

U.S. DEPARTMENT OF AGRICULTURE
WASHINGTON, D.C. 20250

DEPARTMENTAL REGULATION	Number: DR 3650-001
SUBJECT: Cloud Computing	DATE: September 30, 2015
	OPI: Office of the Chief Information Officer – National Information Technology Center

<u>Section</u>	<u>Page</u>
1. Purpose	1
2. Special Instructions/Cancellations	1
3. Scope	2
4. Policy	3
5. Acquisition Guidance	3
6. Roles and Responsibilities	4
7. Policy Exceptions	7
8. Inquiries	8
Appendix A Acronyms and Abbreviations	A-1
Appendix B Authorities and References	B-1
Appendix C Definitions	C-1
Appendix D Cost Analysis when Selecting a Cloud Service Provider	D-1
Appendix E Annual Certification of Cloud Service Offerings	E-1

1. PURPOSE

This Departmental Regulation (DR) establishes the United States Department of Agriculture (USDA) policy for implementing the Federal Cloud Computing Initiative across the USDA's information technology (IT) portfolio of information and information systems.

2. SPECIAL INSTRUCTIONS/CANCELLATIONS

- a. This DR adheres to the guidance identified in the National Institute of Standards and Technology (NIST) Special Publication [\(SP\) 800-53](#) Revision 4, *Security and Privacy*

- Controls for Federal Information Systems and Organizations*, as amended, and the Federal Information Processing Standards Publication ([FIPS PUB\) 199](#), *Standards for Security Categorization of Federal Information and Information Systems* for information and systems with a security classification of low, moderate, or high.
- b. Per the Federal Risk and Authorization Management Program (FedRAMP) *Concept of Operations* ([CONOPS](#)), Section 4.1, “Federal agencies must use the baseline controls and accompanying FedRAMP requirements (templates, test cases, and guidance) when leveraging assessments and authorizations or initiating assessments for cloud services.”
 - c. Per the Office of Management and Budget (OMB) [Memorandum for Chief Information Officers](#), *Security Authorization of Information Systems in Cloud Computing Environments*, Footnote 10, “For all currently implemented cloud services or those services currently in the acquisition process prior to FedRAMP being declared operational, security authorizations must meet the FedRAMP security authorization requirement within 2 years of FedRAMP being declared operational.” FedRAMP reached initial operating capability on June 6, 2012.
 - d. The OMB memorandum further provides in Footnote 4 that “Executive departments or agencies that: (i) select a private cloud deployment model (i.e., the cloud environment is operated solely for the use of their organization); (ii) implement the private cloud on premise (i.e., within a Federal facility); and (iii) are not providing cloud services from the cloud-based information system to any external entities (including bureaus, components, or subordinate organizations within their agencies), are exempted from the FedRAMP requirements. In such situations, Executive departments or agencies shall continue to comply with the current [FISMA](#) [*Federal Information Security Management Act*] requirements and the appropriate NIST security standards and guidelines for private cloud-based information systems.”
 - e. This directive does not apply to classified systems, National Security Systems (NSS), or National Security Information (NSI).

3. SCOPE

- a. This directive applies to all USDA cloud capable information systems in USDA’s information systems portfolio (see Appendix C, paragraphs g and j for information system definitions). USDA shall comply with NIST [SP 800-145](#), *The NIST Definition of Cloud Computing*.
- b. The scope of this directive extends to USDA’s cloud capable information systems operated by USDA agencies, staff offices, contractors, grantees, and others working for or on behalf of the USDA.

4. POLICY

- a. All USDA information systems shall adopt a “[Cloud First](#)” policy.
- b. IT investments shall support OMB’s strategy for “[Cloud First Policy \(IT Reform\)](#).”
- c. Cloud computing services shall comply with all current Federal laws, and USDA IT security and risk management policies.
- d. USDA cloud computing services shall comply with all Federal and Departmental privacy requirements, regulations and policies.
- e. Cloud computing service acquisition vehicles shall include clear and concise language identifying the cloud computing source responsibilities for accommodating FISMA reporting and privacy management requirements per OMB Memorandum [M-09-29](#), *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*.
- f. Cloud computing services shall comply with [DR 3180-001](#), *Information Technology Network Standards*.
- g. Cloud computing services shall comply with the Agriculture Security Operations Center (ASOC) Compliance, Audits, Policy and Enforcement Division (CAPE) standard operating procedure (SOP) [CAPE-SOP-004](#), *USDA Six Step Risk Management Framework (RMF) Process Guide*.
- h. Cloud computing services shall comply with [DR 3540-003](#), *Security Assessment and Authorization* procedures.

5. ACQUISITION GUIDANCE

- a. USDA’s [Integrated Information Technology \(IT\) Governance Framework](#) (IITGF) shall guide agencies and staff offices when acquiring cloud computing services.
- b. Agencies and staff offices shall evaluate existing Departmental contracts and cloud computing solutions for applicability before acquiring or developing new services. If a new acquisition is essential, the services to be obtained shall be considered in the following order:
 - (1) An existing FedRAMP accredited commercial or Federal cloud service provider (CSP);
 - (2) An existing FedRAMP compliant Federal enclave; or

- (3) A USDA sponsored commercial CSP.
- c. Agencies and staff offices shall include language in acquisition vehicles that protect the interests of USDA and allow for adequate administrative control, security monitoring, reporting, and risk mitigation.

6. ROLES AND RESPONSIBILITIES

- a. The USDA CIO shall:
 - (1) Serve as the chief policy advisor to the Secretary on cloud computing policy;
 - (2) Develop and maintain Departmentwide policy for USDA information systems operating on CSP offerings;
 - (3) Direct the USDA enterprise-class data center private cloud service development;
 - (4) Ensure policy compliance with the provisions of this policy;
 - (5) Provide the Federal CIO with a written list of all cloud services that the Department has determined cannot or are not required to meet FedRAMP security authorization requirements. This list shall be provided annually and jointly signed by the USDA CIO and Chief Financial Officer; and
 - (6) Ensure the Office of General Counsel is engaged for advice and counsel with respect to the acquisition and offering of cloud services, when appropriate.
- b. The USDA Chief Information Security Officer shall:
 - (1) Advise the USDA CIO about strategies and methodologies for securing cloud computing services at non-USDA CSPs; and
 - (2) Advise Departmental CSPs on achieving compliance with USDA's Information Security Program.
- c. The Associate Chief Information Officer (ACIO), Agriculture Security Operations Center (ASOC) shall:
 - (1) Serve the Department as the Cloud Auditor;
 - (2) Determine if CSP offerings have an acceptable risk level under the USDA RMF;
 - (3) Prepare risk-based analysis through concurrency reviews to ensure that all private and commercial CSPs fully implement the USDA RMF;

- (4) Assign plans of action and milestones (POA&Ms) for CSP offerings determined not to have an acceptable risk level under the USDA RMF; and
 - (5) Ensure Departmental CSPs complete security monitoring, security auditing, and remediation of security concerns in accordance with Federal and Departmental guidelines.
- d. The ACIO, Data Center Operations (DCO) shall:
- (1) Serve the Department as the Cloud Broker;
 - (2) Serve as the cloud computing policy coordinator and technical advisor to the USDA CIO;
 - (3) Administer any certifications regarding cloud services and/or cloud-based information systems that are required (see Appendix E);
 - (4) Provide signature authority for routine cloud computing correspondence to agencies and staff offices from the Office of the Chief Information Officer (OCIO);
 - (5) Monitor policy compliance and report cloud policy deviations to the USDA CIO within 10 business days of discovery for resolution; and
 - (6) Partner with agencies and staff offices where appropriate to ensure the effective and efficient use of cloud services.
- e. The ACIO, Information Resource Management (IRM) shall:
- (1) Ensure cloud service offerings comply with Federal and Departmental records management, [eDiscovery](#), litigation hold, and electronically stored information records retention requirements, regulations, and policies;
 - (2) Ensure cloud service offerings comply with Federal and Departmental Section 508 requirements, regulations, and policies; and
 - (3) Ensure cloud service offerings comply with Federal and Departmental enterprise architecture (EA) regulations, policies, standards, and requirements.
- f. The ACIO, Policy, E-Government and Fair Information Practices shall:
- (1) Ensure cloud service offerings comply with Federal and Departmental *Freedom of Information Act* ([FOIA](#)) requirements, regulations, and policies; and
 - (2) Ensure cloud service offerings comply with Federal and Departmental privacy requirements, regulations, and policies.

g. The Director, Enterprise Network Services shall:

- (1) Serve the Department as the Cloud Carrier;
- (2) Design, develop, and implement networking architectures that provide CSPs with the necessary connectivity to deliver cloud services to agencies and staff offices;
- (3) Require CSPs to route their traffic to meet the requirements of the Trusted Internet Connection (TIC 2), consistent with Department of Homeland Security guidance;
- (4) Assign Internet Protocol (IP) addresses under IPv4 and IPv6 for CSPs and record IP addresses in the IP addressing management system for incident response;
- (5) Manage CSP firewalls for all agency locations as part of the USDA enterprise network;
- (6) Manage any domain name system (DNS) and domain name system security extensions (DNSSEC) for the CSPs as part of the USDA enterprise network; and
- (7) Manage and monitor the USDA enterprise network performance characteristics, such as bandwidth usage and latency, for the transport of cloud services between USDA and the CSPs.

h. Agency and Staff Office CIOs shall:

- (1) Ensure that their agencies and staff offices comply with this directive and other applicable Federal and USDA policies, regulations, and guidance pertaining to cloud computing;
- (2) Ensure IT entities working for or on behalf of USDA understand their responsibilities when implementing cloud computing services;
- (3) Assign agency and staff office Information Systems Security Program Managers (ISSPMs) with ensuring CSPs are in full compliance with FISMA, FIPS PUB 199, and NIST [SP 800-60](#), *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories*;
- (4) Ensure actions are taken to secure USDA information and information systems as required under Federal and USDA policies and guidance;
- (5) Ensure that contract language for acquiring services addresses security monitoring, security auditing, and remediation of security concerns in accordance with Federal and USDA regulations and standards;

- (6) Record, track, and resolve all POA&Ms for CSP offerings in the USDA FISMA data management and reporting tool;
- (7) Provide the USDA CIO with a written analysis each fiscal year on the progress of moving IT systems into compliance with this policy. The analysis shall identify, prioritize, and provide rationale for each production environment system as to its viability to move to the cloud within 2-5 years or not at all;
- (8) Be responsive to cloud computing data calls and certifications as required; and
- (9) Contain total cost of ownership expenditures for USDA information systems following operational analysis methods as identified in Appendix D.

7. POLICY EXCEPTIONS

- a. All USDA agencies and staff offices are required to conform to this policy. In the event that a policy requirement cannot be met as explicitly stated, the agency or staff office CIO, via the agency or staff office ISSPM, must submit a waiver request to the ACIO DCO for internal OCIO coordination on behalf of the USDA CIO.
- b. The waiver request must explain the reason for the request, identify compensating controls/actions that meet the intent of the policy, and identify how the compensating controls/actions provide a comparable or greater level of defense or compliance than required by the policy.
- c. Waivers granted approval by the USDA CIO must be associated with a NIST control and recorded and tracked as a POA&M item in the USDA FISMA data management and reporting tool. Waivers will expire at the end of the fiscal year or six months from the date of approval, whichever is longer. Unless otherwise specified, agencies and staff offices shall review and renew approved policy waivers every fiscal year.

8. INQUIRIES

Inquiries about this policy shall be directed to the ACIO DCO. Contact the ACIO DCO through the National Information Technology Center (NITC) data center service desk at 888-USE-NITC or (816-926-6660) or NITCServicedesk@ocio.usda.gov.

-END-

APPENDIX A

ACRONYMS AND ABBREVIATIONS

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46

ACIO	Associate Chief Information Officer
ASOC	Agriculture Security Operations Center
CAPE	Compliance, Audits, Policy and Enforcement
CIO	Chief Information Officer
CONOPS	Concept of Operations
CSP	Cloud Service Provider
DCO	Data Center Operations
DM	Departmental Manual
DNS	Domain Name System
DNSSEC	Domain Name System Security Extension
DR	Departmental Regulation
EA	Enterprise Architecture
ENS	Enterprise Network Services
FedRAMP	Federal Risk and Authorization Management Program
FIPS PUB	Federal Information Processing Standards Publication
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
GAO	Government Accountability Office
HSPD	Homeland Security Presidential Directive
IITGF	Integrated Information Technology Governance Framework
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IRM	Information Resource Management
ISSPM	Information Systems Security Program Manager
IT	Information Technology
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency or Internal Report
NITC	National Information Technology Center
NSI	National Security Information
NSPD	National Security Presidential Directive
NSS	National Security System
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
POA&M	Plans of Action and Milestones
RMF	Risk Management Framework
SOP	Standard Operating Procedure
SP	Special Publication
TIC 2	Trusted Internet Connection
U.S.C.	United States Code

48 APPENDIX B

49
50 AUTHORITIES AND REFERENCES

51
52
53 AUTHORITIES

54
55 *The Clinger-Cohen Act of 1996, [40 United States Code \(U.S.C.\) 1401 et seq.](#)*

56
57 *Definitions, [41 U.S.C. 403](#)*

58
59 *Federal Information Security Management Act of 2002 ([FISMA](#)), 44 U.S.C. 3541, et seq.*
60 *(2014)*

61
62 *Freedom of Information Act (FOIA), [5 U.S.C. 552](#)*

63
64 *Homeland Security Presidential Directive ([HSPD](#)) 20, *National Continuity Policy*, May 4,*
65 *2007*

66
67 *National Security Presidential Directive ([NSPD](#)) 51, *National Continuity Policy*, May 4,*
68 *2007*

69
70 *The Paperwork Reduction Act of 1995, [44 U.S.C. 3502](#)*

71
72 *The Privacy Act of 1974, [5 U.S.C. 552a](#)*

73
74 *Responsibilities for Federal Information Systems Standards, [40 U.S.C. 11331](#)*

75
76
77 REFERENCES

78
79 *CIO Council, [Federal Shared Services Implementation Guide](#), April 16, 2013*

80
81 *[CAPE-SOP-004](#), *USDA Six Step Risk Management Framework (RMF) Process Guide*,*
82 *Revision 2.44, May 2015*

83
84 *Departmental Manual ([DM](#)) 3515-000, *Privacy Requirements*, February 17, 2005*

85
86 *[DM 3515-002](#), *Privacy Impact Assessment*, February 17, 2005*

87
88 *[DR 3060-000](#), *USDA Information and Technology Transformation*, November 2, 2004*

89
90 *[DR 3080-001](#), *Records Management*, May 23, 2013*

91
92 *[DR 3085-001](#), *Vital Records Management Program*, August 19, 2011*

93

94 [DR 3090-001](#), *Litigation Retention Policy for Documentary Materials including*
95 *Electronically Stored Information*, May 28, 2008
96
97 [DR 3099-001](#), *Records Management Policy for Departing Employees, Contractors,*
98 *Volunteers and Political Appointees*, July 2, 2012
99
100 [DR 3130-008](#), *Definition of Major Information Technology (IT) Investments*, February 27,
101 2015
102
103 [DR 3180-001](#), *Information Technology Network Standards*, May 12, 2015
104
105 [DR 3450-001](#), *Computer Matching Projects Involving Individual Privacy Data*, April 17,
106 1984
107
108 [DR 3450-002](#), *Freedom of Information Act Implementing Regulations*, February 7, 2003
109
110 [DR 3540-003](#), *Security Assessment and Authorization*, August 12, 2014
111
112 [DR 4030-001](#), *Section 508 Implementation - Final Guidance*, July 23, 2003
113
114 GAO, [GAO-08-536](#), *Alternatives Exist for Enhancing Protection of Personally Identifiable*
115 *Information*, May 19, 2008
116
117 General Services Administration (GSA), *FedRAMP Concept of Operations* ([CONOPS](#))
118 Version 1.2, July 27, 2012
119
120 NIST, [FIPS PUB199](#), *Standards for Security Categorization of Federal Information and*
121 *Information Systems*, February 2004
122
123 NIST, [NISTIR 7298](#) Revision 2, *Glossary of Key Information Security Terms*, May 2013
124
125 NIST, [NISTIR 7956](#), *Cryptographic Key Management Issues and Challenges in Cloud*
126 *Services*, September 2013
127
128 NIST, [SP 500-291](#) Version 2, *NIST Cloud Computing Standards Roadmap*, July 2013
129
130 NIST, [SP 500-292](#), *NIST Cloud Computing Reference Architecture*, September 2011
131
132 NIST, [SP 500-293](#), *US Government Cloud Computing Technology Roadmap, Volume I and*
133 *Volume II*, October 2014
134
135 NIST, [SP 500-299](#), *NIST Cloud Computing Security Reference Architecture (Draft)*
136
137 NIST, [SP 800-34](#) Revision 1, *Contingency Planning Guide for Federal Information Systems*,
138 May 2010 (errata as of November 11, 2010)
139

140 NIST, [SP 800-37](#) Revision 1, *Guide for Applying the Risk Management Framework to*
141 *Federal Information Systems: A Security Life Cycle Approach*, February 2010
142
143 NIST, [SP 800-53](#) Revision 4, *Security and Privacy Controls for Federal Information Systems*
144 *and Organizations*, April 2013 (errata as of January 15, 2014)
145
146 NIST, [SP 800-53A](#) Revision 4, *Guide for Assessing the Security Controls in Federal*
147 *Information Systems and Organizations: Building Effective Security Assessment Plans*,
148 *December 2014*
149
150 NIST, [SP 800-60](#) *Volume I: Guide for Mapping Types of Information and Information*
151 *Systems to Security Categories*, August 2008
152
153 NIST, [SP 800-122](#), *Guide to Protecting the Confidentiality of Personally Identifiable*
154 *Information (PII)*, April 2010
155
156 NIST, [SP 800-125](#), *Guide to Security for Full Virtualization Technologies*, January 2011
157
158 NIST, [SP 800-144](#), *Guidelines on Security and Privacy in Public Cloud Computing*,
159 *December 2011*
160
161 NIST, [SP 800-145](#), *The NIST Definition of Cloud Computing*, September 2011 (errata as of
162 April 27, 2012)
163
164 NIST, [SP 800-146](#), *Cloud Computing Synopsis and Recommendations*, May 2012
165
166 OMB, [25 Point Implementation Plan to Reform Federal Information Technology](#)
167 [Management](#), December 9, 2010
168
169 OMB, [Federal Cloud Computing Strategy](#), February 8, 2011
170
171 OMB, [Federal Information Technology Shared Services Strategy](#), May 2, 2012
172
173 OMB, [Guidance on Exhibit 53—Information Technology and E-Government](#), July 1, 2013
174
175 OMB, [Memorandum for Federal Chief Information Officers](#), *Increasing Shared Approaches*
176 *to Information Technology Services*, May 2, 2012
177
178 OMB, [Memorandum for Chief Information Officers](#), *Security Authorization of Information*
179 *Systems in Cloud Computing Environments*, December 8, 2011
180
181 OMB, Memorandum [M-09-29](#), *FY 2009 Reporting Instructions for the Federal Information*
182 *Security Management Act and Agency Privacy Management*, August 20, 2009
183
184 OMB, Memorandum [M-11-29](#), *Chief Information Officer Authorities*, August 8, 2011
185

186 OMB, Memorandum [M-12-20](#), *FY 2012 Reporting Instructions for the Federal Information*
187 *Security Management Act and Agency Privacy Management*, September 27, 2012
188
189 USDA, [OCIO Integrated IT Governance Framework: Guidebook](#) Version 3.2, April 1, 2014

190 APPENDIX C

191 DEFINITIONS

- 192
- 193
- 194
- 195 a. Cloud Auditor. A party that can conduct independent assessment of cloud services,
196 information system operations, performance and security of the cloud
197 implementation. (Source: NIST SP 500-292)
- 198
- 199 b. Cloud Broker. An entity that manages the use, performance and delivery of cloud
200 services, and negotiates relationships between Cloud Providers and Cloud
201 Consumers. (Source: NIST SP 500-292)
- 202
- 203 c. Cloud Computing. Cloud computing is a model for enabling ubiquitous, convenient,
204 on-demand network access to a shared pool of configurable computing resources (i.e.,
205 networks, servers, storage, applications, and services) that can be rapidly provisioned
206 and released with minimal management effort or service provider interaction. The
207 NIST cloud model is composed of five essential characteristics, three service models,
208 and four deployment models. (Source: NIST SP 800-145)
- 209
- 210 d. Cloud Carrier. An intermediary that provides connectivity and transport of cloud
211 services from Cloud Providers to Cloud Consumers. (Source: NIST SP 500-292)
- 212
- 213 e. Contractor Support. Contractor support encompasses on-site or off-site contractor
214 technical or other support staff. (Source: OMB M-12-20)
- 215
- 216 f. Core Data Connection Services. At the start of a contract for the acquisition of cloud
217 services, any one-time network interconnection setup between services at each
218 disparate location including to USDA’s Universal Telecommunication Network. The
219 specific details of these connections must be developed in coordination with OCIO
220 ENS, OCIO ASOC, and the CSP’s support team.
- 221
- 222 g. Domain Name System (DNS) Services. DNS services are used by a CSP to run DNS
223 servers for networking.
- 224
- 225 h. Enterprise Data Center. A professionally managed and operated, institutionally
226 supported facility, providing convenient access to, manipulation of, and/or
227 distribution of data (including supporting information and expertise) for a wide
228 community of users. It has a long-term charter (not tied to the lifetime of a specific
229 project) and is capable of hosting systems that may be Departmentwide, shared
230 services or agency-specific. The facility must meet USDA specified physical
231 standards and sustain USDA specific operational standards and sustain USDA
232 specified operationally. (Source: [OCFO/OCIO memorandum](#))
- 233
- 234 i. Executive Agency. An executive department specified in 5 U.S.C. 101; a military
235 department specified in 5 U.S.C. 102; an independent establishment as defined in 5

- 236 U.S.C. 104(1); and a wholly owned Government corporation fully subject to the
237 provisions of 31 U.S.C. 91. (Source: 41 U.S.C. 403)
238
- 239 j. Federal Information System. An information system used or operated by an
240 executive agency, by a contractor of an executive agency, or by another organization
241 on behalf of an executive agency. (Source: 40 U.S.C. 11331)
242
- 243 k. Information. Information is categorized according to its information type. An
244 information type is a specific category of information (e.g., privacy, medical,
245 proprietary, financial, investigative, contractor sensitive, security management)
246 defined by an organization or, in some instances, by a specific law, Executive Order,
247 directive, policy, or regulation. (Source: FIPS PUB 199)
248
- 249 l. Information Resources. Information and related resources, such as personnel,
250 equipment, funds, and information technology. (Source: 44 U.S.C. 3502)
251
- 252 m. Information System. A discrete set of information resources organized for the
253 collection, processing, maintenance, use, sharing, dissemination, or disposition of
254 information. (Source: 44 U.S.C. 3502)
255
- 256 n. Information System Operated by a Contractor on Behalf of an Agency. An
257 information system operated by a contractor on behalf of an agency must be treated in
258 the same way as agency-operated information systems. The level of effort required
259 for security authorization depends of the impact level of the information contained in
260 the system. The security authorization boundary for these systems must be carefully
261 mapped to ensure that Federal information: (a) is adequately protected, (b) is
262 segregated from the contractor, state or grantee corporate infrastructure, and (c) there
263 is an interconnection security agreement in place to address connections from the
264 contractor, state or grantee system containing the agency information to systems
265 external to the security authorization boundary. (Source: OMB M-12-20)
266
- 267 o. Information Technology. Any equipment or interconnected system or subsystem of
268 equipment that is used in the automatic acquisition, storage, manipulation,
269 management, movement, control, display, switching, interchange, transmission, or
270 reception of data or information by the executive agency. For purposes of the
271 preceding sentence, equipment is used by an executive agency if the equipment is
272 used by the executive agency directly or is used by a contractor under a contract with
273 the executive agency which: (i) requires the use of such equipment; or (ii) requires the
274 use, to a significant extent, of such equipment in the performance of a service or the
275 furnishing of a product. The term information technology includes computers,
276 ancillary equipment, software, firmware and similar procedures, services (including
277 support services), and related resources. (Source: 40 U.S.C. 1401)
278
- 279 p. Private Cloud. The cloud infrastructure is provisioned for exclusive use by a single
280 organization comprising multiple cloud consumers (e.g., business units). It may be
281 owned, managed, and operated by the organization, a third party, or some

282 combination of them, and it may exist on or off premises. (Source: NIST SP 800-
283 145)

284

285 q. Service Provider. A service provider encompasses the typical outsourcing of system
286 or network operations, telecommunication services, or other managed services
287 (including those provided by another agency or subscribing to software services.
288 (Source: OMB M-12-20)

APPENDIX D

COST ANALYSIS WHEN SELECTING A CLOUD SERVICE PROVIDER

The USDA Integrated Information Technology Governance Framework (IITGF) - Operational Analysis instructions direct the review and management of an information technology portfolio. Selection of a CSP is an important decision for USDA system owners that deliver programs on behalf of the Department. Any CSPs under consideration shall comply with the current FISMA requirements, the appropriate NIST security standards, and NIST guidelines for cloud-based information systems. When comparing CSPs for the best value to USDA, it is recommended that agencies and staff offices evaluate total cost of ownership lifecycle costs. At a minimum, a lifecycle cost analysis should include:

- a. Start-up services for establishing hosting environments for CSPs. These start-up services may include:
 - (1) Core data connection services;
 - (2) DNS services;
 - (3) Configuration of the hosting environment for IP addressing, security zones, and other configuration management;
 - (4) CSP orientation training about the acquired environment;
 - (5) Portal installation costs; and
 - (6) Virtual private cloud connection costs.
- b. Data storage services for Tier-1, Tier-2, Tier-3, and long term archival.
- c. Recurring charges such as end point virus protection, firewall maintenance, operating system patching, data intra and inter-region transfer, elastic load balancing, consumption metrics, and data snapshots.
- d. Other professional services such as integration services project manager, integration services quality control analyst, integration services system architect, integration services systems programmer, integration services hardware/software specialist, and integration services security specialist.
- e. Security services to comply with all current Federal laws, and USDA IT security and risk management policies.
- f. Operations and maintenance costs for out-year CSP contract renewals.

334
335
336
337
338
339
340
341
342

APPENDIX E

ANNUAL CERTIFICATION OF CLOUD SERVICE OFFERINGS

The annual certification form for cloud service offerings can be found at:

N:\work\HOME\PEO\Cloud Policy\OGC - Rework - August 2015\ADxxxx_18AUG2015 graphic.pdf.