MEMORANDUM FOR: OCIO Personnel Involved in Cloud Services Acquisitions and Authorizations

FROM: Paul E. Blahusch, Chief Information Security Officer

X Paul Blahusch

Signed by: PAUL BLAHUSCH

SUBJECT: DOL Policy for Modernizing the Federal Risk and Authorization Management Program (FedRAMP)

Please be advised that the Department of Labor (DOL) has updated its Cybersecurity Policy Portfolio (CPP) Volumes 4, 15, and 22 to align with requirements outlined in the Office of Management and Budget (OMB) Memorandum M-24-15, *Modernizing the Federal Risk and Authorization Management Program (FedRAMP).*

The updated CPP language is:

CPP Volume 4 – Assessment, Authorization, and Monitoring (CA)

Section 2.6, CA-6: Authorization, Additional DOL Requirements:

a. *[Not applicable to FedRAMP policy updates]*
b. Authorizations of cloud products and services must adhere to the process outlined in OMB Memorandum M-24-15, *Modernizing the Federal Risk and Authorization Management Program (FedRAMP).*
    1. DOL is required to leverage a FedRAMP authorization for cloud computing products and services (such as Infrastructure as a Service [IaaS], Platform as a Service [PaaS], and Software as a Service [SaaS] that create, collect, process, store, or maintain Federal information on behalf of DOL, and that are not otherwise specified as out of scope. Out of scope products include:
        a. Information systems that are only used for DOL's operations, hosted on cloud infrastructure or platform, and are not offered as a shared service or do not operate with a shared responsibility model;
        b. Social media and communications platforms used in accordance with DOL social media policies;
        c. Search engines;
        d. Widely available services that provide commercially available information to agencies, but do not collect Federal information;
        e. Ancillary services whose compromise would pose a negligible risk to Federal information or information systems, such as systems that make

external measurements or only ingest information from other publicly available services;

f. Any other categories of products or services identified for exclusion by the FedRAMP Board, with the concurrence of the Federal CIO.

2. DOL must leverage other agency security authorization materials within the FedRAMP repository to the greatest extent possible.
3. When DOL leverages a FedRAMP authorization (e.g., an Agency or Program authorization), DOL must presume the authorization, including the security assessment, is adequate for DOL's use at the given FIPS 199 impact level.
4. When DOL issues or leverages a FedRAMP authorization, the Authorizing Official (AO) or designee must provide to the FedRAMP Program Management Office (PMO):
    a. A copy of DOL's authorization letter and any relevant supplementary information, including DOL-specific configuration information, as deemed appropriate, that may be helpful to other agencies;
    b. Artifacts that meet FedRAMP requirements and are sufficient for reuse by other agencies; and
    c. Authorization materials in machine-readable and interoperable formats (i.e., Open Secure Control Assessment Language [OSCAL]) in accordance with any applicable guidance from FedRAMP.

Section 2.7, CA-7: Continuous Monitoring, Additional DOL Requirements:

a. *[Not applicable to FedRAMP policy updates]*
b. For cloud products and services, the Cloud Service Provider (CSP) implementation of FedRAMP continuous monitoring satisfies continuous monitoring for CSP-implemented controls. Unless a Corrective Action Plan (CAP), Suspension, or Revocation is present in the FedRAMP repository, DOL may presume adequacy of CSP's monitoring of controls.
c. *[Not applicable to FedRAMP policy updates]*
d. *[Not applicable to FedRAMP policy updates]*

Section 2.7, CA-7: Continuous Monitoring, Procedures:

DOL must:

a. Review the FedRAMP repository for documentation of any CAP, Suspension, or Revocation at least monthly; and
b. Review 3PAO assessment results annually.

CPP Volume 15 – System and Services Acquisition (SA)

Section 2.4, SA-4: Acquisition Process, Additional DOL Requirements:

When procuring a cloud product or service, Agencies must:

a. First review the Federal Risk and Authorization Management Program (FedRAMP) marketplace for an existing FedRAMP-authorized product or service; and
b. Include in relevant contracts the FedRAMP security authorization requirements established by the General Services Administration (GSA).

CPP Volume 22 – Supplemental Guidance

CA-6: Authorization:

a. *[Not applicable to FedRAMP policy updates]*
b. *[Not applicable to FedRAMP policy updates]*
c. *[Not applicable to FedRAMP policy updates]*
d. *[Not applicable to FedRAMP policy updates]*
e. *[Not applicable to FedRAMP policy updates]*
f. The FedRAMP "presumption of adequacy" means that DOL can accept the results of a FedRAMP authorization package without conducting additional assessments on the contents of the authorization. DOL is still responsible for assessing and authorizing controls for which it is responsible (e.g., Customer-implemented or Hybrid controls.)
g. For additional information on FedRAMP processes, see OMB Memorandum M-24-15, *Modernizing the Federal Risk and Authorization Management Program (FedRAMP)*.

CA-7: Continuous Monitoring:

FedRAMP Continuous Monitoring

For additional details on FedRAMP continuous monitoring process, see the FedRAMP Continuous Monitoring Performance Management Guide.