DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N3-13-27
Baltimore, Maryland 21244-1850

OFFICE OF INFORMATION SERVICES

CISO Memorandum 14-02

DATE: **July 10, 2014**

TO: CMS Component Heads and Business Owners

FROM: Teresa Fryer /s/ CMS Chief Information Security Officer (CISO) and Director, Enterprise Information Security Group (EISG)

SUBJECT: CISO Memorandum 14-02 – CMS Cloud Computing and Federal Risk and Authorization Management Program Guidance– **INFORMATION**

Background

Cloud computing is a model, as defined[1] by the *National Institute of Standards and Technology (NIST)*, for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models, which are listed below.

- Cloud Essential Characteristics include: On-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.
- Cloud Service Models include: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).
- Cloud Deployment Models include: Private, Community, Public, and Hybrid.

The White House established the *Federal Risk and Authorization Management Program (FedRAMP)* on December 8, 2011 via an official memorandum[2] from the Federal Chief Information Officer (CIO) to all agency CIOs. FedRAMP was established in close collaboration with the *NIST*, the *General Services Administration (GSA)*, the *Department of Homeland Security (DHS)*, and other federal agencies, and working bodies such as the *Information Security and Identity Management Committee (ISIMC)*. FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services that are applicable for Federal Information Processing Standards Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*, low and moderate impact information systems. The purpose of FedRAMP is to ensure that cloud based services have adequate information

[1] NIST Special Publication 800-145, *The NIST Definition of Cloud Computing*, dated September 2011 is available at: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. HHS has clarified this definition in the *HHS Cloud Computing and Federal Risk and Authorization Management Program (FedRAMP) Guidance* is available on the HHS Intranet at http://intranet.hhs.gov/it/cybersecurity/policies/index.html.

[2] Federal CIO Memorandum: *Security Authorization of Information Systems in Cloud Computing Environments*, dated December 8, 2011 is available at: http://www.cio.gov/wp-content/uploads/2012/09/fedrampmemo.pdf.

security, eliminate duplication of effort, reduce risk management costs, and enable rapid and cost-effective procurement of information systems/services for federal agencies.[3]

Purpose

The purpose of this INFORMATIONAL memorandum is to reiterate to CMS Components and Business Owners the CMS cloud computing security guidelines and requirements for compliance with FedRAMP.

Information

As of June 6, 2012, all new cloud services to be used by all federal agencies ***must*** have met the FedRAMP requirements, utilized the FedRAMP templates, and have security authorization packages available in the FedRAMP repository.

Additionally, all federal agencies have until June 6, 2014 to update the security authorization package of any legacy/existing *Cloud Service Provider (CSP)* currently in use, and ensure they meet the FedRAMP requirements, and have security authorization packages available in the FedRAMP repository.

To help facilitate these actions, CMS Business Owners should ensure that relevant CMS FedRAMP language[4] is included in all new and existing contracts associated with services involving information technology and/or cloud computing.

A Cloud Frequently Asked Questions document is attached to assist with understanding FedRAMP requirements. Additional information and guidance is available in the CMS *Risk Management Handbook (RMH)*, Volume III, Standard 3.2, *Cloud Computing*, available in the CMS security library at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

Contacts

If you have questions or require additional information regarding this FedRAMP requirement, please contact the CMS Enterprise Information Security Group (EISG), Governance and Oversight Lead, at mailto:ciso@cms.hhs.gov for assistance and guidance.

Teresa Fryer

Digitally signed by Teresa Fryer
DN: cn=Teresa Fryer, o, ou, email=teresa.fryer@cms.hhs.gov, c=US
Date: 2014.07.11 09:20:52 -04'00'

Teresa Fryer
CISO and Director EISG

cc:
Distribution
Attachment: *"Cloud Frequently Asked Questions (FAQ)"*

[3] *Federal Risk and Authorization Management Program Concept of Operations*, dated February 7, 2012 is available at: http://cloud.cio.gov/document/concept-operations.
[4] *CMS Information Security Contract Clause/Provision* language is available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

Cloud Frequently Asked Questions (FAQ)

Q1: What constitutes a "Cloud" system?

Clouds are defined in the CMS *Risk Management Handbook (RMH)*, Volume III, Standard 3.2, *Cloud Computing* (available in the CMS Information Security Library at: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html. Essentially they are defined as:

> *Cloud computing is a model, as defined by the* National Institute of Standards and Technology (NIST)*, for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned (by a CMS business owner) and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five Essential Characteristics, three Service Models, and four Deployment Models.*

HHS considers systems to be *cloud* systems if they contain two or more NIST-specified essential characteristics, or define themselves as cloud. Systems that have fewer than two of these characteristics should follow existing HHS and CMS system security requirements and procedures. This definition is aligned with the FedRAMP security assessment and authorization process. Implementations that meet these criteria will be deemed "clouds" at CMS. Further details can be found in the RMH Standard on *Cloud Computing*.

Q2: What are the plans for CMS cloud systems already in use?

Business Owners are responsible for ensuring their cloud systems are FedRAMP approved, including legacy implementations. The target is to either 1) gain FedRAMP approval for all legacy CMS CSPs, or 2) move the affected CMS programs into other CSPs that have a FedRAMP approval. All non-FedRAMP approved cloud systems must be reported as *non-compliant* to the Department, and the Office of Management and Budget (OMB), and must provide justifications for *why* those systems are not yet compliant. In addition, OMB requires that *Corrective Action Plans* be submitted for each non-compliant cloud implementation. Please contact the CMS Enterprise Information Security Group (EISG) Governance and Oversight Lead at mailto:ciso@cms.hhs.gov for specific case-by-case assistance and guidance.

Q3: I am using a Cloud Service Provider (CSP) that is not FedRAMP approved. What should I do?

Ensure that you have gone through or in the process of going through the eXpedited Lifecycle (XLC). All CSP Services should be working towards a FedRAMP approved Authorization to Operate (ATO), whether it obtains a FedRAMP Joint Authorization Board (JAB) Provisional ATO, or obtains a FedRAMP Agency ATO. Systems and services should be documented accordingly. Contact the Enterprise Information Security Group at the CISO Mailbox: CISO@cms.hhs.gov for further assistance and guidance.

Q4: Should the CSP go through the FedRAMP Joint Authorization Board (JAB) or through CMS to receive FedRAMP Approval?

The steps and work necessary for a FedRAMP approval is essentially the same, regardless of which path is chosen. If the CSP has more than two implementations within the CMS or HHS environment it is recommended that the CSP work with HHS to obtain a FedRAMP Agency ATO. If your CSP has 2 or less cloud implementations within the CMS environment they *may* be a candidate for CMS Sponsorship. However, note that the *ideal* goal is to seek out a CSP that is ALREADY approved by the FedRAMP process. Contact the CMS Enterprise Information Security Group (EISG) Governance and Oversight Lead at mailto:ciso@cms.hhs.gov for specific case-by-case assistance and guidance.

Q5: Who should the CSP contact to go through the JAB approval process?

The initial contact is for *the CSP* to contact the FedRAMP Program Management Office (PMO) at www.fedramp.gov and complete the FedRAMP initiation form (available at http://cloud.cio.gov/site-page/fedramp-initiation-request.) For CMS Business Owners, please contact the CMS Enterprise Information Security Group (EISG) Governance and Oversight Lead at mailto:ciso@cms.hhs.gov for assistance and guidance.

Q6: I am using a CSP that has registered for a JAB FedRAMP approval and is in a queue but won't get FedRAMP Approval for some time. What should I do?

Please contact the CMS Enterprise Information Security Group (EISG) Governance and Oversight Lead at mailto:ciso@cms.hhs.gov for specific case-by-case assistance and guidance.

Q7: I am currently using a CSP that is not FedRAMP approved, but is expected to receive FedRAMP Approval in about six months, and my system is not authorized, what should I do?

Please contact the CMS Enterprise Information Security Group (EISG) Governance and Oversight Lead at mailto:ciso@cms.hhs.gov for specific case-by-case assistance and guidance.

Q8: What are CMS' requirements for a CSP, and how are they different from the FedRAMP requirements?

With the exception of other *legal* requirements, CMS accepts the *minimum* settings and control requirements established by the FedRAMP program; even when those settings and baselines may be different from (or even conflict with) settings and baselines established in the CMS ARS. However, when additional *Statutory* or *Regulatory* requirements apply to a particular business process, those requirements MUST still be met—even when they are not addressed by minimum FedRAMP requirements. For CMS business process, those requirements typically include additional requirements associated with *HIPAA*, *HITECH*, the *Privacy Act*, the *Federal Records Act*, and/or *Internal Revenue Code (IRC)*. Note that those additional requirements may be addressed by *either* the CSP, *or* by CMS applications hosted within the CSP. It is *not* required to be address by both. Please contact the CMS Enterprise Information Security Group (EISG) Governance and Oversight Lead at mailto:ciso@cms.hhs.gov for assistance and guidance on those additional requirements.

Q9: How can I review a FedRAMP-approved CSP to ensure it meets CMS' requirements?

Business Owners must review the FedRAMP documentation for the specific FedRAMP-approved CSP to determine the CSP suitability for the proposed business. Complete the FedRAMP package request Form available at http://cloud.cio.gov/document/fedramp-package-request-form and submit the completed form to the Governance and Oversight Lead at mailto:ciso@cms.hhs.gov. This form must then be signed and forwarded by the CMS CISO to the FedRAMP PMO. Upon approval, CMS Business Owners should review available CSP documentation to ensure that the CSP offering meets the CMS business need, as well as any additional security and privacy requirements that may be applicable to the business being conducted. Additional guidance is available in the CMS *Risk Management Handbook (RMH)*, Volume III, Standard 3.2, *Cloud Computing*, available in the CMS security library at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html. Please contact the CMS Enterprise Information Security Group (EISG) Governance and Oversight Lead at mailto:ciso@cms.hhs.gov for assistance and guidance.

Q10: My CSP has a FedRAMP ATO. Does it also need to be approved by CMS? What are my next steps?

All CSPs *must* have a CMS ATO. The CMS ATO states that it has met minimum CMS requirements prior to its implementation, and any known *risk* is at an acceptable level to operate within a CMS environment. Any CMS applications associated with the CSP must *also* receive the proper CMS ATO prior to moving into the *production* environment. CMS may *leverage* the FedRAMP approval. However, the CSP must also meet any additional *statutory* and *regulatory* requirements which may be applicable to CMS businesses. EISG will soon be publishing procedures in the CMS *Risk Management Handbook*, Volume II, Procedure 8.2, *Utilizing External IT Services/Resources (Clouds)*. Please contact the CMS Enterprise Information Security Group (EISG) Governance and Oversight Lead at mailto:ciso@cms.hhs.gov for assistance and guidance.

Q11: After I have received approval to access the CSP's FedRAMP documentation, how long will I have access to review it?

You have 30 days to complete your review, after which access will automatically be revoked. If more time is needed please contact the Enterprise Information Security Group Governance and Oversight Lead at mailto:ciso@cms.hhs.gov for assistance and guidance.

Q12: Do I need to go through the XLC if I am using a CSP?

Yes, it is CMS' expectation that *all* systems will go through the XLC to ensure that the system is properly documented prior to it going into the production environment.

Q13: As a Business Owner, what controls am I responsible for when using a CSP?

The Business/System Owner is ultimately responsible for *ALL* control implementations associated with a system or application. The required FedRAMP documentation includes a *Control Implementation Summary (CIS)*, which specifies the *distribution* of control responsibility between the CSP and any associated system or application hosted within the CSP. Systems or applications that are hosted *within* a CSP must meet the current ARS control

requirements. For inherited controls provided by the CSP, CMS will accept CSP-provided inherited control implementations at their associated FedRAMP-specified settings. Please contact the CMS Enterprise Information Security Group (EISG) Governance and Oversight Lead at mailto:ciso@cms.hhs.gov for assistance and guidance.

Q14: Who can perform the security assessment for a Cloud Service Provider for the purposes of receiving FedRAMP (and CMS) approval?

Any prospective CSP must use a certified *Third Party Assessment Organization (3PAO)* to perform the independent security assessment of the FedRAMP security controls in place. The FedRAMP PMO has approved *American Association for Laboratory Accreditation (A2LA)* to accredit 3PAOs. Additional information on 3PAO certification is available at http://cloud.cio.gov/fedramp/3pao. A list of certified 3PAOs is available at http://cloud.cio.gov/fedramp/accredited-3paos.

Q15: What version of the FedRAMP controls does a CSP need to meet (based on 800- R3 or the newly released R4 FedRAMP Controls)?

If the CSP has already engaged with FedRAMP prior to mid-May 2014, they will likely be allowed to complete their process using the R3 FedRAMP control set, with the expectation of providing an *update* to the FedRAMP package within 6-months of the initial FedRAMP approval. All others will be required to complete their packages using the FedRAMP controls (and templates) released in the first week of June 2014.