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

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.
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.

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.
## APPENDIX A

### ACRONYMS AND ABBREVIATIONS

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

AUTHORITIES AND REFERENCES

AUTHORITIES


Definitions, 41 U.S.C. 403


Freedom of Information Act (FOIA), 5 U.S.C. 552


The Privacy Act of 1974, 5 U.S.C. 552a


REFERENCES


Departmental Manual (DM) 3515-000, Privacy Requirements, February 17, 2005

DM 3515-002, Privacy Impact Assessment, February 17, 2005

DR 3060-000, USDA Information and Technology Transformation, November 2, 2004

DR 3080-001, Records Management, May 23, 2013

DR 3085-001, Vital Records Management Program, August 19, 2011

NIST, SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013 (errata as of January 15, 2014)


NIST, SP 800-60 Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008

NIST, SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PHI), April 2010

NIST, SP 800-125, Guide to Security for Full Virtualization Technologies, January 2011

NIST, SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing, December 2011

NIST, SP 800-145, The NIST Definition of Cloud Computing, September 2011 (errata as of April 27, 2012)

NIST, SP 800-146, Cloud Computing Synopsis and Recommendations, May 2012

OMB, 25 Point Implementation Plan to Reform Federal Information Technology Management, December 9, 2010


OMB, Federal Information Technology Shared Services Strategy, May 2, 2012

OMB, Guidance on Exhibit 53—Information Technology and E-Government, July 1, 2013

OMB, Memorandum for Federal Chief Information Officers, Increasing Shared Approaches to Information Technology Services, May 2, 2012


OMB, Memorandum M-11-29, Chief Information Officer Authorities, August 8, 2011

B-3
OMB, Memorandum M-12-20, FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, September 27, 2012

USDA, *OCIO Integrated IT Governance Framework: Guidebook* Version 3.2, April 1, 2014
APPENDIX C

DEFINITIONS

a. **Cloud Auditor.** A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation. (Source: NIST SP 500-292)

b. **Cloud Broker.** An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers. (Source: NIST SP 500-292)

c. **Cloud Computing.** Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (i.e., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The NIST cloud model is composed of five essential characteristics, three service models, and four deployment models. (Source: NIST SP 800-145)

d. **Cloud Carrier.** An intermediary that provides connectivity and transport of cloud services from Cloud Providers to Cloud Consumers. (Source: NIST SP 500-292)

e. **Contractor Support.** Contractor support encompasses on-site or off-site contractor technical or other support staff. (Source: OMB M-12-20)

f. **Core Data Connection Services.** At the start of a contract for the acquisition of cloud services, any one-time network interconnection setup between services at each disparate location including to USDA’s Universal Telecommunication Network. The specific details of these connections must be developed in coordination with OCIO ENS, OCIO ASOC, and the CSP’s support team.

g. **Domain Name System (DNS) Services.** DNS services are used by a CSP to run DNS servers for networking.

h. **Enterprise Data Center.** A professionally managed and operated, institutionally supported facility, providing convenient access to, manipulation of, and/or distribution of data (including supporting information and expertise) for a wide community of users. It has a long-term charter (not tied to the lifetime of a specific project) and is capable of hosting systems that may be Departmentwide, shared services or agency-specific. The facility must meet USDA specified physical standards and sustain USDA specific operational standards and sustain USDA specified operationally. (Source: OCFO/OCIO memorandum)

i. **Executive Agency.** An executive department specified in 5 U.S.C. 101; a military department specified in 5 U.S.C. 102; an independent establishment as defined in 5
j. **Federal Information System.** An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. (Source: 40 U.S.C. 11331)

k. **Information.** Information is categorized according to its information type. An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive Order, directive, policy, or regulation. (Source: FIPS PUB 199)

l. **Information Resources.** Information and related resources, such as personnel, equipment, funds, and information technology. (Source: 44 U.S.C. 3502)

m. **Information System.** A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (Source: 44 U.S.C. 3502)

n. **Information System Operated by a Contractor on Behalf of an Agency.** An information system operated by a contractor on behalf of an agency must be treated in the same way as agency-operated information systems. The level of effort required for security authorization depends on the impact level of the information contained in the system. The security authorization boundary for these systems must be carefully mapped to ensure that Federal information: (a) is adequately protected, (b) is segregated from the contractor, state or grantee corporate infrastructure, and (c) there is an interconnection security agreement in place to address connections from the contractor, state or grantee system containing the agency information to systems external to the security authorization boundary. (Source: OMB M-12-20)

o. **Information Technology.** Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. (Source: 40 U.S.C. 1401)

p. **Private Cloud.** The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple cloud consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some
combination of them, and it may exist on or off premises. (Source: NIST SP 800-145)

q. **Service Provider.** A service provider encompasses the typical outsourcing of system or network operations, telecommunication services, or other managed services (including those provided by another agency or subscribing to software services. (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.
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.