Appendix D

Agency Response to Draft Report

U.S. Department of Labor

MAR 25 2009

Employment and Training Administration
200 Constitution Avenue, N.W.
Washington, D.C. 20210

MEMORANDUM FOR: ELLIOT P. LEWIS
Assistant Inspector General for Audit

FROM: DOUGLAS F. SMALL
Deputy Assistant Secretary

SUBJECT: Unemployment Insurance Systems' Information Technology Contingency Plans Need Improvement; Draft Audit Report Number: 23-09-001-03-315

Thank you for the opportunity to respond to your draft report cited above. The Employment and Training Administration (ETA) shares your view that effective state information technology (IT) contingency plans are vitally important to ensure that eligible unemployed workers receive unemployment insurance (UI) payments following IT failures caused by disasters or other disruption of normal operations.

While the recommendation provided by this audit is similar to the earlier audit of the SWAs' IT Contingency plans, ETA appreciates the detailed analysis this audit provides on the content of the SWAs' IT contingency plans. The individual SWA IT Contingency Plan assessments as well as the IT Contingency Plan Maturity and Corresponding Risk matrix provides ETA with a better understanding of the current status of SWAs' IT Contingency Planning.

In preparation for Year 2000 (Y2K), ETA made a significant investment (approximately $200 million) of Federal funds to ensure state UI systems would not be disrupted. These efforts included disaster recovery, contingency, and business continuity of operations plans. Because specific funds were provided for these purposes, ETA required and received evidence from each state that these plans had been verified and validated by an independent entity and tested.

Since that time, overall funding for UI, like many other programs, has declined, and no specific funds were available for independent verification and validation of IT contingency plans. Therefore, ETA has relied upon assurances provided by states as a part of their UI administrative grant agreements that they have Disaster Recovery and Automated Information Systems Security plans.

ETA has continued to take a leadership role with states in promoting strategies to minimize service disruptions, operations, and services to UI beneficiaries. In

addition to the leadership efforts previously mentioned in ETA's response to the OIG's draft report "The Federal/State Unemployment Insurance Partnership Needs Enhanced Federal Oversight to Establish Reliable Information Technology Contingency Plans"; Draft Audit Report Number: 23-08-004-03-315, ETA has taken the following steps to promote SWAs IT security and contingency planning.

- Provided states with a compact disk (CD) and an Executive Manager's Paper on current IT Security guidance (2009). The enhanced CD and paper also includes:

    a. IT Security Templates (2005 - 2006, 2009) for various IT Security Plans and Policies.
    b. A Guide to NIST Information Security Documents (2009) which categorizes the over 250 NIST guidance documents by topic, family or legal requirement.
    c. A Roadmap to NIST Information Security Documents (2009) which summarizes the aforementioned Guide in a handy one-page tri-fold format.
    d. Current information (2009) on the NIST Federal Agency Security Practices (FASP) web site. The FASP web site contains information on:
        - Submitted Departmental / Agency Policies and Procedures (Best Practices)
        - Public / Private / Academia Practices
        - FASP Contacts
        - List of Frequently Asked Questions

- Provided $31.6 million in supplemental funds to SWAs from FY 2004 - FY 2007 to resolve IT Security findings addressed by State IT Audits, Federal OIG IT Audits, and/or IT Security Self-Assessments that met NIST SP 800-53 guidance. Many of the efforts for which these funds were used supported IT Contingency / Disaster Recovery activities.

- Updated the ET Handbook No. 336, State Quality Service Plan (SQSP) Ed. 18, (2009 - in clearance) to incorporate:

    a. IT Security guidance including IT Contingency Planning, Risk Management and System Security Planning as well as associated NIST supported template plans.
    b. An updated assurance on IT Contingency Planning:
        (1) Date when implemented
        (2) Date when reviewed / updated

(3) Date when tested

c. An updated assurance on Automated Information Systems Security
   (1) Date when most recent Risk Assessment was conducted
   (2) Date when most recent System Security Plan was reviewed / updated.

Within available resources, we believe that ETA has provided states with strong guidance and leadership related to IT contingency planning. We also believe that ETA's oversight of state IT contingency planning would be greatly strengthen by implementation of the OIG's recommendations to conduct an annual verification of the SWAs' IT Contingency Plans for existence and reliability using risk-based approaches that consider the SWAs' contingency planning maturity and likelihood of disasters.

However, implementation of this recommendation would be quite resource intensive. We estimate that plan development and independent validation and verification of the plans would require about $19 million in the initial year with lower on-going annual costs for updating, maintaining, and testing the plans.

Please be assured that ETA will implement the recommendations of this report to the extent that resources allow. We share your concern that states have adequate IT contingency and disaster recovery plans in place to ensure that UI benefits would continue to be provided in any state impacted by a disaster or other disruption in order to avoid a negative impact on eligible unemployed workers, their families, and communities.