U.S. Department of Labor

Office of Inspector General—Office of Audit

EMPLOYMENT AND TRAINING ADMINISTRATION

UNEMPLOYMENT INSURANCE SYSTEMS' INFORMATION TECHNOLOGY CONTINGENCY PLANS NEED IMPROVEMENT

Date: March 31, 2009
Report Number: 23-09-002-03-315

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

BRIEFLY…

Highlights of Report Number: 23-09-002-03-315, to the Deputy Assistant Secretary for Employment and Training.

WHY READ THE REPORT

After Hurricanes Katrina and Rita devastated the Gulf Coast in 2005, the Employment and Training Administration (ETA) found the states impacted by the hurricanes had large disparities in their level of preparedness in information technology (IT) and operational recovery of the Unemployment Insurance (UI) program.

Based on this, the Assistant Secretary requested the Office of the Inspector General (OIG) conduct an audit, as ETA was interested in knowing which states had viable plans to deal with emergencies. In September 2008, the OIG issued audit report number 23-08-004-03-315. This audit identified that while ETA required state workforce agencies (SWAs) to develop and implement IT contingency plans as a condition of their grant agreements, it did not verify that the plans were developed or tested. Specifically, the audit found three of the four SWAs reviewed may not be able to recover the UI 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 conducted this follow-on audit to assess the IT contingency plans for the UI Tax and Benefit Systems administered by all 53 of the nation's SWAs.

WHY OIG DID THE AUDIT

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

> Has ETA ensured SWA partners establish and maintain required IT contingency plans vital for UI services to continue reliably in the event of a disaster or system interruption?

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/2009/23-09-002-03-315.pdf

March 2009

Unemployment Insurance Systems' Information Technology Contingency Plans Need Improvement

WHAT OIG FOUND

While ETA encouraged SWAs to follow best practices, it did not ensure the SWAs' plans contained best practices, i.e., IT contingency plan elements. Specifically, two SWAs did not have plans and 49 out of the remaining 51 SWAs' plans did not include elements determined to be critical to ensure continued availability of the UI systems.

This situation existed because ETA did not verify SWA plan existence, nor did the SWAs provide ETA with evidentiary verification of their IT contingency plans. In addition, in some cases, the SWAs did not carry out the attestations in their respective grant agreements to maintain plans. While the SWAs annually attest to maintaining disaster preparedness plans, ETA did not conduct specific verification to ensure the validity of the SWAs' self attestations. As a result, ETA relied on inaccurate information from the SWA self-attestations.

WHAT OIG RECOMMENDED

We recommended that the Deputy Assistant Secretary for Employment and Training conduct annual verifications of SWAs' IT contingency plans for existence and reliability using risk-based approaches that consider the SWAs' contingency planning maturity and likelihood of disasters.

ETA generally agreed with OIG's recommendation that ETA's oversight of state IT contingency planning would be greatly strengthened by implementing an annual verification of the SWAs' IT Contingency Plans for existence and reliability.

Table of Contents

PAGE INTENTIONALLY LEFT BLANK

U.S. Department of Labor

Office of Inspector General
Washington, D.C. 20210

March 31, 2009

Assistant Inspector General's Report

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

After Hurricanes Katrina and Rita devastated the Gulf Coast in 2005, the Employment and Training Administration (ETA) found the states impacted by the hurricanes had large disparities in their level of preparedness in information technology (IT) and operational recovery of the Unemployment Insurance (UI) program. Based on this, the Assistant Secretary requested the Office of Inspector General (OIG) conduct an audit, as ETA was interested in knowing which states had viable plans to deal with emergencies.

In September 2008, in response to this request, the OIG issued audit report, No. 23-08-004-03-315. The audit identified that while ETA required state workforce agencies (SWAs) to develop and implement IT contingency plans as a condition of their grant agreements, it did not verify that the plans were developed or tested. Specifically, the audit found three of the four SWAs reviewed may not be able to recover the UI 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.

To assess the viability of IT contingency planning capabilities for Department of Labor's (DOL) UI program nationwide, the OIG performed this follow-on audit which focused on analyzing all SWA documents submitted to OIG as contingency plans for the UI Tax and Benefit Systems (UI Systems).

The audit objective was to answer the following question:

> Has ETA ensured SWA partners establish and maintain required IT contingency plans vital for UI services to continue reliably in the event of a disaster or system interruption?

The audit covered SWAs' contingency plans for the UI Systems in all 53 states and territories having UI programs. To achieve the audit objective, from each SWA, we obtained their UI system IT contingency plans; other documents purported to be IT contingency plans; or notifications that no such plans existed. We assessed the documentation received from 51 SWAs - 2 SWAs (NY and NH) responded that no plan was in place - for the presence of elements needed in establishing and maintaining a viable IT contingency planning capability, according to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, *Contingency Planning for Information Technology Systems*.

RESULTS IN BRIEF

While ETA encouraged SWAs to follow best practices, it did not ensure the SWAs' plans contained best practices, i.e., IT contingency plan elements. Although many SWAs had plans, the plans did not contain all the elements needed to ensure the continued, reliable operation of UI services in the event of a disaster or system interruption. Specifically, 49 out of 51 plans did not include elements determined to be critical to ensure continued availability of the UI systems.

This situation existed because ETA did not verify SWA plan existence, nor did the SWAs provide ETA with evidentiary verification of their IT contingency plans. In addition, in some cases, the SWAs did not carry out the attestations in their respective grant agreements to maintain plans. While the SWAs annually attest to maintaining disaster preparedness plans, ETA did not conduct specific verification to ensure the validity of the SWAs' self attestations. As a result, ETA relied on inaccurate information from the SWA self-attestations.

Without adequate IT contingency plans, critical support services provided by these UI systems may not be available during a disaster or disruption. This may result in the inability to provide benefits to individuals who rely upon UI for their daily sustenance during periods of unemployment.

AGENCY RESPONSE

ETA generally agreed with OIG's recommendation that ETA's oversight of state IT contingency planning would be greatly strengthened by implementing 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. In addition, ETA provided funding estimates needed to implement the OIG recommendation. The response is provided in full in Appendix D.

OIG CONCLUSION

ETA management shares our 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. We feel the implementation of our recommendation will greatly enhance the UI Program and the accountability at the Federal level.

RESULTS AND FINDINGS

Objective — Has ETA ensured SWA partners establish and maintain required IT contingency plans vital for UI services to continue reliably in the event of a disaster or system interruption?

No, ETA did not ensure SWA partners established and maintained required IT contingency plans.

Although ETA took steps to encourage the SWAs to implement IT contingency plans that meet recognized best practices, the agency did not ensure the SWAs had plans in place which included elements vital for UI services to continue in the event of a disaster or system interruption.

Finding — ETA did not ensure SWAs' UI Tax and Benefit Systems' IT Contingency Plans were reliable.

Many SWAs did not maintain IT contingency plans for the UI Systems that follow best practices encouraged by ETA. Best practices are deemed necessary to allow for reliable continued operation of UI services in the event of a disaster or system interruption. ETA has strongly encouraged the SWAs to utilize NIST IT security documents and guidelines, including NIST SP 800-34, since 2004, when it issued UI Program Letter (UIPL) Number 24-04: *Unemployment Insurance Information Technology Security.* We found many UI Systems' IT contingency plans did not contain elements we determined to be critical to reliably implement the contingency plan and maintain the information systems' operations in the event of a disaster or system interruption. While all SWAs are expected to have viable IT contingency plans, it is imperative that those SWAs prone to a higher frequency of disasters make better preparations, starting with maintaining complete and well-documented IT contingency plans. (See Exhibit 1 for a plot of contingency planning maturity and corresponding risk.)

NIST SP 800-34 states: "IT contingency plan development is a critical step in the process of implementing a comprehensive contingency planning program."

NIST also iterates that:

> Information technology (IT) and automated information systems are vital elements in most business processes. Because these IT resources are so essential to an organization's success, it is critical that the services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans and procedures and technical measures that can enable a system to be recovered quickly and effectively following a service disruption or disaster.

UI Systems' Contingency Plans Absent of Critical Elements

We evaluated the submissions from the 51 SWAs for the existence of plan elements based on best practices encouraged for use by ETA and found in NIST SP 800-34. For each of the 17 elements outlined in the chart below, we determined if the element was present in the documentation submitted. (See Exhibit 2 for a complete listing of the 17 elements' presence across the 51 SWAs' plans.) We focused on the plans' inclusion of the following 4 elements which, in our judgment, are critical to ensuring a plan is actionable based on their role in the plan: Line of Succession, Detailed Recovery Procedures, Reconstitution Phase Procedures, and Contact Information of Contingency Plan Teams.

List of 17 Plan Elements

--	Purpose	--	Damage Assessment Procedures
--	Applicability	--	**Detailed Recovery Procedures***
--	Scope	--	**Reconstitution Phase Procedures***
--	Record of Changes	--	**Contact information of CP teams***
--	System Description	--	Vendor contact information
--	**Line of Succession***	--	Checklists for system recovery
--	Responsibilities	--	Equip/System requirements lists
--	Activation Criteria	--	Description/Direction to alternative sites
--	Documented Notification Procedures		

* These critical elements are discussed further in the report, including examples of problems found.

Absence of the Four Critical Elements - We found many UI Systems' IT contingency plans did not contain all of the four critical elements to reliably implement the contingency plan and maintain the information systems' operations in the event of a disaster or system interruption. Specifically, of the 51 SWAs that provided planning documents, 49 out of 51 did not contain all 4 critical elements. Furthermore, 32 of the 51 plans were lacking in all 4 critical areas. Only two SWAs, Massachusetts and South Dakota, had plans containing all four critical elements. Exhibit 2 shows the distribution of the 17 elements throughout all 51 SWAs.

Although many SWAs did not have plans with all the critical elements, there were SWAs that showed signs of attempting to put forth a qualified plan in accordance with the best practices encouraged by ETA. For example, 3 SWAs had plans with 75 percent of the 17 elements (13 or more). Exhibit 3 provides a bar graph with a visual representation of the existence of the critical planning elements across the 51 SWAs.

With the understanding these four critical elements should be in place for a contingency plan to be viable during a time of disaster, the following assessment results reveal the magnitude of the SWAs' problems across the four critical areas.

Line of Succession

The line, or order, of succession defines who assumes responsibility for IT contingency plan execution in the event the highest authority is unavailable or unable to do so. Twenty-nine of 51 SWA submissions did not include a line of succession. Twelve SWAs included a partial line of succession; they were missing a full description.

The severity of this condition is exacerbated when related to the frequency of disasters declared in each state. The Federal Emergency Management Agency (FEMA) tracks and reports the frequency of disasters declared in each state annually. FEMA ranks the states by total number of disasters, which we used for purposes of this audit. (See Appendix B: Methodology, for complete ranking.) Of FEMA's top 25 highest-risk SWAs: 11 had contingency plans that were missing a line of succession; 1 responded it did not

have a contingency plan; and 7 had contingency plans that included a partial line of succession. This left only 6 of the highest-risk SWAs with plans that included this critical element.

Examples of the types of problems related to this critical element include:

- The third highest-risk SWA's plan omitted the line of succession element. Other documentation from this SWA contained team contact information with team leader alternatives but not a fully detailed line of succession.
- The sixth highest-risk SWA's plan had not been updated since 2004 and it did not contain any line of succession information.
- The seventh highest-risk SWA submitted a document which contained an appendix with contact information, and organizational charts, but did not address the line of succession that would be effective during an emergency.

NIST SP 800-34 states:

> The order of succession will define who assumes responsibility for contingency plan execution in the event that the highest authority (usually starting with the Chief Information Officer [CIO]) is unavailable or unable to do so.

NIST SP 800-34 also iterates that:

> The order of succession identifies personnel responsible to assume authority for executing the contingency plan in the event the designated person is unavailable or unable to do so.

The line of succession is a critical element of the contingency plan, as it helps the SWA avoid confusion during a disaster or disruption by specifying who is responsible for the plan in the event personnel are incapacitated. As NIST SP 800-34 notes:

> The order of succession will define who assumes responsibility … if the CIO has been injured or killed, the Deputy CIO will assume plan responsibility; if the CIO and Deputy CIO have been injured or killed, the Information Systems Security Manager will assume plan responsibility.

Detailed Recovery Procedures

Detailed recovery procedures are critical to allow personnel to restore the UI System or system components in an approved, step-by-step, manner. Twenty-two of 51 SWA submissions did not have detailed recovery procedures for their respective UI systems. Another 20 SWAs' plans had some recovery procedures, but were missing the full details needed to timely resume operations.

Of FEMA's top 25 highest-risk SWAs: 9 had contingency plans that were missing recovery procedures; 1 responded it did not have a contingency plan, and 9 had contingency plans containing only partial procedures to recover the respective UI Systems. This left only 6 of the highest-risk SWAs with plans that included this critical element.

The following examples highlight the concern further:

- The sixth highest-risk SWA did not have specific recovery procedures relating to its client server operations, i.e., its Windows server recovery procedures included a list of system attributes such as Operating System, Host Name, and amount of memory; however, no written instructions detailing specific recovery steps for the technology listed in the procedure was included.
- The ninth highest-risk SWA submitted eight documents, none of which contained detailed recovery procedures. One document included high-level descriptions of recovery steps, and another contained a reference to a detailed recovery procedures appendix that was not part of the submission package.
- The fourteenth highest-risk SWA submitted three documents, none of which qualified as an IT contingency plan or contained detailed recovery procedures. One document was a business analysis from 2004; another document was a brochure for emergency teams of all types and not relevant to IT; and the third document was a traditional COOP which did not contain the necessary detailed recovery procedures to ensure UI system availability.

Recovery procedures are a critical element of the contingency plan. As NIST 800-34 notes, best practices include:

> Recovery phase activities that focus on contingency measures to execute temporary IT processing capabilities, repair damage to the original system, and restore operational capabilities at the original or new facility. At the completion of the Recovery Phase, the IT system will be operational and performing the functions designated in the plan.

Reconstitution Phase Procedures

Reconstitution phase procedures allow an SWA to return to normal operations of providing UI benefits after the disaster or disruption has been mitigated. Forty-three of 51 SWA submissions did not include reconstitution phase procedures. Five SWAs had some reconstitution procedures, but were missing several necessary procedures that allow for timely system recovery.

Of FEMA's top 25 highest-risk SWAs: 21 had contingency plans that were missing reconstitution phase procedures; 1 responded it did not have a contingency plan, and 2 had contingency plans containing only partial reconstitution information. This left only 1 of the highest-risk SWAs with plans that included this critical element.

The following examples demonstrate the SWAs' vulnerability should a disaster occur:

- Four of the five highest-risk SWAs did not have plans providing details by which an individual could perform reconstitution phase procedures.
- The third highest-risk SWA submitted two documents - one contained reconstitution procedures at only a very high level and the other provided only a narrative description of what reconstitution procedures would be necessary.
- The sixth highest-risk SWA provided documentation that specifically outlined the need to further develop a detailed reconstitution plan as well as the requirements of this document.

Reconstitution phase procedures are an essential part of an IT contingency plan as they allow an SWA to return to normal operations of providing UI benefits after the disaster or disruption has been mitigated. An SWA cannot continue operations at an alternate site for an indefinite period and, without plans to restore normal operations, the SWA may become unable to function. As NIST SP 800-34 notes:

> In the Reconstitution Phase, recovery activities are terminated and normal operations are transferred back to the organization's facility. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new facility to support system processing requirements.

Contact Information of Contingency Plan Teams

Contact information is critical because personnel involved in contingency plan activation must be able to be notified when plan activation occurs. Twenty-one of 51 SWA submissions did not list any contact information. Eighteen SWAs list some contact information, but were missing complete details to contact the contingency plan teams.

Of FEMA's top 25 highest-risk SWAs: 4 had contingency plans that were missing contact information, 1 responded it did not have a contingency plan, and 11 had plans containing only partial contact details. This left only nine of the highest-risk SWAs with plans that included this critical element.

The following examples bring this problem into even greater focus:

- The third highest-risk SWA's plan listed five departments, the contact and one phone number. It did not include alternate numbers or manners of communicating with these key contacts.
- The seventh highest-risk SWA submitted three documents, none of which included adequate contact information — one was a four-page document containing narrative descriptions of what recovery efforts would occur and contact names without including phone numbers for management personnel and personnel at the SWA field offices.

- The fifteenth highest-risk SWA submitted a narrative description of its UI functions and staffing needs during a contingency, but provided no contact information.

Contact information for the contingency plan team is a critical element of the contingency plan. As NIST 800-34 notes:

> Personnel to be notified should be clearly identified in the contact lists appended to the plan. This list should identify personnel by their team position, name, and contact information (e.g., home, work, and pager numbers, e-mail addresses, and home addresses).
>
> The contact lists generally contain sensitive information and should be marked and stored appropriately and disseminated only to those requiring access. The lists should be dated and frequently reviewed to ensure names, positions, and contact information are up to date.

– – – – – – – – –

The SWA attestations of a disaster recovery capability present risks to the Federal/State UI program and operations because they may misrepresent the SWAs' actual level of preparedness to ETA management should a disaster or system interruption occur. These risks need to be considered by ETA in assessing how best to improve the SWAs' contingency planning efforts. ETA is responsible to ensure the Federal funding provided to the SWAs via the annual UI funding agreements is expended in accordance with the grant agreement that require disaster recovery capability. For agencies to consider and manage risk, the Office of Management and Budget (OMB) issued Circular A-123, *Management's Responsibility for Internal Control, Introduction*, (A-123), which 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.

A-123 further identifies that managers should manage risk when implementing and monitoring internal controls:

> Internal control guarantees neither the success of agency programs, nor the absence of waste, fraud, and mismanagement, but is a means of managing the risk associated with Federal programs and operations. Managers should define the control environment (e.g., programs, operations, or financial reporting) and then perform risk assessments to

> identify the most significant areas within that environment in which to place or enhance internal control.

We found many plans lacking substance in their content because ETA did not verify SWA plan existence nor did the SWAs provide ETA with evidentiary verification of their IT contingency plans. Furthermore, two SWAs did not even have plans, yet they attested to ETA that plans existed by signing their annual funding agreements which contained this assurance of a disaster recovery capability. ETA provides administrative funding to the SWAs via annual UI Funding agreements (i.e. grant agreements), which contain requirements of the SWAs. Each SWA must attest to meeting the requirements outlined in the assurance statements annually, via signature, in order to receive Federal grant funding for the administration of the SWA's UI program.

In preparation for the Year 2000 (Y2K), ETA required evidence from each SWA that the UI Systems' IT contingency 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 SWAs as a part of their UI administrative grant agreement that they have plans in place. ETA has taken a leadership role with the SWAs in promoting strategies to minimize service disruptions, operations, and services to UI beneficiaries. However, without requiring specific verification and validation of the plans, ETA's leadership activities have not been entirely effective. By not requiring the SWAs to submit verification of their IT contingency plans, ETA could not ensure SWAs' plans existed or contained all critical elements. The focus on verification of IT contingency plans that existed eight years ago has waned in the interim, which has lead to our identified condition of no ETA verification of IT contingency plan existence. The result was ETA relying on inaccurate information from SWA self-attestations.

In September 2008 we issued audit report no. 23-08-004-03-315 containing recommendations for the Assistant Secretary for Employment and Training to 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. Since our issuance of the report, ETA has developed plans to implement the report's recommendations, which we consider to have been resolved. ETA has not, however, laid out a specific plan to conduct risk-based verification of IT contingency plan existence for the UI systems.

Without adequate IT contingency plans for the UI Systems, the critical services provided by these systems may not be available. A disaster or disruption that strikes an SWA's UI System could potentially result in the inability to provide benefits to individuals who rely upon it for their daily sustenance.

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.

With the February 2009 national unemployment rate at 8.1 percent — 12.5 million individuals, the highest level in 26 years — the importance of IT contingency planning by SWAs to provide uninterrupted UI benefits has been brought to the forefront. A disaster or disruption that strikes an SWA's UI System could potentially result in the SWA's inability to provide benefits to individuals who depend upon it during an economic hardship. If even a small percentage of unemployed individuals were unable to access their UI benefits, the consequences could put that person and/or their family in dire straits.

In summary, reliable SWA contingency plans for the UI program become even more important in a time of high unemployment because of the high resource demands on the UI program. An SWA's UI System must not only be able to survive a disaster or disruption but also a surge in usage. Recently, several SWAs experienced problems ranging from website outages to phone line overloads due to heavy usage. If this scenario were to occur for a prolonged period, and an SWA did not have a reliable IT contingency plan in place to compensate, benefits may be interrupted as well.

Recommendation

We recommend the Deputy Assistant Secretary for Employment and Training:

1. Conduct annual verification of SWAs' IT contingency plans for existence and reliability using risk-based approaches that consider the SWAs' contingency planning maturity and likelihood of disasters.

Elliot P. Lewis

PAGE INTENTIONALLY LEFT BLANK

Exhibits

PAGE INTENTIONALLY LEFT BLANK

Exhibit 1

Contingency Plan Maturity and Corresponding Risk

For each state, the scatter plot displays the risk of a disaster occurring in that state (based on frequency of disasters declared) along with the corresponding percentage of IT contingency plan elements present in the SWA submissions. The higher the percentage of elements documented reflects the greater the plan's maturity and reliability. The data includes plots for each of the 53 UI jurisdictions, including the two SWAs (NY and NH) that represented they did not have a contingency plan.

PAGE INTENTIONALLY LEFT BLANK

Exhibit 2

Presence of 17 IT Contingency Plan Elements in UI Systems' Plans [1]

	State Workforce Authorities																								
Elements	**AL**	**AK**	**AZ**	**AR**	**CA**	**CO**	**CT**	**DC**	**DE**	**FL**	**GA**	**HI**	**ID**	**IL**	**IN**	**IA**	**KS**	**KY**	**LA**	**ME**	**MD**	**MA**	**MI**	**MN**	**MS**	**MO**
Purpose										X				X						X	X	X			X	X
Applicability										X				X						X	X	X			X	X
Scope										X				X						X	X	X			X	X
Record of Changes																						X			X	
System Description														X			X					X			X	X
Line of Succession					X	X										X						X				X
Responsibilities					X	X				X				X		X			X		X	X			X	X
Activation Criteria					X					X				X		X					X	X				
Documented Notification Procedures					X	X				X				X					X		X	X			X	
Damage Assessment Procedures					X	X				X						X			X			X			X	
Detailed Recovery Procedures										X				X								X				
Reconstitution Phase Procedures																						X				
Contact information of CP teams	X													X		X						X			X	X
Vendor contact information	X					X				X				X												X
Checklists for system recovery	X																									X
Equip/System requirements lists	X				X					X				X		X										X
Description/Direction to alternative sites		X														X			X		X					

[1] An X mark in the chart indicates the element was present in the SWA's planning documents. For purposes of this analysis, a plan that contained parts or the element, i.e. received "partial" in the analysis, was not given an X for present, as the element was found deficient in some manner.

PAGE INTENTIONALLY LEFT BLANK

Exhibit 2

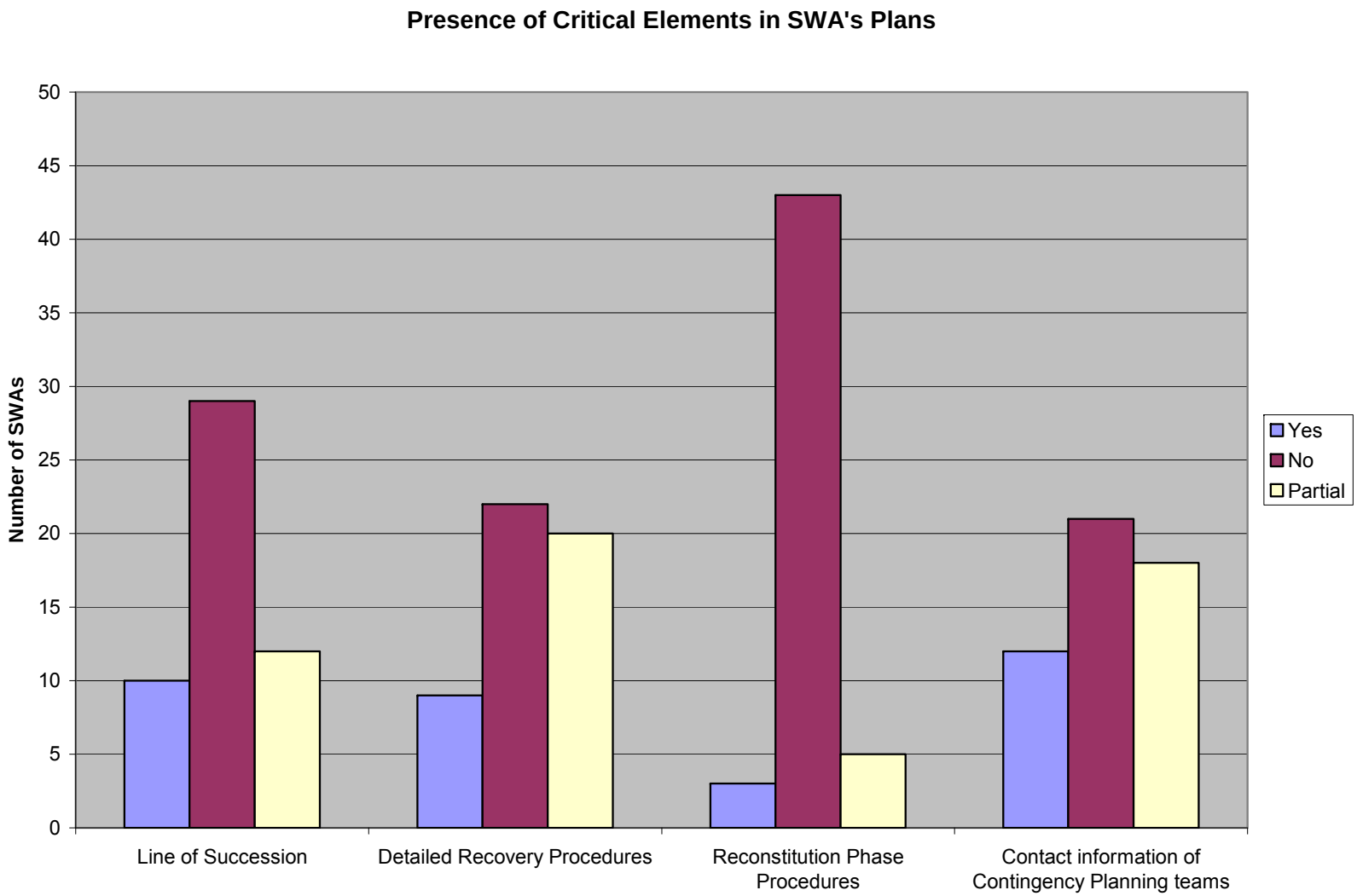
Presence of 17 IT Contingency Plan Elements in UI Systems' Plans (continued)

	State Workforce Authorities																							
Elements	**MT**	**NE**	**NV**	**NJ**	**NM**	**NC**	**ND**	**OH**	**OK**	**OR**	**PA**	**PR**	**RI**	**SC**	**SD**	**TN**	**TX**	**UT**	**VA**	**VI**	**VT**	**WA**	**WV**	**WI**	**WY**
Purpose		X	X		X	X			X						X		X		X			X			
Applicability			X			X			X								X					X	X		
Scope		X	X			X									X	X			X			X			
Record of Changes			X												X										
System Description	X		X						X									X							
Line of Succession			X								X				X				X			X			
Responsibilities			X		X	X	X		X						X	X	X								
Activation Criteria			X			X					X				X		X	X	X			X	X		
Documented Notification Procedures			X			X			X		X				X	X	X	X					X		
Damage Assessment Procedures			X			X			X						X										
Detailed Recovery Procedures			X			X			X						X				X				X		
Reconstitution Phase Procedures						X									X										
Contact information of CP teams			X				X	X	X						X								X		
Vendor contact information			X			X	X		X				X					X					X		
Checklists for system recovery			X			X		X									X							X	
Equip/System requirements lists			X			X	X	X	X		X		X			X							X		
Description/Direction to alternative sites						X			X				X											X	

PAGE INTENTIONALLY LEFT BLANK

Exhibit 3

Presence of Critical Elements in SWAs' Plans



PAGE INTENTIONALLY LEFT BLANK

Appendices

PAGE INTENTIONALLY LEFT BLANK

Appendix A

Background

UI Program 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.

ETA Oversight of UI Program

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.

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 contains an assurance of disaster-recovery capability.

The "Assurance of Disaster Recovery Capability" (Assurance H) is explained in more detail in Employment and Training Handbook No. 336, 18th Edition, Unemployment Insurance State Quality Service Plan (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.

ETA has strongly encouraged the SWAs to utilize NIST IT security documents and guidelines, including NIST SP 800-34, since 2004, when it issued UIPL Number 24-04: Unemployment Insurance Information Technology Security. This guidance provided the SWAs with specific information on the NIST IT security guidelines and a software tool to conduct a security self-assessment of UI computer systems. 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.

Audit Background

After Hurricanes Katrina and Rita devastated the Gulf Coast in 2005, ETA found the states impacted by the hurricanes had large disparities in their level of preparedness in IT and operational recovery of the UI program. Based on this, the Assistant Secretary requested the OIG conduct an audit, as ETA was interested in knowing which states had viable plans to deal with emergencies. In response to this request, the OIG performed a follow-on audit. The previous audit (OIG audit report no. 23-08-004-03-315) assessed the level of preparedness at four high-risk SWAs and ETA's related monitoring and oversight of the SWAs' IT contingency planning efforts. This report is available for view on the OIG's public website at: http://www.oig.dol.gov/public/reports/oa/2008/23-08-004-03-315.pdf.

The previous audit included OIG judgmentally selecting a sample of four SWAs, from a universe of 53, for detailed examination. The sampled SWAs were selected from a list of states determined to be high-risk based on historical data regarding frequency of disasters declared in each state from FEMA.

Pursuant to the audit, ETA requested all 53 UI Systems' IT contingency plans for the OIG's review. The auditors received 51 plans, with 2 SWAs responding that they did not have a plan at the time of the request. Because of time and scope limitations, the audit focused on the four high-risk SWAs where the auditors performed on-site fieldwork to assess the SWAs' UI systems' IT contingency planning controls.

The audit concluded that ETA required 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. The audit showed that three of four SWAs audited may not be able to recover the UI 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. The OIG recommended 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.

In order to get a full picture of the degree of reliability and maturity of contingency planning across all UI jurisdictions, the OIG performed the follow-on audit to assess all UI jurisdictions' IT contingency plans.

PAGE INTENTIONALLY LEFT BLANK

Appendix B

Objective, Scope, Methodology, and Criteria

Objective

Our audit was designed with the following overall objective:

> Has ETA ensured SWA partners establish and maintain required IT contingency plans vital for UI services to continue reliably in the event of a disaster or system interruption?

Scope

Our audit scope comprised an audit universe of 53 UI jurisdictions, including 50 states, the District of Columbia, Virgin Islands, and Puerto Rico. Of the 53 UI jurisdictions, 51 SWAs provided copies of their IT contingency plans or other documents purported to be IT contingency plans for our review. Two jurisdictions, New York and New Hampshire, notified us that they did not have IT contingency plans at the time of our request.

A performance audit includes gaining an understanding of internal controls considered significant to the audit objectives and testing compliance with significant laws, regulations, and other compliance requirements. In order to plan the audit, we considered whether internal controls significant to the audit were properly designed and placed in operation. However, we did not assess overall internal controls.

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

In FY 2008, the OIG conducted an audit to determine if ETA provided 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. The methodology for achieving that audit included examining 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 had 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 the 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.

For the current, follow-on audit, we assessed the quality of the responses received from the 51 SWAs by conducting an examination of the elements that comprise IT contingency plan development according to NIST Special Publication 800-34, Contingency Planning for Information Technology Systems.

In planning and performing the audit, we considered ETA's internal controls as identified in the previous audit, which we updated during this follow-on audit. Specifically, in order to assess ETA's oversight of contingency planning in the SWAs, we conducted interviews and documentation analysis at the ETA National Office 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. Our review of ETA's controls lead us to conclude that while the SWAs annually attest to maintaining disaster preparedness plans, ETA did not conduct specific verification to ensure the validity of the SWAs' self attestations.

Our current audit methodology included a detailed assessment of information that was submitted by the 51 SWAs. We performed a review of documentary evidence at OIG offices using an analytical tool consisting of a spreadsheet designed to segregate and categorize the information received. Data reliability tests were not performed as this was a performance audit that analyzed the content of contingency plans. The nature of the audit did not require any reliance on the validity of system generated data.

Responses submitted from the SWAs consisted of bundled information containing one or more plan(s) or related document(s). Each of those documents were analyzed individually by the auditors using a separate spreadsheet for each plan for the purpose of determining which elements are present in the different plans. For each SWA, a conclusion was made as a whole incorporating all factors being assessed.

The necessity to assess multiple plans was due to overlap in the definition of what constitutes an IT contingency plan. According to NIST SP 800-34, there are several types of plans that are related to IT contingency planning.

> IT contingency planning represents a broad scope of activities designed to sustain and recover critical IT services following an emergency. IT contingency planning fits into a much broader emergency preparedness environment that includes organizational and business process continuity and recovery planning. Ultimately, an organization would use a suite of plans to properly prepare response, recovery, and continuity activities for disruptions affecting the organization's IT systems, business processes, and the facility. Because there is an inherent relationship between an IT system and the business process it supports, there should be coordination between each plan during development and updates to ensure that recovery strategies and supporting resources neither negate each other nor duplicate efforts.

> 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.

NIST SP 800-34 provides a description as a common basis of understanding for these different types of plans. However, because of the lack of standard definitions for these types of plans, the scope of actual plans developed by organizations may vary from the descriptions as defined by NIST SP 800-34. As such, our analysis took into consideration all information submitted by the SWAs in determining which elements were incorporated in the information provided.

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."

Consequently, the information submitted by the UI jurisdictions was only considered to the extent that it related to information technology. If a document was submitted that contained an element, such as a description of the scope, it needed to address the scope as it pertained to computer systems, as opposed to something like building security.

Specifically, the analysis was based on section four of NIST SP 800-34, which deals with IT contingency plan development. This section serves as a guide in deriving a plan format that incorporates elements of contingency planning. This guide identifies five main components of the contingency plan. Those components are the (1) supporting information, (2) notification/activation phase, (3) recovery phase, (4) reconstitution phase, and (5) the plan appendices. We further identified 17 plan elements within the 5 main components to assess. We placed special emphasis on the existence of four elements, in our judgment, that are critical to ensuring a plan is actionable. These elements include:

- Line of Succession,
- Detailed Recovery Procedures,
- Contact information of Contingency Planning (CP) Teams, and
- Reconstitution Phase Procedures.

The 17 plan elements within the five main components of the contingency plan are as follows:

- Supporting Information
  1. Purpose
  2. Applicability
  3. Scope
  4. Record of Changes
  5. System Description

6. Line of Succession
7. Responsibilities

- Notification Phase
  8. Activation Criteria
  9. Documented Notification Procedures
  10. Damage Assessment
- Recovery Phase
  11. Detailed Recovery Procedures

- Reconstitution Phase
  12. Reconstitution Phase Procedures

- Plan Appendices
  13. Contact Information of CP Teams
  14. Vendor Contact Information
  15. Checklist for System Recovery
  16. Equipment/System Requirements Lists
  17. Description/Direction to Alternative Sites

We analyzed the SWAs' submissions to determine the extent to which they included the 17 plan elements, and whether the documentation represented an IT plan in and of itself. We tabulated our conclusions in terms of whether the plan included, did not include, or partially included these elements.

We did not observe SWA personnel activities, perform operational security tests, or interview management or staff involved in the implementation and management of the disaster recovery capability at the SWAs. We based our conclusions solely on evidence provided by the SWAs.

We determined the risk of each SWA UI system based on historical data and professional judgment regarding frequency of disasters declared in each state from FEMA, as shown in the following table:

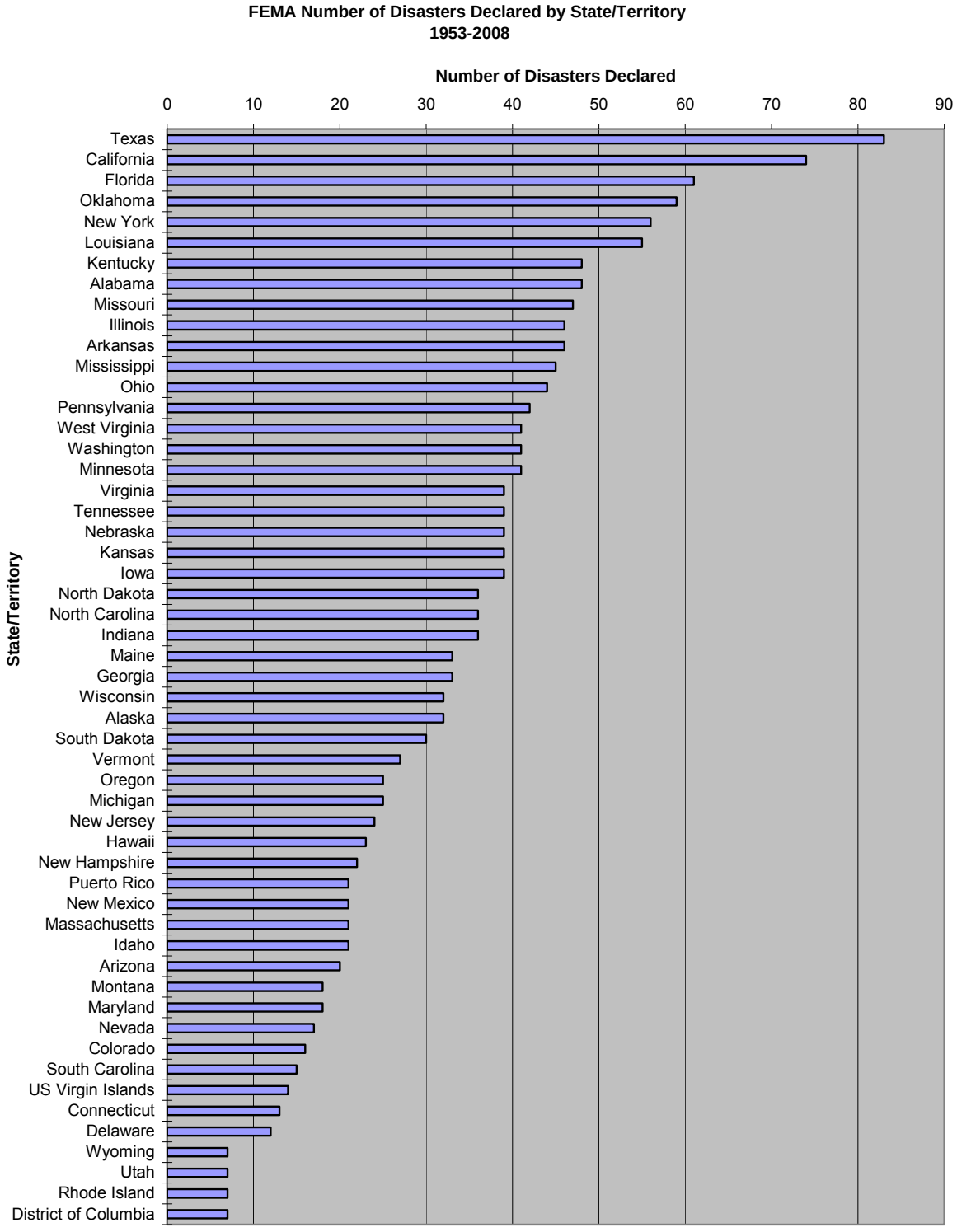


Figure 1: Based on FEMA Number of Disasters Declared by State/Territory.

Criteria

- Social Security Act of 1935
- 20 CFR 602.00 (2008)
- UI Annual Funding Agreement
- ETA Handbook No. 336: UI SQSP Handbook
- NIST SP 800-34, Contingency Planning for Information Technology Systems
- OMB A-123: Management's Responsibility for Internal Control
- FEMA, Declared Disasters by Year or State, as of December 15, 2008
- UIPL Number 24-04: UI IT Security

Appendix C

Acronyms and Abbreviations

A-123	OMB Circular A-123, Management's Responsibility for Internal Control, Introduction
CFR	Code of Federal Regulations
CIO	Chief Information Officer
COOP	Continuity of Operations Plan
CP	Contingency Planning
DOL	United States Department of Labor
DRP	Disaster Recovery Plans
ETA	Employment and Training Administration
FEMA	Federal Emergency Management Agency
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
SP	Special Publication
SQSP	State Quality Service Plan
SWA	State Workforce Agency
UI	Unemployment Insurance
UIPL	Unemployment Insurance Program Letter
UI Systems	UI Tax and Benefit Systems
Y2K	Year 2000

PAGE INTENTIONALLY LEFT BLANK

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.

TO REPORT FRAUD, WASTE, OR ABUSE, PLEASE CONTACT:

Online:	http://www.oig.dol.gov/hotlineform.htm
Email:	hotline@oig.dol.gov
Telephone:	1-800-347-3756 202-693-6999
Fax:	202-693-7020
Address:	Office of Inspector General U.S. Department of Labor 200 Constitution Avenue, N.W. Room S-5506 Washington, D.C. 20210