as cooperation with agency personnel and  
 1815 Inspectors General, particularly in the event of a data breach or related security or privacy  
 1816 incident. Refer to the Federal Acquisition Regulation, Part 7, Acquisition Planning, Subpart  
 1817 7.1, Acquisition Plans for additional requirements pertaining to information technology  
 1818 acquisitions.
- 1819 j. Oversight of Nonfederal Entities Hosting Federal Information
- 1820 Agencies must:
- 1821 1) Provide oversight of information systems used or operated by contractors or other  
 1822 entities on behalf of the Federal government or that contain Federal information, to  
 1823 include:

---

<sup>11</sup> Executive Order 13681, *Improving the Security of Consumer Financial Transactions*, October 2014.

- 1824 a) Documenting policies and procedures for information security and privacy oversight  
 1825 of systems operated on the organization’s behalf, or that contain Federal information,  
 1826 by contractors or other entities;
- 1827 b) Ensuring that appropriate security and privacy controls of such information systems  
 1828 and services are effectively implemented and comply with Federal standards and  
 1829 guidelines and organizational requirements;
- 1830 c) Maintaining and continuously updating a complete inventory of information systems  
 1831 and system components using automated reporting, cataloguing, and inventory tools;
- 1832 d) Ensuring that the inventory identifies interfaces between these systems and  
 1833 organization-operated systems;
- 1834 e) Ensuring that the appropriate procedures are in place for incident response for these  
 1835 systems including timelines for breach notification and required data points;
- 1836 f) Requiring appropriate agreements (e.g., MOUs, Interconnection Security  
 1837 Agreements, contracts) for interfaces between these systems and agency-owned and  
 1838 operated systems; and
- 1839 g) Implementing policies and procedures to ensure that systems that are owned or  
 1840 operated by contractors or entities that contain Federal information are compliant  
 1841 with FISMA requirements, OMB policies, and applicable NIST standards and  
 1842 guidelines; and
- 1843 2) Collaborate with nonfederal entities, and other agencies as appropriate, to ensure that  
 1844 security and privacy requirements pertaining to these nonfederal entities, such as State,  
 1845 local, tribal, and territorial governments, are unified and consistent to the greatest extent  
 1846 possible.
- 1847 k. Mitigation of Deficiencies and Issuance of Status Reports
- 1848 Agencies must correct deficiencies that are identified through information security  
 1849 assessments, ISCM programs, or internal/external audits and reviews. OMB Circular No. A-  
 1850 123, *Management’s Responsibility for Internal Control*, provides guidance to determine  
 1851 whether a deficiency in controls is material when so judged by the agency head against other  
 1852 agency deficiencies. Material deficiencies must be included in the annual Federal Managers  
 1853 Financial Integrity Act (FMFIA) report, and remediation tracked and managed through the  
 1854 agency’s Plan of Action and Milestones (POA&M) process. Less significant deficiencies  
 1855 need not be included in the FMFIA report, but must be tracked and managed through the  
 1856 agency’s POA&M process.
- 1857 l. Reporting
- 1858 Agencies must provide FISMA and privacy management reports in accordance with  
 1859 processes established by OMB and DHS.
- 1860 m. Cybersecurity Framework
- 1861 The Cybersecurity Framework was developed by NIST in response to Executive Order  
 1862 13636, *Improving Critical Infrastructure Cybersecurity*. The Framework describes five core  
 1863 cybersecurity functions (i.e., Identify, Protect, Detect, Respond, and Recover) that may be  
 1864 helpful in raising awareness and facilitating communication among agency stakeholders,

1865 including executive leadership. The Cybersecurity Framework may also be helpful in  
1866 improving communications across organizations, allowing cybersecurity expectations to be  
1867 shared with business partners, suppliers, and among sectors. The Framework is not intended  
1868 to duplicate the current information security and risk management practices in place within  
1869 the Federal Government. However, in the course of managing information security risk using  
1870 the established NIST Risk Management Framework and associated security standards and  
1871 guidelines required by FISMA, agencies can leverage the Cybersecurity Framework to  
1872 complement their current information security programs. NIST will provide additional  
1873 guidance on how agencies can use the Cybersecurity Framework and in particular, how the  
1874 two frameworks can work together synergistically to help agencies develop, implement, and  
1875 continuously improve their information security programs.

1876 n. Independent Evaluations

1877 Agencies must:

- 1878 1) Perform an independent evaluation of the information security programs and practices to  
1879 determine the effectiveness of such programs and practices. The evaluation may include  
1880 an evaluation of their privacy program and practices, as appropriate. Each evaluation  
1881 must include:
  - 1882 a) Testing of the effectiveness of information security policies, procedures, and  
1883 practices of a representative and diverse subset of the agency's information systems;
  - 1884 b) An assessment of the effectiveness of the information security policies, procedures,  
1885 and practices of the agency; and
  - 1886 c) Separate presentations, as appropriate, regarding information security relating to  
1887 national security systems.
- 1888 2) For each agency with an Inspector General appointed under the Inspector General Act of  
1889 1978, the annual evaluation required by this section must be performed by the Inspector  
1890 General or by an independent external auditor, as determined by the Inspector General of  
1891 the agency. For agencies in which the Inspector General Act of 1978 does not apply, the  
1892 head of the agency shall engage an independent external auditor to perform the  
1893 evaluation.

1894 **6. Assignment of Responsibilities**

1895 a. Department of Commerce

1896 The Secretary of Commerce must:

- 1897 1) Develop and issue appropriate standards and guidelines for the security of  
1898 information in Federal information systems, and systems which create, collect,  
1899 process, store, transmit/disseminate, or dispose of information on behalf of the  
1900 Federal Government;
- 1901 2) Review and update guidelines for information security awareness, training, and  
1902 education and accepted information security practices, with assistance from  
1903 OPM;

- 1904 3) Provide agencies guidance for security planning to assist in their development of  
1905 security plans;
- 1906 4) Provide guidance and assistance, as appropriate, to agencies concerning cost-  
1907 effective security controls;
- 1908 5) Evaluate new information technologies to assess their security vulnerabilities,  
1909 with technical assistance from the Department of Defense (DoD) and DHS; and
- 1910 6) Follow a transparent process that allows and addresses input from the agencies  
1911 and the public when developing standards and guidelines.
- 1912 b. Department of Homeland Security
- 1913 The Secretary of Homeland Security must:
- 1914 1) Monitor and assist agencies with the implementation of information security policies and  
1915 practices for information systems;
- 1916 2) Assist OMB in carrying out its information security oversight and policy responsibilities;
- 1917 3) Develop and oversee the implementation of binding operational directives that  
1918 implement the policies, principles, standards, and guidelines developed by OMB, that  
1919 focus on:
- 1920 a) Requirements for the mitigation of exigent risks to information systems;
- 1921 b) Requirements for reporting incidents to the Federal information security incident  
1922 center; and
- 1923 c) Other operational requirements, as deemed necessary by OMB;
- 1924 4) Coordinate the development of binding operational directives and the oversight of the  
1925 implementation of such directives with OMB to ensure consistency with OMB policies  
1926 and NIST standards and guidelines;
- 1927 5) Consult with the Director of NIST regarding any binding operational directives that  
1928 implement or affect the standards and guidelines developed by NIST;
- 1929 6) Revise or repeal binding operational directives when OMB determines that the directives  
1930 are not in accordance with OMB policies, principles, standards, or guidelines;
- 1931 7) Convene meetings with senior agency officials to help ensure effective implementation  
1932 of information security policies and procedures;
- 1933 8) Coordinate governmentwide efforts on information security policies and practices,  
1934 including consultation with the Chief Information Officers Council and NIST;
- 1935 9) Manage governmentwide information security programs and provide and operate  
1936 Federal information security shared services, as directed by OMB;
- 1937 10) Provide operational and technical assistance to agencies in implementing policies,  
1938 principles, standards, and guidelines on information security. This includes:
- 1939 a) Operating the Federal information security incident center;

- 1940 b) Deploying technology to assist agencies to continuously diagnose and mitigate cyber  
1941 threats and vulnerabilities, with or without reimbursement and at the request of the  
1942 agency;
- 1943 c) Compiling and analyzing data on agency information security; and
- 1944 d) Developing and conducting targeted operational evaluations, including threat and  
1945 vulnerability assessments, on information systems;
- 1946 11) Provide agencies with intelligence about cyber threats, vulnerabilities, and incidents for  
1947 risk assessments;
- 1948 12) Consult with OMB to determine what other actions may be necessary to support  
1949 implementation of effective governmentwide information security programs; and
- 1950 13) Provide the public with timely notice and opportunities for comment on proposed  
1951 information security directives and procedures to the extent that such directives and  
1952 procedures affect the public or communication with the public.
- 1953 c. Department of Defense
- 1954 The Secretary of Defense must:
- 1955 1) Provide appropriate technical advice and assistance to the Departments of  
1956 Commerce and Homeland Security; and
- 1957 2) Assist the Departments of Commerce and Homeland Security in evaluating the  
1958 vulnerabilities of emerging information technologies.
- 1959 d. Department of Justice
- 1960 The Attorney General must:
- 1961 1) Provide appropriate guidance to agencies on legal remedies regarding security  
1962 incidents and ways to report and work with law enforcement concerning such  
1963 incidents; and
- 1964 2) Pursue appropriate legal actions when security incidents occur.
- 1965 e. General Services Administration
- 1966 The Administrator of General Services must:
- 1967 1) Provide guidance to agencies on addressing security considerations when  
1968 acquiring information technology resources;
- 1969 2) Facilitate the development of contract vehicles for agencies to use in the  
1970 acquisition of cost-effective security products and services;
- 1971 3) Provide appropriate security-related services to meet the needs of agencies to the  
1972 extent that such services are cost-effective;
- 1973 4) Maintain a public key infrastructure framework to allow efficient interoperability  
1974 among executive agencies when using digital certificates; and
- 1975 5) Ensure effective security controls are in place to protect the confidentiality,  
1976 integrity, availability of the Federal public key infrastructure.

- 1977 f. Office of Personnel Management
- 1978 The Director of the Office of Personnel Management must:
- 1979 1) Ensure that its regulations concerning information security training for Federal  
1980 civilian employees are effective;
- 1981 2) Assist the Department of Commerce in updating and maintaining guidelines for  
1982 security training and education; and
- 1983 3) Determine minimum investigative requirements for Federal employees and  
1984 contractors requiring access to Federal facilities, information, and/or information  
1985 systems.

1986 **Discussion of the Major Provisions in the Appendix**

1987 **1. NIST Standards and Guidelines**

1988 NIST standards and guidelines associate each information system with an impact level. The  
1989 standards and guidelines also provide a corresponding starting set of baseline security controls  
1990 and tailoring guidance to ensure that the set of security controls in the security plan (approved by  
1991 the authorizing official) and privacy controls in the privacy plan (approved by the SAOP), satisfy  
1992 the information security, privacy, and mission/business protection needs of the organization.

1993 For non-national security programs and information systems, agencies must follow NIST  
1994 guidelines unless otherwise stated by OMB. Federal Information Processing Standards (FIPS)  
1995 are mandatory. There is flexibility within NIST's guidelines (specifically in the 800-series) in  
1996 how agencies apply those guidelines. Unless specified by additional implementing policy by  
1997 OMB, the concepts and principles described in NIST guidelines must be followed. However,  
1998 NIST guidelines generally allow agencies latitude in their application. Consequently, the  
1999 application of NIST guidelines by agencies can result in different security solutions that are  
2000 equally acceptable and compliant with the guidelines.

2001 For legacy information systems, agencies are expected to meet the requirements of, and be in  
2002 compliance, with NIST standards and guidelines within one year of their respective publication  
2003 dates unless otherwise directed by OMB. The one-year compliance date for revisions to NIST  
2004 publications applies only to new or updated material in the publications. For information systems  
2005 under development or for legacy systems undergoing significant changes, agencies are expected  
2006 to meet the requirements of, and be in compliance with, NIST standards and guidelines  
2007 immediately upon deployment of the systems.

2008 **2. Security and Privacy Assessments**

2009 Agencies must ensure that periodic testing and evaluation of the effectiveness of information  
2010 security and privacy policies, procedures, and practices are performed with a frequency  
2011 depending on risk, but no less than annually. This requirement does not imply that agencies must  
2012 assess every selected and implemented security and privacy control at least annually. Rather,  
2013 agencies must continuously monitor all implemented security and privacy controls (i.e., system-  
2014 specific, hybrid, and common controls) with a frequency determined by the organization in  
2015 accordance with the ISCM and PCM strategies. These strategies will define the specific security  
2016 and privacy controls selected for assessment during any one-year period (i.e., the annual  
2017 assessment window) with the understanding that all controls may not be formally assessed every

2018 year. Rotational assessment of security and privacy controls is consistent with the transition to  
2019 ongoing authorization and assumes the information system has completed an initial authorization  
2020 where all controls were formally assessed for effectiveness.

2021 Security and privacy control assessments should ensure that security and privacy controls  
2022 selected by agencies are implemented correctly, operating as intended, and effective in satisfying  
2023 security and privacy requirements. The security of information may change over time based on  
2024 changes in the threat, organizational missions/business functions, personnel, technology, or  
2025 environments of operation. Consequently, maintaining a capability for real-time or near real-time  
2026 analysis of the threat environment and situational awareness following a cyber-attack is  
2027 paramount. The type, rigor, and frequency of control assessments should be commensurate with  
2028 the level of awareness necessary for effectively determining information security risk that is  
2029 established by the organization's risk tolerance and risk management strategy. Technical security  
2030 tools such as malicious code scanners, vulnerability assessment products (which look for known  
2031 security weaknesses, configuration errors, and the installation of the latest patches), and  
2032 penetration testing can assist in the ongoing assessment of information systems.

### 2033 **3. Responding to Information Security Risk**

2034 Risk response identifies, evaluates, decides on, and implements appropriate courses of action to  
2035 accept, avoid, mitigate, share, or transfer risk to organizational operations and assets, individuals,  
2036 other organizations, and the Nation, resulting from the operation and use of information systems.  
2037 Identifying and analyzing alternative courses of action typically occurs at Tier 1 (organizational  
2038 governance level) or Tier 2 (mission/business process level). Alternative courses of action (i.e.,  
2039 potential risk responses) are evaluated in terms of anticipated organization-wide impacts and the  
2040 ability of organizations to continue to successfully carry out missions and business functions.  
2041 Decisions to employ risk response measures organization-wide are typically made at Tier 1,  
2042 although the decisions are informed by risk-related information from the lower tiers. At Tier 2,  
2043 alternative courses of action are evaluated in terms of anticipated impacts on missions/business  
2044 functions, the associated mission/business processes, and resource requirements. At Tier 3  
2045 (information system level), alternative courses of action tend to be evaluated in terms of the  
2046 system development life cycle or the maximum amount of time available for implementing the  
2047 selected course(s) of action. The breadth of potential risk responses is a major factor for whether  
2048 the activity is carried out at Tier 1, Tier 2, or Tier 3. Risk decisions are influenced by  
2049 organizational risk tolerance developed as part of risk framing activities at Tier 1. Organizations  
2050 can implement risk decisions at any of the risk management tiers with different objectives and  
2051 utility of information produced.

### 2052 **4. Authorization to Operate**

2053 The authorization to operate an information system and the authorization of organization-  
2054 designated common controls granted by senior Federal officials provide an important quality  
2055 control for agencies. By authorizing an information system, a Federal official accepts the risk  
2056 associated with operating that system to include the risk associated with the inherited common  
2057 controls, which may have been separately authorized by another Federal official. Authorization  
2058 is an inherently Federal responsibility and must be conducted by a Federal official. The decision  
2059 to authorize a system to operate should be based on a review of the authorization package and  
2060 includes an assessment of compliance with applicable requirements and risk to organizational

2061 operations (including mission, functions, image, and reputation), organizational assets,  
2062 individuals, other organizations, and the Nation.

2063 The decision to authorize a system, or organization-defined common controls, should be made  
2064 by the appropriate authorizing official – an agency official responsible for the associated  
2065 missions, business functions, and/or supporting infrastructure. Since the security plan and  
2066 privacy plan establish the security and privacy controls selected for implementation, those plans  
2067 are a critical part of the authorization package and should form the basis for the authorization,  
2068 supplemented by more specific information as needed. The authorizing official should consult  
2069 with the SAOP prior to making risk determination and risk acceptance decisions. The SAOP  
2070 should review authorization packages and determine that all applicable privacy requirements are  
2071 met and the risk to PII is sufficiently addressed before authorizing officials make risk  
2072 determination and risk acceptance decisions. In situations where the authorizing official and  
2073 SAOP cannot reach a final resolution regarding the appropriate protection for the organizational  
2074 information and information system, the head of the agency must review the associated risks and  
2075 requirements and makes a final determination regarding the issuance of the authorization to  
2076 operate.

## 2077 **5. Ongoing Authorization**

2078 Ongoing authorization<sup>12</sup> is a process whereby the authorizing official makes risk determination  
2079 and risk acceptance decisions subsequent to the initial authorization, taken at agreed-upon and  
2080 documented frequencies in accordance with the organization’s risk tolerance and  
2081 mission/business requirements. Ongoing authorization is a time-driven or event-driven  
2082 authorization process whereby the authorizing official is provided with the necessary and  
2083 sufficient information regarding the near real-time state of the information system and inherited  
2084 common controls to determine whether or not all applicable security and privacy requirements  
2085 have been satisfied and the mission/business risk is acceptable. Effective ongoing authorization  
2086 requires robust ISCM and PCM strategies and effective operational ISCM and PCM programs.  
2087 Agencies can move from a static, point-in-time authorization process to a dynamic, near real-  
2088 time ongoing authorization process for information systems and common controls after having  
2089 satisfied two conditions: the system and/or common controls have been granted an initial  
2090 authorization to operate by the designated authorizing official; and ISCM and PCM programs are  
2091 in place to monitor all implemented security and privacy controls with the appropriate degree of  
2092 rigor and at the appropriate frequencies in accordance with applicable ISCM and PCM strategies  
2093 and OMB and NIST guidance.

2094 Agencies must define and implement a process to specifically designate information systems  
2095 and/or common controls that have satisfied the following two conditions and have been  
2096 transitioned to ongoing authorization. The authorizing official formally acknowledges that the  
2097 information system and/or common controls are being managed under an ongoing authorization  
2098 process and accepts the responsibility for ensuring all necessary activities associated with the  
2099 ongoing authorization process are performed. Until a formal approval is obtained from the  
2100 authorizing official to transition to ongoing authorization, information systems (and common

---

<sup>12</sup> For additional information on Ongoing Authorization and its relationship to initial authorization and reauthorization, refer to NIST *Supplemental Guidance on Ongoing Authorization: Transitioning to Near Real-Time Risk Management*.

2101 controls) remain under a static authorization process with specific authorization termination  
2102 dates enforced by the agency.

## 2103 **6. Reauthorization**

2104 Reauthorization consists of a review of the information system similar to the review carried out  
2105 during the initial authorization but conducted during the operations/maintenance phase of the  
2106 system development life cycle rather than prior to that phase. In general, reauthorization actions  
2107 may be time-driven or event-driven. However, under ongoing authorization, reauthorization is  
2108 typically an event-driven action initiated by the authorizing official or directed by the Risk  
2109 Executive (function) in response to an event that drives information security above the  
2110 previously agreed-upon organizational risk tolerance. Changes in statutory requirements and  
2111 OMB or NIST guidance may also trigger a reauthorization.

2112 The reauthorization process differs from the initial authorization inasmuch as the authorizing  
2113 official can initiate: a complete zero-base review of the information system or common controls;  
2114 or a targeted review based on the type of event that triggered the reauthorization, the assessment  
2115 of risk related to the event, the risk response of the organization, and the organizational risk  
2116 tolerance. Reauthorization is a separate activity from the ongoing authorization process, though  
2117 security- and privacy-related information from the organization's ISCM and PCM programs may  
2118 still be leveraged to support reauthorization. Note also that reauthorization actions may  
2119 necessitate a review of and changes to the ISCM or PCM strategy, which may in turn affect  
2120 ongoing authorization.

## 2121 **7. Joint and Leveraged Authorizations**

2122 Agencies are encouraged to use joint and leveraged authorizations whenever practicable.<sup>13</sup> Joint  
2123 authorizations can be used when multiple organizational officials either from the same  
2124 organization or different organizations, have a shared interest in authorizing an information  
2125 system or common controls. The participating officials are collectively responsible and  
2126 accountable for the system and the common controls and jointly accept the information security  
2127 risks that may adversely impact organizational operations and assets, individuals, other  
2128 organizations, and the Nation. Organizations choosing a joint authorization approach should  
2129 work together on the planning and the execution of the Risk Management Framework tasks  
2130 described in NIST Special Publication 800-37 and document their agreement and progress in  
2131 implementing the tasks. The specific terms and conditions of the joint authorization are  
2132 established by the participating parties in the joint authorization including, for example, the  
2133 process for ongoing determination and acceptance of risk. The joint authorization remains in  
2134 effect only as long as there is mutual agreement among authorizing officials and the  
2135 authorization meets the requirements established by Federal and/or organizational policies.

2136 Leveraged authorizations can be used when an agency chooses to accept some or all of the  
2137 information in an existing authorization package generated by another agency based on the need  
2138 to use the same information resources (e.g., information system and/or services provided by the  
2139 system). The leveraging organization reviews the owning organization's authorization package  
2140 as the basis for determining risk to the leveraging organization. The leveraging organization

---

<sup>13</sup> NIST Special Publication 800-37 provides guidance on joint and leveraged security authorizations.

2141 considers risk factors such as the time elapsed since the authorization results were produced,  
2142 differences in environments of operation (if applicable), the impact of the information to be  
2143 processed, stored, or transmitted, and the overall risk tolerance of the leveraging organization.  
2144 The leveraging organization may determine that additional security measures are needed and  
2145 negotiate with the owning organization to provide such measures. To the extent that a leveraged  
2146 authorization includes an information system that collects, processes, stores, maintains,  
2147 transmits, or disseminates PII, leveraging organizations must consult their SAOP. The SAOP  
2148 may determine that additional measures are required to protect PII prior to leveraging the  
2149 authorization.

## 2150 **8. Continuous Monitoring**

2151 Agencies must develop ISCM and PCM strategies across organizational tiers (e.g.,  
2152 organization/governance tier, mission/business process tier, information system tier) and  
2153 implement ISCM and PCM activities in accordance with applicable laws, directives, policies,  
2154 instructions, regulations, standards, and guidelines. Agencies have the flexibility to develop an  
2155 overarching ISCM and PCM strategy (e.g., at the agency, bureau, or component level) that  
2156 address all information systems, or continuous monitoring strategies that address each agency  
2157 information system individually. The ISCM and PCM strategies must address all security and  
2158 privacy controls selected and implemented by agencies, including the frequency of and degree of  
2159 rigor associated with the monitoring process. ISCM and PCM strategies, which must be  
2160 approved by the SAOP and appropriate agency authorizing official, must also include all  
2161 common controls inherited by organizational information systems.

## 2162 **9. Critical Infrastructure**

2163 Agencies that operate information systems that are part of the critical infrastructure must employ  
2164 organizational assessment and management of risk to ensure that security controls for those  
2165 systems are appropriately tailored (including the deployment of additional controls, when  
2166 necessary), thus providing the required level of protection for critical Federal missions and  
2167 business operations. In addition, organizations must ensure that the privacy controls assigned to  
2168 critical infrastructure meet all applicable requirements and adequately protect individual privacy.  
2169 This includes the ongoing monitoring of deployed security and privacy controls in critical  
2170 infrastructure systems to determine the ongoing effectiveness of those controls against current  
2171 threats; improving the effectiveness of those controls, when necessary; managing associated  
2172 changes to the systems and environments of operation; and satisfying specific protection and  
2173 compliance requirements in statutes, Executive Orders, directives, and policies required for  
2174 critical infrastructure protection.

## 2175 **10. Encryption**

2176 Where technically feasible, agencies must encrypt Federal information at rest and in transit  
2177 unless otherwise protected by alternative physical safeguards. Encrypting information at rest and  
2178 in transit helps protect the confidentiality, integrity, and availability of such information by  
2179 making it less susceptible to unauthorized disclosure or modification. Encryption requirements  
2180 apply to Federal information categorized as either moderate or high impact in accordance with  
2181 FIPS Publication 199. Only FIPS-validated and NSA-approved cryptography are approved for  
2182 use in Federal information systems.

2183 **11. Digital Signatures**

2184 Digital signatures can mitigate a variety of security vulnerabilities by providing authentication  
2185 and non-repudiation capabilities, and ensuring the integrity of Federal information whether such  
2186 information is used in day-to-day operations or archived for future use. Additionally, digital  
2187 signatures can help agencies streamline mission/business processes and transition manual  
2188 processes to more automated processes to include, for example, online transactions. Because of  
2189 the advantages provided by this technology, OMB expects agencies to implement digital  
2190 signature capabilities in accordance with Federal Public Key Infrastructure (PKI) policy, and  
2191 NIST standards and guidelines. For employees and contractors, agencies should require use the  
2192 digital signature capability of the Personal Identity Verification (PIV) credentials.<sup>14</sup> For  
2193 individuals that fall outside the scope of PIV applicability, agencies should leverage approved  
2194 Federal PKI credentials when using digital signatures.

2195 **12. Identity Assurance**

2196 To streamline the process of citizens, businesses, and other partners<sup>15</sup> securely accessing  
2197 government services online requires a risk-appropriate demand of identity assurance. Identity  
2198 assurance, in an online context, is the ability of an agency to determine that a claim to a  
2199 particular identity made by an individual can be trusted to actually be the individual's "true"  
2200 identity. Citizens, businesses, and other partners that interact with the Federal Government need  
2201 to have and be able to present electronic identity credentials to identify and  
2202 authenticate themselves remotely and securely when accessing Federal information resources.  
2203 An agency needs to be able to know, to a degree of certainty commensurate with the risk  
2204 determination, that the presented electronic identity credential truly represents the individual  
2205 presenting the credential before a transaction is authorized.<sup>16</sup>

2206 To transform processes for citizens, businesses, and other partners accessing Federal services  
2207 online, OMB expects agencies to use a standards-based federated identity management approach  
2208 that enables security, privacy, ease-of-use, and interoperability among electronic authentication  
2209 systems. In doing so, agencies are expected to leverage Federal shared services intended to allow  
2210 a user to authenticate with multiple information systems across agencies by selecting from a set  
2211 of interoperable credentials that are appropriate for the level of identity assurance required.

2212 **13. Unsupported Information System Components**

2213 Unsupported information system components (e.g., when vendors are no longer providing  
2214 critical software patches) provide a substantial opportunity for adversaries to exploit new  
2215 weaknesses discovered in the currently installed components. Exceptions to replacing  
2216 unsupported system components may include, for example, systems that provide critical  
2217 mission/business capability where newer technologies are not available or where the systems are  
2218 so isolated that installing replacement components is not an option. For such systems,  
2219 organizations can establish in-house support, for example, by developing customized patches for  
2220 critical software components or secure the services of external providers who through contractual

---

<sup>14</sup> NIST FIPS 201 provides additional information on use of Personal Identity Verification credentials.

<sup>15</sup> "Other partners" may include contractors not subject to the NIST FIPS 201 identity standard.

<sup>16</sup> NIST Special Publication 800-63 provides additional guidance on identity assurance.

2221 relationships, provide ongoing support for the designated unsupported components. Such  
2222 contractual relationships can include, for example, Open Source Software value-added vendors.

#### 2223 **14. FISMA Applicability to Nonfederal Entities**

2224 The Federal Information Security Modernization Act describes Federal agency security  
2225 responsibilities as including “information collected or maintained by or on behalf of an  
2226 agency” and “information systems used or operated by an agency or by a contractor of an  
2227 agency or other organization on behalf of an agency.” FISMA requires each agency to provide  
2228 information security for the information and “information systems that support the operations  
2229 and assets of the agency, including those provided or managed by another agency, contractor,  
2230 or other source.” This includes services which are either fully or partially provided, including  
2231 agency hosted, outsourced, and cloud-based solutions.

2232 Additionally, because FISMA applies to Federal information and information systems, in certain  
2233 circumstances, its requirements also apply to a specific class of information technology that the  
2234 Clinger-Cohen Act of 1996 (40 U.S.C. § 1401(3)) did not include, i.e., “equipment that is  
2235 acquired by a Federal contractor incidental to a Federal contract.” Therefore, when Federal  
2236 information is used within incidentally acquired equipment, the agency continues to be  
2237 responsible and accountable for ensuring that FISMA requirements are met for such information.

#### 2238 **15. Other Requirements**

2239 Agencies must adhere to all other applicable information requirements such as the privacy  
2240 requirements in accordance with the Privacy Act of 1974 and OMB guidance, the Confidential  
2241 Information Protection and Statistical Efficiency Act of 2002 and OMB implementation  
2242 guidance, and to laws and regulations pertaining to management of Federal records, and other  
2243 relevant statutes, Executive Orders, Presidential Directives, and policies.

#### 2244 **References<sup>17</sup>**

- 2245 1. Privacy Act of 1974 (P.L. 93-579), December 1974.
- 2246 2. E-Government Act of 2002 (P.L. 107-347), December 2002.
- 2247 3. Federal Information Security Modernization Act of 2014 (P.L. 113-283, Title II), December  
2248 2014.
- 2249 4. Executive Order 13556, *Controlled Unclassified Information*, November 2010.
- 2250 5. Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, February 2013.
- 2251 6. Executive Order 13681, *Improving the Security of Consumer Financial Transactions*,  
2252 October 2014.
- 2253 7. National Institute of Standards and Technology Federal Information Processing Standards  
2254 Publication 199 (as amended), *Standards for Security Categorization of Federal Information  
2255 and Information Systems*.

---

<sup>17</sup> OMB policy documents can be located at [https://www.whitehouse.gov/omb/circulars\\_default](https://www.whitehouse.gov/omb/circulars_default) and [https://www.whitehouse.gov/omb/memoranda\\_default](https://www.whitehouse.gov/omb/memoranda_default).

- 2256 8. National Institute of Standards and Technology Federal Information Processing Standards  
2257 Publication 200 (as amended), *Minimum Security Requirements for Federal Information and*  
2258 *Information Systems*.
- 2259 9. National Institute of Standards and Technology Federal Information Processing Standards  
2260 Publication 201 (as amended), *Personal Identity Verification of Federal Employees and*  
2261 *Contractors*.
- 2262 10. Committee on National Security Systems Instruction 1253 (as amended), *Security*  
2263 *Categorization and Control Selection for National Security Systems*.
- 2264 11. National Institute of Standards and Technology Special Publication 800-18 (as amended),  
2265 *Guide for Developing Security Plans for Federal Information Systems*.
- 2266 12. National Institute of Standards and Technology Special Publication 800-30 (as amended),  
2267 *Guide for Conducting Risk Assessments*.
- 2268 13. National Institute of Standards and Technology Special Publication 800-37 (as amended),  
2269 *Guide for Applying the Risk Management Framework to Federal Information Systems: A*  
2270 *Security Life Cycle Approach*.
- 2271 14. National Institute of Standards and Technology Special Publication 800-39 (as amended),  
2272 *Managing Information Security Risk: Organization, Mission, and Information System View*.
- 2273 15. National Institute of Standards and Technology Special Publication 800-47 (as amended),  
2274 *Security Guide for Interconnecting Information Technology Systems*.
- 2275 16. National Institute of Standards and Technology Special Publication 800-53 (as amended),  
2276 *Security and Privacy Controls for Federal Information Systems and Organizations*.
- 2277 17. National Institute of Standards and Technology Special Publication 800-53A (as amended),  
2278 *Guide for Assessing the Security Controls in Federal Information Systems and*  
2279 *Organizations: Building Effective Security Assessment Plans*.
- 2280 18. National Institute of Standards and Technology Special Publication 800-59 (as amended),  
2281 *Guideline for Identifying an Information System as a National Security System*.
- 2282 19. National Institute of Standards and Technology Special Publication 800-60 (as amended),  
2283 *Guide for Mapping Types of Information and Information Systems to Security Categories*.
- 2284 20. National Institute of Standards and Technology Special Publication 800-63 (as amended),  
2285 *Electronic Authentication Guideline*.
- 2286 21. National Institute of Standards and Technology Special Publication 800-137 (as amended),  
2287 *Information Security Continuous Monitoring for Federal Information Systems and*  
2288 *Organizations*.
- 2289 22. National Institute of Standards and Technology *Framework for Improving Critical*  
2290 *Infrastructure Cybersecurity* (as amended).
- 2291 23. National Institute of Standards and Technology *Supplemental Guidance on Ongoing*  
2292 *Authorization: Transitioning to Near Real-Time Risk Management* (as amended).