U.S. Department of Labor

Office of Inspector General
Washington, DC 20210

March 22, 2023

MEMORANDUM FOR: GUNDEEP AHLUWALIA
Chief Information Officer

FROM: CAROLYN R. HANTZ
Assistant Inspector General
for Audit

SUBJECT: IT Contingency Plan Audit, Project No. 23-P23-003-07-720

Please be advised the Office of Inspector General is initiating an audit of DOL's Information Technology (IT) Contingency Plan process. We will be setting up an Entrance Conference to discuss the following:

Objective: To what extent did the Chief Information Officer (CIO) work with the Department to ensure Contingency Planning maintains the availability of the IT services and systems in a time of emergency.

We plan to begin work immediately after our meeting and would appreciate your notifying the appropriate officials of our plans. To facilitate the start of the audit, we have attached an initial Document Request Listing and would appreciate these items being provided prior to the meeting so we may begin our planning.

If you have any questions, please contact Stephen Fowler, Audit Director, Office of Information Technology Audits, at (202) 693-7013.

Attachment

Document Request Listing
Points of Contact and Policy/Guidance

For the purposes of these requests, "contingency planning" refers to any planning, testing and execution efforts for restoring and/or reconstituting IT systems and services.

Points of Contact (POCs)

Please provide the following information to Naomi Reynolds at Reynolds.Naomi@oig.dol.gov by March 28, 2023.

1. POCs for the Directorate, Division, or Branch within OCIO that is responsible for DOL's contingency planning efforts.
2. OCIO contingency planning POCs and Agency POCs (if applicable) for:
    a. Agencies incorporated as part of IT Shared Services
    b. Bureau of Labor Statistics
    c. Office of Chief Financial Officer
    d. OIG
3. OCIO POC for the Emergency Management Center
4. Primary Emergency Management Center POC for OCIO

Policy/Guidance

Our initial research has identified the following Department policy and guidance regarding Contingency Planning, if there is other applicable material followed or relied upon please let us know:

1. Cybersecurity Policy Portfolio (CPP) Volume 6
2. CPP Volume 22 – Supplemental Guidance
3. DLMS 7-400: IT Security
4. DLMS 7-800: Networks Operations and LAN Management
5. DLMS 7-1100: Safeguarding Sensitives Data Including Personally Identifiable Information

Please provide OCIO specific policies and standard operating procedures related to contingency planning, not listed above, to Naomi Reynolds at Reynolds.Naomi@oig.dol.gov by March 31, 2023.