**APPENDIX C—FedRAMP *Tailored* ATO Letter Template**

{Federal Agency/Office logo}

{Insert Date}

{Cloud System Owner Name}

{Insert Cloud Service Name} Cloud System Owner

{Insert Address}

Mr./Mrs. {CSP System Owner Name}:

*Instructions: Replace all the information between angle brackets (< >) with information specific to your letter.*

*Delete these instructions when done.*

<Federal Agency/Office> has completed the security review of the <Cloud Service Provider (CSP) Name> (<CSP Acronym>) <System Name> (<System Acronym>), which leverages the <CSP Name> (<CSP Acronym>) <System Name> (<System Acronym>) <Select IaaS or *PaaS>*. Based on the Federal Information Processing Standard (FIPS) security impact categorization of Low (Confidentiality = Low, Integrity = Low, Availability = Low) and specifically the FedRAMP *Tailored* Low Impact Software-as-a-Service (LISaaS) Security Requirements,[[1]](#footnote-1) <Federal Agency/Office> has determined that <System Acronym> meets the information security requirements and is granted <Federal Agency/Office> FedRAMP Authorization to Operate (ATO).

The FedRAMP *Tailored* LISaaS Baseline established by the FedRAMP Joint Authorization Board (JAB) defines the minimum security requirements for SaaS systems and applications that meet specific criteria for use by agencies.

*<Insert information regarding the appropriate use, purposes and restrictions for use of this SaaS>*

The <Federal Agency/Office> has determined this <CSP system Name> ATO is applicable for use by <Federal Agency/Office> users for the following purposes, and with the following restrictions:

* *Purpose Example: This application is authorized for use by <Federal Agency/Office> users and contractors for Federal business collaboration and management purposes only.*
* *Restriction Example: No Personally Identifiable Information (PII) data may be stored, processed, or transmitted with this application.*

Based on the assessment conducted by <Assessment Organization Name>, and review by <Federal Agency/Office’s> Authorization Organization the <CSP and/or CSP System Name> has been implemented and is maintained at an acceptable level of risk.

<*Edit the following as appropriate, if known risks or security controls are not implemented and have been accepted by the Authorization Organization specifically for this ATO*>

The following is a list of known vulnerabilities and risks of the <CSP Name/System Name> that have been determined as acceptable for the specific use and with the specified restrictions:

* *Example risk accepted: Support for acceptance of PIV/CAC credentials for Federal privileged users <has not been implemented* or *is planned for implementation> by <date>.*
* *Example risk accepted: Implementation of continuous monitoring is based on <enter continuous monitoring process information here>.*

The security authorization of the information system will remain in effect for a length of time in alignment with Office of Management and Budget Circular A-130 as long as:

1. <CSP Acronym> satisfies the requirement of implementing continuous monitoring activities in accordance with FedRAMP *Tailored* LISaaS continuous monitoring requirements and/or as agreed between <Federal Agency/Office> and <System Acronym>.
2. <CSP Acronym> mitigates open vulnerabilities in accordance with FedRAMP requirements and as agreed between <Federal Agency/Office> and <System Acronym>.
3. Significant changes or critical vulnerabilities are identified and managed in accordance with applicable Federal law, guidelines, policies, and best practices.

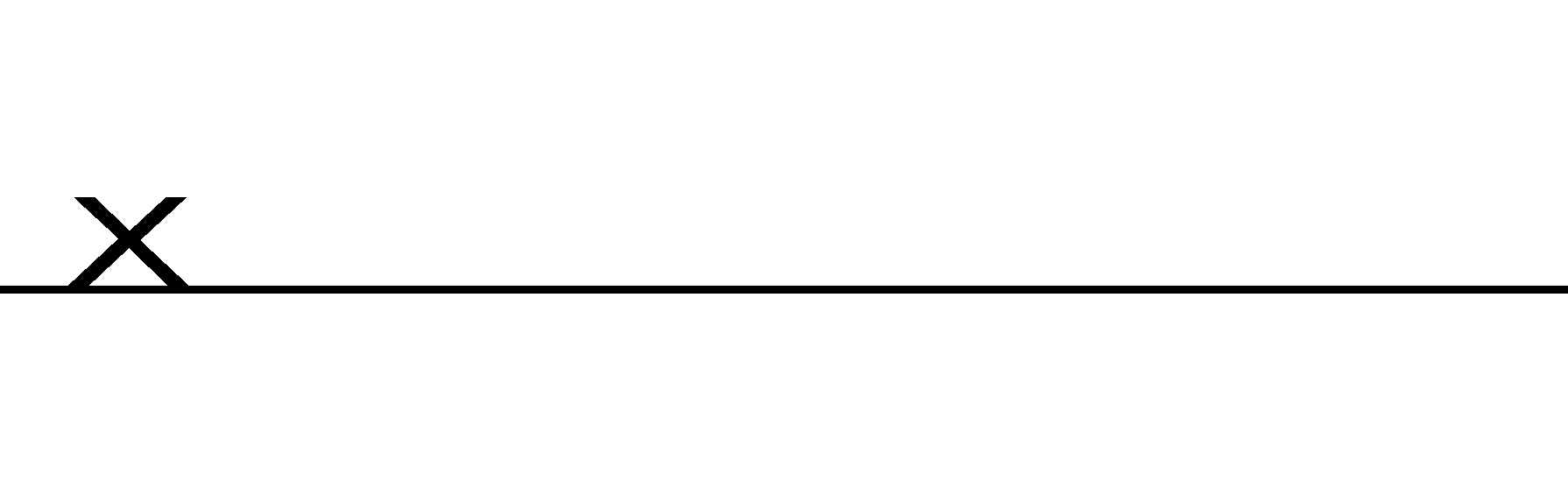
<System Acronym> is delivered as an SaaS offering using a multi-tenant <Deployment Model> cloud computing environment. It is available to <Insert scope of customers exactly as stated in the documentation (for example, Public, Federal Only, Hybrid community)>.

<Brief system description provided by CSP>

Federal Agencies are encouraged to leverage this Agency FedRAMP ATO as a key element of their own ATO as applicable. The package associated with the IaaS and/or PaaS <System Acronym> ATO must be considered with this <System Acronym>ATO. <Federal Agency/Office> believes the <System Acronym> and <System Acronym> FedRAMP Security Authorization Packages accurately document and clearly define the aggregate outstanding risk considerations, when viewed in concert. Agency customers must consider the aggregate risk for the LISaaS and underlying systems when granting an ATO.

Copies of authorization packages are available for agency review in the FedRAMP Secure Repository. If you have any questions or comments regarding this ATO, please contact <Agency ATO contact information>.

**APPROVED:**



<Agency AO Name>

<Agency AO Title>

<Agency Name>

1. *FedRAMP Tailored Low Impact Software-as-a Service (LISaaS) Requirements* and *FedRAMP Tailored Low Impact Software-as-a-Service* *Template* are available at [www.fedramp.gov](http://www.fedramp.gov). [↑](#footnote-ref-1)