U.S. Department of Labor

Office of Inspector General—Office of Audit

EMPLOYMENT AND TRAINING ADMINISTRATION

THE FEDERAL/STATE UNEMPLOYMENT INSURANCE PARTNERSHIP NEEDS ENHANCED FEDERAL OVERSIGHT TO ESTABLISH RELIABLE INFORMATION TECHNOLOGY CONTINGENCY PLANS

Date Issued: September 29, 2008
Report Number: 23-08-004-03-315

U.S. Department of Labor
Office of Inspector General
Office of Audit

BRIEFLY…

Highlights of Report Number: 23-08-004-03-315, to the Deputy Assistant Secretary for Employment and Training.

WHY READ THE REPORT

As a result of widespread congressional and public interest in disaster preparedness planning, the Office of Inspector General (OIG) conducted a performance audit of the Employment and Training Administration's (ETA) oversight of Information Technology (IT) contingency planning performed by State Workforce Agencies (SWA) in support of the Unemployment Insurance (UI) program.

The UI program, a Federal-state partnership, is the Department of Labor's (DOL) largest income-maintenance program. While Federal law determines the framework of the program, benefits for individuals are dependent on state law and administered by the SWA. The UI program provides unemployment benefits to eligible workers who are unemployed through no fault of their own. The Assistant Secretary of ETA has the responsibility for oversight of the SWAs' administration of the program. SWAs use the UI Tax and Benefit IT Systems to administer and deliver benefits to eligible claimants.

WHY OIG DID THE AUDIT

The purpose of our audit was to answer the following question:

> Does ETA provide sufficient oversight of SWAs IT contingency planning for the UI program in order to minimize service disruption in the event of a disaster or other situation that may disrupt normal operations?

READ THE FULL REPORT

To view the report, including the scope, methodology, and full agency response, go to:

http://www.oig.dol.gov/public/reports/oa/2008/23-08-004-03-315.pdf

September 2008

The Federal/State Unemployment Insurance Partnership Needs Enhanced Federal Oversight to Establish Reliable Information Technology Contingency Plans

WHAT OIG FOUND

Our audit disclosed that ETA requires the SWAs to develop and implement disaster-recovery plans as a condition of their grant agreements, but does not verify that the plans are developed, tested, or meet accepted practices. Our audit showed that three of four SWAs audited may not be able to recover the UI Tax and Benefit Systems necessary to maintain operational capability in a timely, orderly manner or perform essential functions during an emergency or other situation that may disrupt normal operations. We also found inconsistent validation methodologies used among the SWAs for reaching assurance of a disaster-response capability.

These conditions occurred because ETA has not fully carried out its leadership responsibilities in overseeing the UI program by providing needed oversight and targeted guidance to the SWAs regarding ETA's expectation of an IT disaster-recovery capability. ETA had not ensured the SWAs developed and maintained contingency plans.

As a result, ETA does not have assurance that UI program benefits would be provided to eligible claimants in the event of a disaster or service disruption which could have a negative financial impact on individuals, families, and state economies. Without ETA providing effective oversight and guidance, it is not likely reliable SWA contingency plans will be in place when needed the most. Further, ETA officials do not have a high degree of knowledge or involvement in the SWAs' readiness to deal with how disasters affect their delivery of benefits to eligible claimants.

WHAT OIG RECOMMENDED

We recommended that the Assistant Secretary for Employment and Training: enact a monitoring and review process to verify SWAs develop and test IT contingency plans necessary to sustain the UI program; and identify and address any weaknesses found in IT contingency plans. The Deputy Assistant Secretary for Employment and Training agreed with the recommendations.

Table of Contents

PAGE WAS INTENTIONALLY LEFT BLANK

Executive Summary

As a result of widespread congressional and public interest in disaster preparedness planning, the Office of Inspector General (OIG) conducted a performance audit of the Employment and Training Administration's (ETA) oversight of Information Technology (IT) contingency planning performed by State Workforce Agencies (SWA) in support of the Unemployment Insurance (UI) program. The UI program, a Federal-state partnership, is the Department of Labor's (DOL) largest income maintenance program. While Federal law determines the framework of the program, benefits for individuals are dependent on state law and administered by SWA. The UI program provides unemployment benefits to eligible workers who are unemployed through no fault of their own. The Assistant Secretary of ETA has the responsibility for oversight of the SWAs' administration of the program. SWAs use the UI Tax and Benefit IT Systems to administer and deliver benefits to eligible claimants.

The audit objective was to answer the following question:

Does ETA provide sufficient oversight of SWAs IT contingency planning for the UI program in order to minimize service disruption in the event of a disaster or other situation that may disrupt normal operations?

To achieve our objective, we evaluated contingency plans in place at four SWAs. We also reviewed ETA oversight activities at ETA regional offices (RO) and ETA's headquarters (HQ).

Summary of Results and Findings

ETA needs to strengthen its oversight of SWA IT contingency planning for the UI program in order to minimize service disruption in the event of a disaster or other situation that may disrupt normal operations.

Our audit disclosed that, while ETA requires SWAs to develop and implement disaster recovery plans as a condition of their grant agreements, it does not verify that the plans are developed or tested. Our audit showed that three of four SWAs audited may not be able to recover the UI Tax and Benefit Systems necessary to maintain operational capability in a timely, orderly manner or perform essential functions during an emergency or other situation that may disrupt normal operations. Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources* (A-130), states that agency managers should ensure contingency plans be periodically tested to perform the agency function supported by the computer application in the event of failure of its automated support.

For three SWAs, we identified the following deficiencies:

- One SWA did not develop an IT contingency plan for the UI Tax and Benefit System even though it had obtained supplemental grants totaling $198,500 for this purpose. In years when funding is available, ETA awards supplemental funds to selected SWAs to address the UI IT security weaknesses that have been identified by previous security audits, or by SWA IT self-assessment that comply with National Institute of Standards and Technology (NIST) IT security guidelines. SWAs apply for these funds through supplemental budget requests that address a specific security weakness. By submitting the proposal, the SWA agrees to provide any additional funds, if needed, to complete the project. The SWA was able to provide us with a project plan to complete the IT contingency plan, but officials told us they could not identify the resources that will be needed to maintain it.
- One SWA did not address the recovery of all critical systems and components necessary to ensure continuity of operations. Specifically, the plan did not address an alternative to printing benefit checks in the event of a service disruption at the state's check printing facility. In addition, the plan did not include adequate backup telecommunications systems or procedures to allow for reconstitution of all UI systems.
- One SWA had not updated its IT contingency plan since 2004, and it contained information that was either outdated, obsolete, or missing. In addition, the plan contained deficiencies in the design and implementation of controls that are critical to ensure the continued functioning of the UI program. We also found the two other SWAs did not update their contingency plans in a timely manner.

In addition, three of the four SWAs did not have a training program for personnel with critical IT UI roles and responsibilities; did not finalize and implement IT contingency-planning policies; and had not performed adequate testing of their IT contingency plans. In addition, the SWAs did not have, or used inconsistent validation methods, for basing their assurance of disaster-response capability.

These conditions occurred in part because ETA did not provide effective oversight and lacked necessary policies and procedures to verify that SWAs developed and tested contingency plans for the UI Tax and Benefit System. As a result, ETA does not have assurance that UI program benefits would be provided to eligible claimants in the event of a disaster or service disruption which could have a negative financial impact on individuals, families, and state economies.

Recommendations

In summary, we recommend the Assistant Secretary for Employment and Training: enact a monitoring and review process to verify SWAs develop and test IT Contingency Plans necessary to sustain the UI program; and identify and address any weaknesses found in IT contingency plans.

Agency Response

The Deputy Assistant Secretary for Employment and Training agreed the recommendations will enhance ETA's ability to perform oversight of IT contingency planning in the SWAs; and also provided funding estimates needed to implement the recommendations. ETA's response also outlined efforts the agency has made regarding IT contingency planning over the past eight years within its available resources. The response is provided in full in Appendix D.

OIG Conclusion

Based on ETA's response to the draft report, the report recommendations remain unresolved. The recommendations will be resolved when ETA provides documentation indicating plans and milestone dates for implementing corrective actions. The recommendations will be closed upon receipt of documentation showing that the planned corrective actions have been completed, and OIG verifications of those actions.

PAGE WAS INTENTIONALLY LEFT BLANK

U.S. Department of Labor

Office of Inspector General
Washington, DC 20210

September 29, 2008

Assistant Inspector General's Report

Mr. Brent R. Orrell
Deputy Assistant Secretary for
Employment and Training
U. S. Department of Labor
Frances Perkins Building
200 Constitution Avenue, NW
Washington, DC 20210

The devastating impact of Hurricanes Katrina and Rita to the Gulf Coast Region in 2005 has increased awareness of the effects natural disasters can have on our society. The Department's agencies have felt the impact internally, particularly in ETA in its responsibility for oversight of the Federal-State UI program. The UI program, a Federal-State partnership, is the Department's largest income-maintenance program. The UI program provides unemployment benefits to eligible workers who are unemployed through no fault of their own. The Assistant Secretary of ETA has the responsibility for oversight of the SWAs' administration of the program. Collaboratively, ETA provides oversight through guidance, direction and distribution of administrative funds to the SWAs, while SWAs utilize the UI Tax and Benefit IT Systems to administer and deliver benefits to eligible claimants. ETA provides administrative funding to the SWAs via annual UI funding agreements (grant agreements), which contain requirements for the SWAs to ensure timely UI benefits payments can be made.

As a result of widespread congressional and public interest in disaster preparedness planning, the OIG conducted a performance audit of ETA's oversight of IT contingency planning performed by SWAs in support of the UI program. In the aftermath of the 2005 hurricanes, Federal officials began to question the ability of the SWAs to continue operating the UI program without interruption in the event of a disaster or other service disruption. The OIG initiated this audit of SWA IT contingency plans for the UI tax and benefit systems based on the Assistant Secretary of ETA's inquiry regarding their viability.

Specifically, the audit objective was to answer the following question:

> Does ETA provide sufficient oversight of SWA IT contingency planning for the UI program in order to minimize service disruption in the event of a disaster or other situation that may disrupt normal operations?

We tested to determine if the SWAs have adequate IT contingency plans in place to support critical UI program functions in the event of a disaster or service disruption to

the IT supporting the UI program. We selected a sample of four SWAs from a universe of 53 for detailed examination. These states were determined to be high risk based on historical data and professional judgment regarding frequency of disasters declared in each state from the Federal Emergency Management Agency (FEMA). In addition, we assessed the Federal oversight of SWA IT contingency planning and UI grant administration. This was accomplished through assessing the monitoring activities conducted by ETA in support of the Federal-State UI partnership. We reviewed the Federal-State UI grant agreement and the level of guidance, review and monitoring done at the Federal level by ETA.

Based on our audit results, we concluded ETA needs to strengthen its oversight of SWA IT contingency planning for the UI program in order to minimize service disruptions in the event of a disaster or other situation that may disrupt normal operations. This report details our findings and recommendations related to our objective.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Our objective, scope, methodology, and criteria are detailed in Appendix B.

Objective – Does ETA provide sufficient oversight of SWA IT contingency planning for the UI program in order to minimize service disruption in the event of a disaster or other situation that may disrupt normal operations?

ETA needs to strengthen its oversight of SWA IT contingency planning for the UI program in order to minimize service disruptions in the event of a disaster or other situation that may disrupt normal operations.

Our audit disclosed that ETA requires the SWAs to develop and implement disaster recovery plans as a condition of their grant agreements. However, ETA does not verify the plans are developed, tested, or meet accepted practices. Our audit showed that three of four SWAs audited may not be able to recover the UI Tax and Benefit Systems necessary to maintain operational capability in a timely, orderly manner or perform essential functions during an emergency or other situation that may disrupt normal operations. We also found inconsistent validation methodologies used among the SWAs for reaching assurance of a disaster-response capability.

These conditions occurred because ETA has not fully carried out its leadership responsibilities in overseeing the UI program by providing needed oversight and targeted guidance to the SWAs regarding ETA's expectation of an IT disaster-recovery capability. ETA lacked the necessary policies and procedures to verify that the SWAs have developed and tested contingency plans for the UI Tax and Benefit System. Further, the SWAs did not recognize the importance of the assurance statements in the grant administration process. ETA had not ensured the SWAs developed and maintained plans, and several SWAs had not placed a focus on IT contingency planning.

As a result, ETA does not have assurance that UI program benefits would be provided to eligible claimants in the event of a disaster or service disruption which could have a negative financial impact on individuals, families, and state economies. Without ETA providing effective oversight and guidance, it is not likely reliable SWA contingency plans will be in place when needed the most. Further, ETA officials do not have a high degree of knowledge or involvement in the SWAs' readiness to deal with how disasters affect their delivery of benefits to eligible claimants.

The Social Security Act of 1935, section 303 (a)(1), requires that the SWAs have means of administering the UI program that ". . . are found by the Secretary of Labor to be reasonably calculated to insure full payment of unemployment compensation when due." In order for the Secretary of Labor to ensure that SWAs have adequate disaster-recovery capabilities, the grant agreement between DOL and each SWA contains an assurance of disaster-recovery capability. Assurance H in the grant agreement is the "Assurance of Disaster Recovery Capability," which is explained in further detail in Employment and Training (ET) Handbook No. 336, as "The state assures that it will maintain a Disaster Recovery Plan." Each SWA must attest to this assurance via

signature in order to receive annual Federal grant funding for the administration of the SWA UI program.

The following are areas in which weaknesses were found in UI IT contingency plans and related oversight.

I. Unreliable IT Contingency-Planning Capabilities

Through our audit of a sample of four high-risk states and collection of IT contingency plans from the SWAs, we determined that IT contingency-planning activities conducted by the SWAs were not adequate and may not allow for the timely recovery of the UI programs if the IT supporting those programs were affected by a disaster or other service interruption. Three of four SWAs audited may not be able to recover the UI Tax and Benefit Systems necessary to maintain operational capability in a timely, orderly manner or perform essential functions during an emergency or other situation that may disrupt normal operations. Additionally, our analysis of all 53 SWAs' responses to our request for IT contingency plans revealed that 2 SWAs had no plan at all, although all 53 have certified in their grants they have disaster-recovery capability.

Specifically, in the four SWAs we identified the following:

- One SWA did not develop an IT contingency plan for the UI Tax and Benefit System. The SWA had obtained $198,500 from supplemental ETA grants for this purpose. In years when funding is available, ETA awards supplemental funds to selected SWAs to address the UI IT security weaknesses that have been identified by previous security audits, or by SWA IT self-assessment that comply with NIST IT security guidelines. SWAs apply for these funds through supplemental budget requests that address a specific security weakness. By submitting the proposal, the SWA agrees to provide any additional funds, if needed, to complete the project. While the SWA provided a project plan to complete the IT contingency plan, it had not identified the resources needed to develop the contingency plan once completed.
- One SWA's contingency plan did not address the recovery of all critical systems and components necessary to ensure continuity of operations. Specifically, the plan did not address an alternative to printing benefit checks in the event of a service disruption at the state's check printing facility. In addition, the plan did not include adequate backup telecommunications systems or procedures to allow for reconstitution of all UI systems.
- One SWA had not updated its IT contingency plan since 2004, and the plan contained information that was either outdated, obsolete, or missing. In addition, the plan contained deficiencies in the design and implementation of controls that are critical to ensure the continued functioning of the UI program.
- One SWA had a generally robust IT contingency-planning capability; however, the SWA had not implemented an IT contingency-planning policy. This robustness was based on the SWA implementing key controls to support its IT contingency-planning capability including maintaining critical UI information

> system backups, having alternate processing and storage facilities, utilizing telecommunications redundancy, documenting reconstitution procedures, as well as testing its IT contingency-planning capability.

In accordance with NIST Special Publication (SP) 800-34, *Contingency Planning Guide for Information Technology Systems* (NIST SP 800-34), proper IT contingency planning can assist in maintaining the continued availability of an information system in the event of disaster or other system disruption.

II. Specific Contingency-Planning Control Deficiencies

Based on the analysis of the commonalities in control deficiencies identified across the four SWAs audited, we found specific issues in IT contingency-planning training, updating, policy, and testing. Three of the four states audited had no training program for personnel with critical IT UI roles and responsibilities; did not update IT contingency plans in a timely manner; did not have finalized and implemented IT contingency-planning policies in place; and had not performed adequate testing of their IT contingency-planning capabilities. Each deficiency is detailed below:

IT Contingency Plan Training

Three of the four SWAs had no training program for personnel with critical IT UI roles and responsibilities. In one SWA, training had not been done in four years, and the auditors were told this was because the core personnel had remained static since the training was conducted.

NIST SP 800-34, notes:

> Training for personnel with contingency plan responsibilities should complement testing. Training should be provided at least annually; new hires who will have plan responsibilities should receive training shortly after they are hired. Ultimately, contingency plan personnel should be trained to the extent that that they are able to execute their respective recovery procedures without aid of the actual document. This is an important goal in the event that paper or electronic versions of the plan are unavailable for the first few hours resulting from the extent of the disaster.

IT Contingency Plan Updates

In three of the four SWAs the IT contingency plans were not updated in a timely manner. In one of those three SWAs, the plan had not been updated since 2004 (a three year time lapse). In another, the update was done annually; however, the auditors found names and contact information that were incorrect because they had changed since the previous update.

NIST SP 800-34 relates:

> To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. IT systems undergo frequent changes because of shifting business needs, technology upgrades, or new internal or external policies. Therefore, it is essential that the contingency plan be reviewed and updated regularly, as part of the organization's change management process, to ensure new information is documented and contingency measures are revised if required.

IT Contingency Plan Policy

Three of four SWAs did not have finalized and implemented IT contingency-planning policies in place at the time our audit, although two of these SWAs' policies were in various stages of development.

NIST SP 800-34 describes:

> To be effective and to ensure that personnel fully understand the agency's contingency planning requirements, the contingency plan must be based on a clearly defined policy. The contingency planning policy statement should define the agency's overall contingency objectives and establish the organizational framework and responsibilities for IT contingency planning. To be successful, senior management, most likely the Chief Information Officer, must support a contingency program. These officials should be included in the process to develop the program policy, structure, objectives, and roles and responsibilities.

IT Contingency Plan Testing

Three of four SWAs performed inadequate testing of their IT contingency-planning capabilities. In one SWA, no testing was done at all; in another, testing had not been completed since 2006 (a 15 month time lapse); and in a third SWA, a comprehensive test involving all of the necessary systems for administering the UI program had never been completed.

NIST SP 800-34 states:

> Plan testing is a critical element of a viable contingency capability. Testing enables plan deficiencies to be identified and addressed. Testing also helps evaluate the ability of the recovery staff to implement the plan quickly and effectively. Each IT contingency plan element should be tested to confirm the accuracy of individual recovery procedures and the overall effectiveness of the plan.

III. Inconsistent Validation Methodologies

We found inconsistent validation methodologies used among the four SWAs for reaching assurance of a disaster-response capability they attest to ETA annually in their grant agreements. Across the four SWAs audited we found:

- In one SWA, budget and fiscal officials stated they have comfort in signing the assurance of a disaster-recovery capability based on the knowledge that there is a continuity-of-business plan for the SWA. When asked if there is any review of the IT contingency plan, they stated they are aware the Information Security Office (ISO) puts the plan together and that was satisfactory. However, the ISO does not perform, and has no expectations of, an integrated review that incorporates the multiple branches of the SWA for the purpose of coordinating the IT contingency plan.
- In one SWA, the auditors were unable to determine whether the State's Secretary of Labor sought input from anyone with regard to IT disaster recovery before signing the grant agreement. IT officials did not discuss the grant agreement with the Secretary, yet they expressed confidence the Secretary was aware of the assurance of IT disaster recovery.
- In one SWA, program officials look at the assurance statements in the grant agreement and determine if anything has been added from the previous year, and, if not, they presumptuously sign the document. According to SWA officials, this is a process they have been doing for many years, which started before the current officials joined the SWA.
- In one SWA, the signatory official was highly involved in the IT contingency plan process and aware of the capability when signing; however, this was not due to any specific actions taken by ETA.

Although there is no specific criteria for states to utilize in verifying their respective disaster-response capability assurances, ETA may respond to noncompliance of an assurance in the grant agreement. Specifically, Title 29, Code of Federal Regulations (CFR), Section 97.43 (29 CFR 97.43), establishes ETA as an enforcement authority empowered to award the grant only when all requirements of it are met. Additionally, 29 CFR, Section 97.50 (29 CFR 97.50), entitles ETA to respond to noncompliance with an assurance by taking action ranging from withholding current or future funding, holding hearings or pursuing further legal remediation.

IV. Insufficient ETA Oversight

Assurance of Grant Compliance

ETA requires the SWAs to develop and implement disaster-recovery plans as a condition of their grant agreements. ETA, however, does not verify the plans are developed, tested, or meet accepted practices. As the Federal agency responsible for monitoring the proper stewardship of Federal grant funding by the SWAs for the administration of the UI program, ETA is responsible to ensure the SWAs are in

compliance with all provisions of the Federal UI grant agreement. The agreement lays out requirements of receiving these Federal resources. Without assurance the SWAs meet the requirements of their respective grant agreements, ETA cannot ensure resources are being properly utilized. ETA Office of Workforce Security officials stated the assurances in the grant agreements are self-certifications. ETA officials from the three ROs with direct oversight responsibility for the audited SWAs' also stated they do not complete any systematic verification to determine if the SWAs maintain the assurances of an IT disaster-recovery capability. ETA, therefore, accepts the SWAs' assurance statements at face value. ETA officials were unaware that a State with a high frequency of declared disasters had no IT contingency plan for the UI program at all until we presented our audit results to them. Based on this, we concluded ETA officials do not have a high degree of knowledge or involvement in the SWAs' readiness to deal with disasters that may effect their systems.

OMB Circular A-123, *Management's Responsibility for Internal Control, Introduction*, (A-123), describes agency managers' and staff's responsibilities for efficient use of resources as:

> The proper stewardship of Federal resources is a fundamental responsibility of agency managers and staff. Federal employees must ensure that government resources are used efficiently and effectively to achieve intended program results. Resources must be used consistent with agency mission, in compliance with law and regulation, and with minimal potential for waste, fraud, and mismanagement.

Compliance with Social Security Act

Maintaining IT contingency plans is a requirement of SWAs receiving Federal funding for the administration of the UI Program. ETA officials did not, however, require the SWAs to maintain such plans pursuant to meeting Federal law outlined in the Social Security Act. This Act requires state laws provide for methods of administration as will reasonably ensure the prompt and full payment of unemployment benefits to eligible claimants, and collection and handling of income for the State unemployment fund, with the greatest accuracy feasible. Title 20, CFR- Employee Benefits, Part 602 - *Quality Control in the Federal-State Unemployment Insurance System* (20 CFR 602), contains the Secretary of Labor's interpretation of the Social Security Act section 303 (a)(1), "Such methods of administrations … as are found by the Secretary of Labor to be reasonably calculated to insure full payment of unemployment compensation when due."

The Secretary's interpretation of Social Security Act section 303 (a)(1) is as follows:

> (a) The Secretary interprets section 303(a)(1), Social Security Act, to require that a State law provide for such methods of administration as will reasonably ensure the prompt and full payment of unemployment benefits to eligible claimants, and collection and handling of income for the State

> unemployment fund (particularly taxes and reimbursements), with the greatest accuracy feasible.

ETA stated the SWAs would be able to administer the UI program manually in case of a disaster. OMB A-130 specifically notes that manual processes are not an acceptable solution for interruptions to service:

> Inevitably, there will be service interruptions. Agency plans should assure that there is an ability to recover and provide service sufficient to meet the minimal needs of users of the system. Manual procedures are generally NOT a viable back-up option. When automated support is not available, many functions of the organization will effectively cease. Therefore, it is important to take cost effective steps to manage any disruption of service.

OMB A-130 outlines that managers should implement security controls, including IT contingency planning, consistent with guidance developed by NIST for automated systems. NIST provides specific guidelines for IT contingency planning.

Guidance

ETA does help the SWAs understand the use of industrial best practices for IT contingency plan development by distributing relevant information regarding industry best practices. In previous years, ETA has issued guidance to the SWAs regarding IT security control implementation. In June 2004, ETA issued Unemployment Insurance Program Letter (UIPL) No. 24-04 - *Unemployment Insurance Information Technology Security*. The purpose of UIPL No. 24-04 was to provide SWAs with specific information on NIST IT security guidelines and a software tool for conducting a security self-assessment of UI systems. The SWAs are encouraged to use this guidance, but there is no requirement to adhere to it or to use the self-assessment tool. In addition, the NIST guidance encompasses many IT security controls and is not targeted for IT contingency planning.

The SWAs are not required by law to meet Federal guidelines for securing the SWA UI Systems. However, ETA, in the absence of equal or better policy, should rely on Federal guidance to accomplish effective oversight in determining what constitutes required SWA IT contingency plans. OMB A-130 describes managers' responsibilities for contingency planning, as follows:

> Managers should plan for how they will perform their mission and/or recover from the loss of existing application support, whether the loss is due to the inability of the application to function or a general support system failure. Experience has demonstrated that testing a contingency plan significantly improves its viability. Indeed, untested plans or plans not tested for a long period of time may create a false sense of ability to recover in a timely manner.

Conclusion

There is concern that the deficiency in ETA's oversight and the conditions found in the SWAs occurred in part from ETA not taking needed and appropriate leadership actions to carry the message to the SWAs regarding the importance of the assurance statement in the grant agreement. We found ETA lacked necessary policies and procedures to verify that the SWAs developed and tested contingency plans for the UI Tax and Benefit System which contributes to this concern. In addition, ETA did not have a process in place to verify the SWAs assurance of a disaster-response capability, which in turn led to the SWAs not focusing on IT contingency planning.

According to one SWA's Business Impact Analysis for the UI program:

> UI offers the first line of defense against the ripple effects of unemployment by providing payments to unemployed workers to ensure that at least a proportion of life's necessities can be met on a week-to-week basis while searching for work.

In the event of a major disruption that delays or halts the UI program, unemployed workers may suffer grave consequences and a state's economy would be affected. One SWA estimated the potential affect of such an occurrence to be $7 million, also resulting in 44,500 individuals not receiving their unemployment benefits checks and 10,000 individuals not filing UI claims.

Recommendations

We recommend the Assistant Secretary for ETA:

1) Develop a comprehensive framework for IT contingency planning that when implemented by the SWAs provides a consistent level of risk reduction. This framework shall include minimum standards regarding implementation of critical control elements of an IT disaster-recovery capability that are widely recognized to be necessary to reduce the risk of system unavailability. For example, update the ET Handbook to expand the details of Assurance H. "Assurance of Disaster Recovery Capability" in ET Handbook No. 336, *Unemployment Insurance SQSP Planning and Reporting Guidelines, 18th Edition,* to include this framework.

2) Develop and implement a monitoring and review process whereby ETA or a third party:

   a) Verifies that SWAs have IT contingency plans as required in the grant agreement;
   b) Ensures SWA IT contingency plans will provide adequate support to critical UI program functions in the event of a disaster or service disruption by validating and signing-off on each SWAs' grant agreement's assurance of a disaster-recovery capability; and

c) Ensures any IT contingency-planning weaknesses identified in the validations, or independently by the SWAs, are captured in specific corrective action plans for remediation which will include acceptable timelines for completion.

Agency Response

The Deputy Assistant Secretary for Employment and Training agreed the recommendations will enhance ETA's ability to perform oversight of IT contingency planning in the SWAs; and also provided funding estimates needed to implement the recommendations. ETA's response also outlined efforts the agency has made regarding IT contingency planning over the past eight years within its available resources. The response is provided in full in Appendix D.

OIG Conclusion

Based on ETA's response to the draft report, the report recommendations remain unresolved. The recommendations will be resolved when ETA provides documentation indicating plans and milestone dates for implementing corrective actions. The recommendations will be closed upon receipt of documentation showing that the planned corrective actions have been completed, and OIG verifications of those actions.

Elliot P. Lewis

PAGE WAS INTENTIONALLY LEFT BLANK

Appendices

PAGE WAS INTENTIONALLY LEFT BLANK

APPENDIX A

BACKGROUND

In 1935, in order to confront the economic woes in the United States caused by massive job losses during the Great Depression the Federal-State UI program was created to help out-of-work individuals, businesses, and the nation's economy as a whole. The purpose of the program is to provide aid to individuals who are unemployed due to circumstances outside of their control**.**

The UI program, a Federal-State partnership, is DOL's largest income-maintenance program. The primary law that established the Federal-State UI partnership is the Social Security Act of 1935. In accordance with Title III, Section 302, of the Social Security Act, which authorizes the Secretary of Labor to provide funds to administer the UI program, and Sections 303 (a) (8) and (9), which govern the expenditure of those funds, the Secretary of Labor has a responsibility to ensure the funds are appropriately approved for reporting to the Secretary of the Treasury.

While Federal law determines the framework of the program, benefits for individuals are dependent on state law and administered by the SWAs. The Federal government is charged with collecting taxes; distributing administrative funding to the states; maintaining responsibility for the Unemployment Trust Fund; setting and tracking performance measures; monitoring compliance with both Federal and state regulations; and creating policy nationwide for administering the program. The SWAs are charged with constructing policy and procedures in accordance with Federal criteria; establishing and collecting state taxes; validating claims and paying them out when acceptable; and running the program according to existing criteria.

According to 20 CFR, Part 602, the Secretary's interpretation of the Social Security Act section 303 (a)(1), is, in part, "Such methods of administrations…as are found by the Secretary of Labor to be reasonably calculated to insure full payment of unemployment compensation when due."

The Secretary of Labor oversees the program through ETA, which oversees the UI program. ETA provides administrative funding to the SWAs via annual UI Funding agreements (i.e. grant agreements), which contain requirements of the SWAs. Although the Federal Government is charged with providing funds for the administration of the UI program, since 1995, there has been a decline in this funding to SWAs from DOL. This is due to grant calculations no longer taking inflation into account. Some SWAs supplement Federal funds with state funding to help cover the administrative costs of the UI program. Further, the SWAs have had increased difficulty in receiving additional funds for the administration of the program in times of high unemployment.

Some of the requirements of the grant agreement are included in the assurances that each SWA must annually attest to via signature in order to receive annual Federal grant funding for the administration of the SWA UI program. In order for the Secretary of

Labor to ensure that SWAs have adequate disaster-recovery capabilities, the grant agreement between the DOL and each SWA contain an assurance of disaster-recovery capability. The SWAs must also submit State Quality Service Plans (SQSPs) with their UI grant applications in order to receive Federal funding for the year. The SQSP serves as a tool for the SWA UI program to plan and report performance goals to DOL. Item 10 of the grant agreement requires the SWAs (grantees) to comply with the assurances in the grant and is incorporated by reference into the SQSP:

> 10. Certifications and Assurances. In performing its responsibilities under this agreement, the Grantee will fully comply with the following SQSP assurances, which are incorporated into this agreement by reference. The SQSP assurances are listed below and are detailed in Chapter 1, Part VII of the *SQSP Planning and Reporting Guidelines*, Employment and Training Handbook No. 336 (18th Edition).

The "Assurance of Disaster Recovery Capability" (Assurance H) is explained in more detail in ET Handbook No. 336, 18th Edition*, Unemployment Insurance SQSP Planning and Reporting Guidelines*. The handbook details that, "The state assures that it will maintain a Disaster Recovery Plan."

IT contingency planning is an essential element of a disaster-recovery capability. Proper contingency planning ensures the continued availability of an information system in the event of a disruption due to a disaster or other system interruption. The Secretary requires the SWAs to attest to this capability in order to reduce the risk of UI program unavailability. In accordance with NIST SP 800-34, proper IT contingency planning can assist in maintaining the continued availability of an information system in the event of disaster or other system disruption:

> IT systems are vulnerable to a variety of disruptions, ranging from mild (e.g., short-term power outage, disk drive failure) to severe (e.g., equipment destruction, fire). Many vulnerabilities may be minimized or eliminated through technical, management, or operational solutions as part of the organization's risk management effort...Contingency planning is designed to mitigate the risk of system and service unavailability by focusing on effective and efficient recovery solutions.

OMB A-130 specifically notes that manual processes are not an acceptable solution for interruptions to service:

> Inevitably, there will be service interruptions. Agency plans should assure that there is an ability to recover and provide service sufficient to meet the minimal needs of users of the system. Manual procedures are generally NOT a viable back-up option. When automated support is not available, many functions of the organization will effectively cease. Therefore, it is important to take cost effective steps to manage any disruption of service.

In addition, OMB A-130 explores the importance of testing for contingency plans noting that:

> Experience has shown that recovery plans that are periodically tested are substantially more viable than those that are not. Moreover, untested plans may actually create a false sense of security.

OMB A-130 also stresses the importance of NIST as a tool to guide management in IT contingency planning, detailing that managers should:

> Plan for adequate security of each general support system as part of the organization's information resources management planning process. The security plan shall be consistent with guidance issued by the National Institute of Standards and Technology.

PAGE WAS INTENTIONALLY LEFT BLANK

APPENDIX B

OBJECTIVE, SCOPE, METHODOLOGY AND CRITERIA

Objective

Our audit was designed with the following overall objective:

> Does ETA provide sufficient oversight of SWA IT contingency planning for the UI program in order to minimize service disruption in the event of a disaster or other situation that may disrupt normal operations?

Scope

We conducted audit fieldwork from August 2, 2007, through June 3, 2008. During this period we assessed the monitoring program in place at ETA to determine the sufficiency of its oversight regarding the SWAs' development of IT contingency plans. We conducted detailed audit work assessing the adequacy of the SWA UI system IT contingency plans in four disaster-prone SWAs. In addition, we determined if plans were in place for all 53 SWAs. Our audit included a review of laws and regulations which were reviewed for compliance. This audit was not designed to follow-up on any previous OIG or other organization audit reports.

In planning and performing our audit, we considered internal controls related to SWA IT contingency-planning activities for the UI program and ETA's monitoring of these activities by obtaining an understanding of the program's internal controls, determining whether internal controls had been placed in operations, and assessing control risk in order to determine our auditing procedures for the purpose of achieving our objective. The objective of our audit was not to provide assurance on the internal controls. Consequently, we did not express an opinion on the internal controls as a whole, but rather how they related to our objective. Therefore, we evaluated the internal controls as they pertained to ETA's monitoring of the SWAs' assurances of disaster-recovery capability.

Our consideration of internal controls related to ETA's monitoring of the SWAs' assurances of disaster-recovery capabilities would not necessarily disclose all matters that might be reportable conditions. Because of inherent limitations in internal controls, misstatements, losses, or noncompliance may nevertheless occur and may not be detected.

Our audit scope included an assessment of IT contingency-planning activities. The grant agreement between ETA and the SWAs requires maintenance of a disaster-recovery plan for the UI program, which we interpreted as IT contingency plans. In accordance with NIST SP 800-34:

> IT contingency planning represents a broad scope of activities designed to sustain and recover critical IT services following an emergency… In general, universally accepted definitions for IT contingency planning and these related planning areas have not been available. Occasionally, this unavailability has led to confusion regarding the actual scope and purpose of various types of plans…Because of the lack of standard definitions for these types of plans, in some cases, the scope of actual plans developed by organizations may vary.

NIST SP 800-34 goes on to define Disaster Recovery Plans (DRP) as follows: "Frequently, DRP refers to an IT-focused plan designed to restore operability of the target system, application, or computer facility at an alternate site after an emergency."

Specific work was conducted using a sample of FY2008 SWA UI grant agreements as well as the current IT contingency plans. Fieldwork was completed in four SWAs, three ETA ROs, and the ETA HQ in Washington, DC. Our sampling methodology for detailed contingency plan testing is based on FY 2007 FEMA data of the highest number of disasters declared by state, and comprised the following SWAs: California (CA), Texas (TX), New York (NY), and Louisiana (LA). Selection of these four SWAs led us to review the three ETA ROs located in Dallas, TX; San Francisco, CA; and Boston, Massachusetts with administrative responsibility over the SWAs. Our risk-based approach allowed us to assess all SWAs' contingency plans to some degree, with more focused attention on the highest risk states, based on historical data.

We performed on-site fieldwork at four SWAs where we observed SWA personnel activities; inspected relevant documentation; performed operational security tests when applicable, including expanded testing in the CA SWA. We also interviewed management and staff involved in the implementation and management of the disaster-recovery capabilities at the SWAs to understand the current IT contingency-planning capabilities and the awareness of preparedness and personnel in key roles at the respective SWA locations.

Our on-site fieldwork in the SWAs was conducted in a sequential basis in the four SWAs, as follows:

- At the CA SWA, Employment Development Department (EDD), located in Sacramento, CA from August 24, 2007, through October 26, 2007. Analysis and testing of documentation received occurred at the CA EDD Central Office and our Washington, DC HQ.
- At the NY SWA, New York Department of Labor (NY DOL), located in Albany, NY from November 13, 2007, through December 21, 2007. Analysis and testing of documentation received occurred at the NY DOL Central Office and our Washington, DC HQ.
- At the LA SWA, Louisiana Department of Labor (LDOL), located in Baton Rouge, LA from January 8, 2008, through February 7, 2008. Our audit work included

interviews with the LDOL, and analysis and testing of documentation received at the LDOL Building and our Washington, DC HQ.
- At the TX SWA, Texas Workforce Commission (TWC), located in Austin, TX from January 22, 2008, through February 28, 2008. Analysis and testing of documentation received occurred at the TWC Building and our Washington, DC HQ.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Methodology

To achieve our objective, we evaluated current contingency plans in place at four SWAs located in CA, TX, NY, and LA. We also reviewed ETA oversight activities in ETA ROs and HQ. We tested to determine if the SWAs have adequate IT contingency plans in place to support critical UI program functions in the event of a disaster or service disruption to the IT supporting the UI program. We selected a sample of 4 SWAs, from a universe of 53, for detailed examination. The sample states were judgmentally selected from a list of SWAs determined to be high-risk based on historical data and professional judgment regarding frequency of disasters declared in each state from FEMA, as shown in the following table:

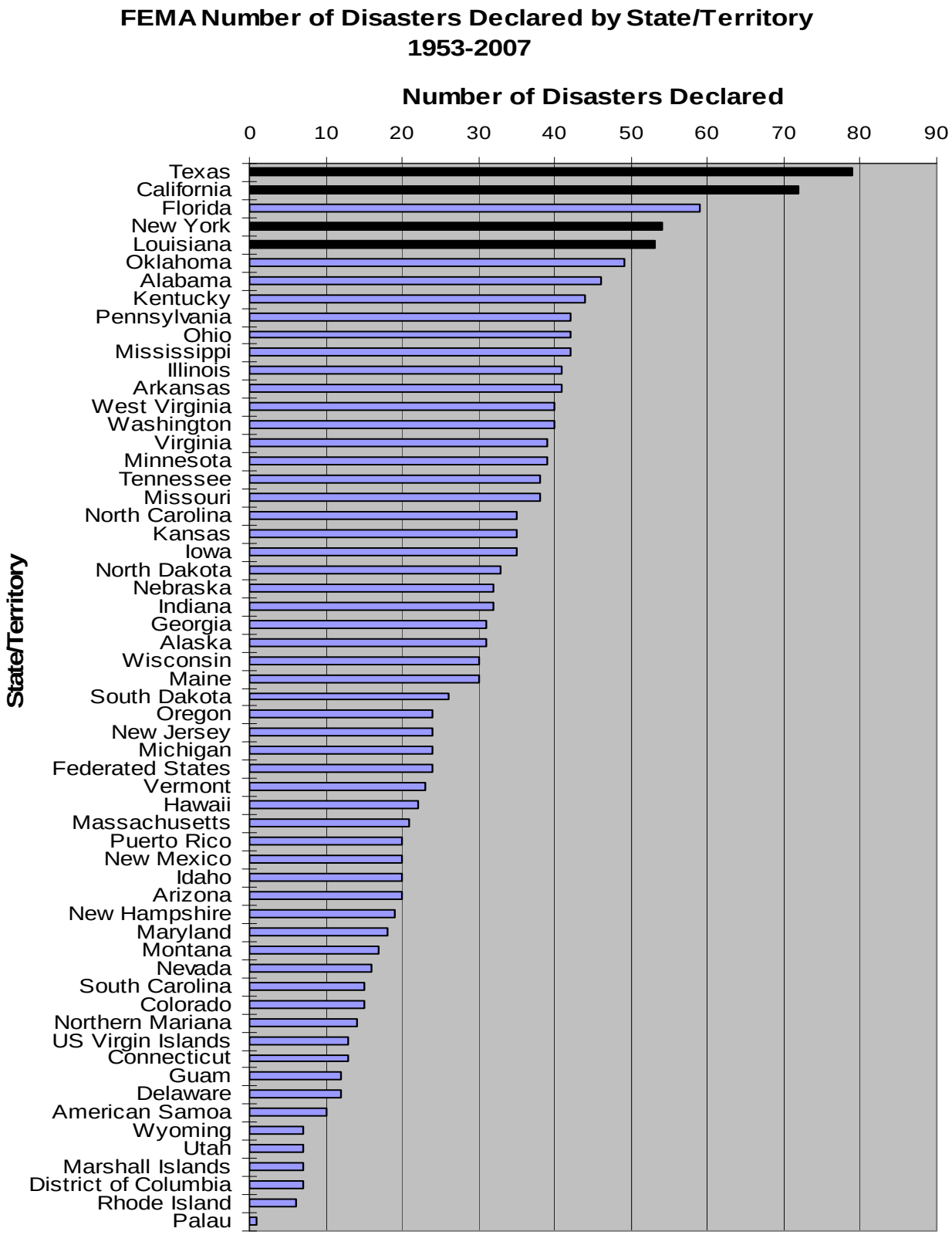

Figure 1: FEMA Number of Disasters Declared by State/Territory.

We assessed the selected sample of SWAs' UI systems' IT contingency-planning controls against NIST SP 800-34 and NIST SP 800-53, Revision 1, *Recommended Security Controls for Federal Information Systems*. These standards are widely recognized as industrial best practices for contingency-planning activities and ETA encourages the SWAs to utilize NIST guidance when implementing information security controls, which include IT contingency planning. Specifically, we assessed the contingency planning (CP) control family including the ten controls in that family, as follows:

- CP-1 Contingency Planning Policy and Procedures
- CP-2 Contingency Plan
- CP-3 Contingency Training
- CP-4 Contingency Plan Testing and Exercises
- CP-5 Contingency Plan Update
- CP-6 Alternate Storage Site
- CP-7 Alternate Processing Site
- CP-8 Telecommunications Services
- CP-9 Information System Backup
- CP-10 Information System Recovery and Reconstitution

Related to the four sampled SWAs, our audit methodology included detailed examinations of SWA IT contingency plans and related documentation. We conducted interviews of personnel and agency officials involved in the implementation and maintenance of the SWAs' IT contingency plans. We briefed and provided a Statement of Facts to SWA officials who generally agreed with the facts presented. We also requested IT contingency plans for the 53 SWAs and reviewed those submitted.

In order to assess ETA's oversight of contingency planning in the SWAs, we conducted interviews and document analysis at the three ETA ROs and the ETA NO. This was designed to assess the grant administration and monitoring activities conducted by ETA in support of the Federal-State UI partnership. We reviewed the Federal-State UI grant agreement and the level of guidance, review, and monitoring done at the Federal level.

Criteria

- ET Handbook No. 336 - *State Quality Assurance Plans*
- UIPL No. 24-04 - *Unemployment Insurance Information Technology Security*
- NIST SP 800-34, *Contingency Planning for Information Technology Systems*
- NIST SP 800-53, Revision-1, *Recommended Security Controls for Federal Information Systems*
- FEMA, *Declared Disasters by Year or State*, as of May 23, 2007.
- OMB A-123, *Management's Responsibility for Internal Control*
- 29 CFR 97.43 (2006)
- 29 CFR 97.50 (2006)
- 20 CFR 602.00 (2008)
- Social Security Act of 1935

- OMB A-130, *Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources*
- Government Auditing Standards, July 2007 Revision

APPENDIX C

ACRONYMS AND ABBREVIATIONS

A-130	Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources
CFR	Code of Federal Regulations
CP	Contingency Planning
DOL	United States Department of Labor
DRP	Disaster Recovery Plans
EDD	Employment Development Department (California)
ETA	Employment and Training Administration
ET	Employment and Training
FEMA	Federal Emergency Management Agency
FY	Fiscal Year
HQ	Headquarters
ISO	Information Security Officer
IT	Information Technology
LDOL	Louisiana Department of Labor
NIST	National Institute of Standards and Technology
NO	National Office
NY DOL	New York Department of Labor
OIG	Office of Inspector General
OMB	Office of Management and Budget
RO	Regional Office
SP	Special Publication
SQSP	State Quality Service Plan
SWA	State Workforce Agency
TWC	Texas Workforce Commission
UI	Unemployment Insurance
UIPL	Unemployment Insurance Program Letter

PAGE WAS INTENTIONALLY LEFT BLANK

APPENDIX D

AGENCY RESPONSE TO REPORT

U.S. Department of Labor

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

SEP 23 2008

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

FROM: BRENT R. ORRELL
Deputy Assistant Secretary

SUBJECT: 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

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.

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.

In the eight years since Y2K, 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. In addition, ETA has continued to take a leadership role with states in promoting strategies to minimize service disruptions, operations, and services to UI beneficiaries. These efforts have included the following:

- Providing states with a compact disk (CD) and an Executive Manager's Paper on current IT Security guidance (2004 – 2006). The CD and paper included:

a. Current National Institute of Standards and Technology (NIST) guidance which included NIST Special Publication (SP) 800-34, *Contingency Planning Guide for Information Technology System;*
b. Office of Management and Budget (OMB) Circulars which included OMB A-130, *Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources;*
c. Federal Information Processing Standards Publications (FIPS Pub);
d. IT Security Federal Laws including *The Federal Information Security Management Act of 2002 (FISMA);* as well as
e. An automated self-assessment application (2005 – 2006) (ASSET) [which followed NIST guidelines] and a manual self-assessment process NIST SP 800-53, *Recommended Security Controls for Federal Information Systems* (2005 – 2007)

- Promoting best practices in disaster recovery and IT contingency planning at national conferences of state UI officials and staff in 2003, 2005, and 2007.

- Developing a report outlining lessons learned from the 2005 hurricanes and containing a set of recommendations concerning disaster preparedness planning including continuity of operations plans. The report "National Unemployment Insurance (UI) Disaster Preparedness Effort" has been completed and is posted to the ETA Web site at: http://www.ows.doleta.gov/unemploy/pdf/prepared.pdf

- Developing, with state staff participation, guidance and procedures for states to include in their respective state-wide continuity of operations plans. The guidance will be completed by the end of 2008.

- Developing a set of protocols, methods, and tools to materially assist a state whose UI claims processing capacity has been rendered temporarily insufficient by a "massive unemployment event" that exceeds its own IT capacity, and therefore, requires interstate assistance. The project will be completed early 2009.

Within available resources, we believe that ETA has provided states with strong guidance and leadership related to IT contingency planning over the past eight years. We also agree that ETA's oversight of state IT contingency planning would be greatly strengthen by implementation of the OIG's recommendations to (1) create a comprehensive framework which includes minimum standards for the implementation of critical control elements for IT disaster recovery and contingency planning, and (2) develop and implement a monitoring and review

process to ensure that SWA IT contingency plans will provide adequate support to critical UI program functions.

However, implementation of these recommendations would be quite resource intensive. While funds were provided for IT contingency planning development, testing, and validation for Y2K, few additional funds have been available for these purposes since that time. We estimate the one-time cost (all states) for plan development at about $17 million, and annual costs of about $5.3 million for independent verification and validation to ensure that plans meet appropriate standards and for state staff to up-date, maintain and test plans annually. Overall funding for UI, like many other programs, has declined in recent years; there has been no inflation adjustment for UI state administration since 1995.

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.