EMPLOYMENT AND TRAINING ADMINISTRATION ADVISORY SYSTEM U.S. DEPARTMENT OF LABOR Washington, D.C. 20210	CLASSIFICATION UI
	CORRESPONDENCE SYMBOL OWS/DPM
	DATE June 4, 2009

ADVISORY: UNEMPLOYMENT INSURANCE PROGRAM LETTER NO. 26-09

TO: STATE WORKFORCE AGENCIES

FROM: DOUGLAS F. SMALL
Deputy Assistant Secretary

SUBJECT: Unemployment Insurance (UI) Fiscal Year (FY) 2009 Supplemental Funding Opportunities to Improve UI Information Technology (IT) Contingency Plans and UI IT Security

1. **Purpose.** To notify State Workforce Agencies (SWAs) of the availability of FY 2009 UI funds to: 1) develop or update UI IT Contingency Plans, including obtaining an Independent Verification and Validation (IV&V), and 2) improve UI IT Security.

2. **References.** ET Handbook No. 336, 18th Edition, the Unemployment Insurance State Quality Service Planning and Reporting Guidelines, Chapter 1, Section VI, C. Supplemental Budget Request (SBR) and Chapter 1, Section VII, H. Assurance of Disaster Recovery; Unemployment Insurance Program Letter (UIPL) 24-04, Change 3, Unemployment Insurance Information Technology Security – Additional Information; Office of Inspector General (OIG) Report No. 23-08-004-03-315[1] and OIG Report No. 23-09-001-03-315[2].

3. **Background.** As SWAs operate their UI programs, there is a continual need to:

   a. Monitor and improve the security of their IT systems;
   b. Address the findings of internal security assessments; and
   c. Address the findings of external audits by third-party entities.

   Periodically, the Employment and Training Administration (ETA) provides up-to-date security guidance to assist SWAs in monitoring and improving their UI IT Security and encourages SWAs to conduct UI IT security self-assessments to identify areas of weakness.

   In FY 2008, the OIG conducted two audits of the SWAs' UI IT contingency plans to

1 The link to this report is http://www.oig.dol.gov/public/reports/oa/2008/23-08-004-03-315.pdf

2 The link to this report is http://www.oig.dol.gov/public/reports/oa/2009/23-09-002-03-315.pdf

RESCISSIONS None	EXPIRATION DATE June 4, 2010

determine if SWAs were prepared to minimize the impact of a disaster or other situations that may disrupt normal UI program operations. The OIG utilized National Institute of Standards and Technology (NIST) standards in evaluating the plans. The summary of findings contained in the OIG audits (OIG Report No. 23-08-004-03-315 issued on September 29, 2008, and OIG Report No. 23-09-001-03-315 issued on March 31, 2009) stated that:

a. SWAs lack IT Contingency Plans that would ensure adequate disaster-response capability as identified in the NIST Special Publication (SP) 800-34, *Contingency Planning for Information Technology Systems*;

b. ETA has not adequately fulfilled its leadership responsibilities in providing oversight and targeted guidance to the SWAs regarding ETA's expectations of an IT disaster-recovery capability; and

c. ETA should conduct an annual verification of SWAs' UI IT contingency plans for existence and reliability.

4. **Fiscal Year 2009 Funding.** ETA will award selected SWAs funding to improve their UI IT Contingency Plans and UI IT Security. Funding to improve UI IT Contingency Plans will be given first priority.

   a. **UI IT Contingency Plan:** SWAs may submit a SBR to develop or update their UI IT Contingency Plans using the guidelines provided in NIST SP 800-34. Attachment 1 provides the NIST SP 800-34 template for an IT Contingency Plan. SWAs can use this template as a guideline to develop a plan or update an existing plan. The SBR should include funds for an IV&V of the completed UI IT Contingency Plan, based on guidelines provided in the NIST SP 800-34, and assurance that a copy of the IV&V certification report will be provided to the Regional Office (RO).

   A state's UI IT Contingency Plan SBR must address all the key elements deemed as missing in its Plan by the OIG Audit and describe the proposed corrections/solutions. See Attachment 3, Extract from the OIG Audit Report: Presence of 17 IT Contingency Plan Elements in UI Systems' Plans, for a complete listing. Each SWA may submit one UI IT Contingency Plan SBR, which includes proposed improvement to their UI Contingency Plan, as well as an IV&V of the UI Contingency Plan, for consideration. The SBR must include the total cost of the project; however, Federal funding for the SBR will not exceed $150,000. By submitting the proposal, the SWA agrees to provide any additional funds needed to complete the project.

b. **UI IT Security**: SWAs may submit multiple UI IT Security SBRs addressing UI IT security weaknesses that have been identified by recent IT security audits (performed within the last 3 years from the date of this UIPL) or by a SWA's UI IT security self-assessment that complies with the NIST IT security guidelines found in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems* and NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems.* Attachment 2 provides a Sample Security Assessment Reporting Form from NIST SP 800-53A, which may be used to perform an IT security assessment of the SWA's UI IT system or associated UI IT segments (e.g., Web Site, Tax System, Benefits System, etc.).

Each UI IT Security SBR must also address the proposed remediation for each security weakness identified and include the total cost to remediate the weakness described; however, Federal funding for each SBR will not exceed $100,000. By submitting the proposal, the SWA agrees to provide any additional funds needed to complete the project.

5. Information Required.

- UI IT Contingency Plan SBRs must include:
  - a list of the key elements identified by the OIG audits as missing in the current plan;
  - a description of how the proposed remediation addresses these elements;
  - plans for an IV & V of the completed UI IT Contingency Plan based on guidelines provided in the NIST SP 800-34; and
  - assurance that the IV & V will be provided to the Regional Office.

- UI IT Security SBRs must include:
  - a copy of the complete audit report or security assessment (performed within the last 3 years from the date of this UIPL), which outlines the finding(s) related to the UI IT Security weakness being addressed; and
  - a description of how the proposed remediation addresses this weakness.

All SBR submissions must include the following:

- A projected cost breakout (including any additional costs to be covered by the SWA);
- A detailed cost proposal, product description and specifications for any equipment, hardware, software, etc., to be purchased to address a security weakness;
- If contract staff is requested, the position description, estimated contract staff hours, anticipated costs per hour, and total staffing cost;
- If a SWA staff position is backfilled, the position description, estimated staff hours, anticipated costs per hour, and total staffing cost for the backfilled position;
- An estimated timeline for the project, i.e. the number of days, weeks or months, or the estimated start and end dates of each identified phase of the project; and
- The name, address, telephone number, and e-mail address of a SWA contact person.

6. **Confidentiality of Information.** Under the provisions of the Freedom of Information Act (FOIA), records received by a Federal agency can be requested by the public. ETA recognizes the SWAs' concern related to disclosure of information about UI IT contingency planning weaknesses that are submitted to support their SBRs. ETA will protect the SWAs' data to the greatest extent permitted by law by invoking one or more of the nine FOIA exemptions that protect sensitive data. SWAs should specifically request that security weakness information provided to support an SBR be kept strictly confidential. Documents submitted in which the SWA requests confidentiality should be clearly marked as "confidential."

   Should ETA receive a FOIA request related to the security material submitted as part of this SBR, it will notify the relevant SWA, seek its views on any potential disclosure, and act in consultation with the affected SWA.

7. **Evaluation Criteria.** A panel will score the proposals and determine the SBR awards based on the following criteria for each category:

   - **UI IT Contingency Plan:**

     - SWAs must address all the missing key elements in their UI IT Contingency Plan as reported by the OIG in Attachment 3;
     - SWAs must utilize the guidelines provided in NIST SP 800-34 to develop the UI IT Contingency Plan;
     - The UI IT Contingency Plan IV&V must use the guidelines provided in the NIST SP 800-34 to evaluate and certify the UI IT Contingency Plan; and
     - SWAs must ensure to submit a copy of the IV&V certification report to their respective RO upon completion.

   - **UI IT Security:**

     Priority will be given to:
     - SWA proposals that adequately addresses the specific security weaknesses documented in a recently-conducted security audit or security assessment report;
     - SWA proposals that address findings with the greatest risk;
     - SWAs that provide assurance that future audits or security assessments will show that the weaknesses have been resolved or mitigated; and
     - Audit and findings of UI IT security that comply with the standards established by the Office of Management and Budget Circular A-130, Appendix III, The Federal Information System Controls Audit Manual and the NIST computer security and information processing publications.

8. **SBR Award Timeline.**

   - SWAs must send the SBRs electronically, via email to ows.sbr@dol.gov no later than June 30, 2009;
   - Evaluation panel completes evaluation by July 31, 2009;
   - Final selection and required notifications made by August 31, 2009;
   - Grants awarded to selected SWAs by September 30, 2009;

9. **SBR Funds Expenditure.** FY 2009 automation funds must be obligated no later than September 30, 2011, and liquidated within 90 days of the obligation deadline. There are no provisions for extending the deadline for obligation of these funds, and any funds not obligated must be returned to the Federal government. States performance in completing funded projects within the applicable timeframe will be considered in awarding future SBRs.

10. **Action Requested.** SWA Administrators are requested to distribute this advisory to appropriate staff. SBRs that meet the above criteria must be sent electronically via email to ows.sbr@dol.gov no later than June 30, 2009. The SWA should ensure that the following are provided:

    - SBR proposal with supporting documentation.
    - Completed forms SF 424 (revised 9-2003), 424a and 424b as required in ET Handbook 336, 18th Edition.

11. **Inquiries.** Direct questions to Jagruti Patel at 202-693-3059 or patel.jagruti@dol.gov or Paul Bankes at 202-693-3053 or bankes.paul@dol.gov.

12. **Attachment.**

    I. Sample IT Contingency Plan Format
    II. Sample Security Assessment Reporting Form
    III. Extract from the OIG Audit Report: Presence of 17 IT Contingency Plan Elements in UI Systems' Plans

SAMPLE IT CONTINGENCY PLAN FORMAT

This sample format provides a template for preparing an information technology (IT) contingency plan. The template is intended to be used as a guide, and the Contingency Planning Coordinator should modify the format as necessary to meet the system's contingency requirements and comply with internal policies. Where practical, the guide provides instructions for completing specific sections. Text is added in certain sections; however, this information is intended only to suggest the type of information that may be found in that section. The text is not comprehensive and should be modified to meet specific agency and system considerations. The IT contingency plan should be marked with the appropriate security label, such as *Official Use Only*.

IT CONTINGENCY PLAN

1. INTRODUCTION

1.1 PURPOSE

This *{system name}* Contingency Plan establishes procedures to recover the *{system name}* following a disruption. The following objectives have been established for this plan:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
  - *Notification/Activation phase* to detect and assess damage and to activate the plan
  - *Recovery phase* to restore temporary IT operations and recover damage done to the original system
  - *Reconstitution phase* to restore IT system-processing capabilities to normal operations.
- Identify the activities, resources, and procedures needed to carry out *{system name}* processing requirements during prolonged interruptions to normal operations.
- Assign responsibilities to designated *{Organization name}* personnel and provide guidance for recovering *{system name}* during prolonged periods of interruption to normal operations.
- Ensure coordination with other *{Organization name}* staff who will participate in the contingency planning strategies. Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

1.2 APPLICABILITY

The *{system name}* Contingency Plan applies to the functions, operations, and resources necessary to restore and resume *{Organization name}'s {system name}* operations as it is installed at *primary location name, City, State*. The *{system name}* Contingency Plan applies to *{Organization name}* and all other persons associated with *{system name}* as identified under Section 2.3, Responsibilities.
The *{system name}* Contingency Plan is supported by *plan name,* which provides the *purpose of plan.* Procedures outlined in this plan are coordinated with and support the *plan name*, which provides *purpose of plan.*

1.3 SCOPE

1.3.1 Planning Principles

Various scenarios were considered to form a basis for the plan, and multiple assumptions were made. The applicability of the plan is predicated on two key principles:

- *The {Organization name}'s* facility in *City, State,* is inaccessible; therefore, *{Organization name}* is unable to perform *{system name}* processing for the *Department.*
- A valid contract exists with the alternate site that designates that site in City, State, as the {Organization name}'s alternate operating facility.

- {Organization name} will use the alternate site building and IT resources to recover {system name} functionality during an emergency that prevents access to the original facility.
- The designated computer system at the alternate site has been configured to begin processing {system name} information.
- The alternate site will be used to continue {system name} recovery and processing throughout the period of disruption, until the return to normal operations.

1.3.2 Assumptions

Based on these principles, the following assumptions were used when developing the IT Contingency Plan:

- The {system name} is inoperable at the {Organization name} computer center and cannot be recovered within 48 hours.
- Key {system name} personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the {system name} Contingency Plan.
- Preventive controls (e.g., generators, environmental controls, waterproof tarps, sprinkler systems, fire extinguishers, and fire department assistance) are operational at the time of the disaster.
- Computer center equipment, including components supporting {system name}, are connected to an uninterruptible power supply (UPS) that provides 45 minutes to 1 hour of electricity during a power failure.
- {system name} hardware and software at the {Organization name} original site are unavailable for at least 48 hours.
- Current backups of the application software and data are intact and available at the offsite storage facility.
- The equipment, connections, and capabilities required to operate {system name} are available at the alternate site in City, State.
- Service agreements are maintained with {system name} hardware, software, and communications providers to support the emergency system recovery.

The {system name} Contingency Plan does not apply to the following situations:

- **Overall recovery and continuity of business operations.** The Business Resumption Plan (BRP) and Continuity of Operations Plan (COOP) are appended to the plan.
- **Emergency evacuation of personnel.** The Occupant Evacuation Plan (OEP) is appended to the plan.
- *Any additional constraints should be added to this list.*

1.4 REFERENCES/REQUIREMENTS

This {system name} Contingency Plan complies with the {Organization name}'s IT contingency planning policy as follows:

The organization shall develop a contingency planning capability to meet the needs of critical supporting operations in the event of a disruption extending beyond 72 hours. The

procedures for execution of such a capability shall be documented in a formal contingency plan and shall be reviewed at least annually and updated as necessary. Personnel responsible for target systems shall be trained to execute contingency procedures. The plan, recovery capabilities, and personnel shall be tested to identify weaknesses of the capability at least annually.

The {system name} Contingency Plan also complies with the following federal and departmental policies:

- The Computer Security Act of 1987
- OMB Circular A-130, Management of Federal Information Resources, Appendix III, November 2000
- Federal Preparedness Circular (FPC) 65, Federal Executive Branch Continuity of Operations, July 1999
- Presidential Decision Directive (PDD) 67, Enduring Constitutional Government and Continuity of Government Operations, October 1998
- PDD 63, Critical Infrastructure Protection, May 1998
- Federal Emergency Management Agency (FEMA), The Federal Response Plan (FRP), April 1999
- Defense Authorization Act (Public Law 106-398), Title X, Subtitle G, "Government Information Security Reform," October 30, 2000
- Any other applicable federal policies should be added
- Any other applicable departmental policies should be added

1.5 RECORD OF CHANGES

Modifications made to this plan since the last printing are as follows:

Record of Changes			
Page No.	**Change Comment**	**Date of Change**	**Signature**

2. CONCEPT OF OPERATIONS

2.1 SYSTEM DESCRIPTION AND ARCHITECTURE

Provide a general description of system architecture and functionality. Indicate the operating environment, physical location, general location of users, and partnerships with external organizations/systems. Include information regarding any other technical considerations that are important for recovery purposes, such as backup procedures. Provide a diagram of the architecture, including security controls and telecommunications connections.

2.2 LINE OF SUCCESSION

The *{organization name}* sets forth an order of succession, in coordination with the order set forth by the *department* to ensure that decision-making authority for the {*system name*} Contingency Plan is uninterrupted. The Chief Information Officer (CIO), {*organization name*} is responsible for ensuring the safety of personnel and the execution of procedures documented within this {*system name*} Contingency Plan. If the CIO is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the Deputy CIO shall function as that authority. *Continue description of succession as applicable.*

2.3 RESPONSIBILITIES

The following teams have been developed and trained to respond to a contingency event affecting the IT system.

The Contingency Plan establishes several teams assigned to participate in recovering *{system name}* operations. The *{team name}* is responsible for recovery of the *{system name}* computer environment and all applications. Members of the *team name* include personnel who are also responsible for the daily operations and maintenance of *{system name}*. The *team leader title* directs the *{team name}*.

Continue to describe each team, their responsibilities, leadership, and coordination with other applicable teams during a recovery operation.

The relationships of the team leaders involved in *system* recovery and their member teams are illustrated in Figure XX below.

> *(Insert hierarchical diagram of recovery teams. Show team names and leaders; do not include actual names of personnel.)*

Describe each team separately, highlighting overall recovery goals and specific responsibilities. Do not detail the procedures that will be used to execute these responsibilities. These procedures will be itemized in the appropriate phase sections.

3. NOTIFICATION AND ACTIVATION PHASE

This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to {*system name*}. Based on the assessment of the event, the plan may be activated by the Contingency Planning Coordinator.

> **In an emergency, the *{Organization name}*'s top priority is to preserve the health and safety of its staff before proceeding to the Notification and Activation procedures.**

Attachment I

Contact information for key personnel is located in Personnel Contact list appendix. The notification sequence is listed below:

- The first responder is to notify the *Contingency Planning Coordinator*. All known information must be relayed to the *Contingency Planning Coordinator*.
- The systems manager is to contact the *Damage Assessment Team Leader* and inform them of the event. The *Contingency Planning Coordinator* is to instruct the *Team Leader* to begin assessment procedures.
- The *Damage Assessment Team Leader* is to notify team members and direct them to complete the assessment procedures outlined below to determine the extent of damage and estimated recovery time. If damage assessment cannot be performed locally because of unsafe conditions, the *Damage Assessment Team* is to follow the outline below.

Damage Assessment Procedures:

(Detailed procedures should be outlined to include activities to determine the cause of the disruption; potential for additional disruption or damage; affected physical area and status of physical infrastructure; status of IT equipment functionality and inventory, including items that will need to be replaced; and estimated time to repair services to normal operations.)

- Upon notification from the *Contingency Planning Coordinator*, the *Damage Assessment Team Leader* is to ...
- The *Damage Assessment Team* is to ....

Alternate Assessment Procedures:

- Upon notification from the *Contingency Planning Coordinator*, the *Damage Assessment Team Leader* is to ...
- The *Damage Assessment Team* is to ....
  - When damage assessment has been completed, the *Damage Assessment Team Leader* is to notify the *Contingency Planning Coordinator* of the results.
  - The *Contingency Planning Coordinator* is to evaluate the results and determine whether the contingency plan is to be activated and if relocation is required.
  - Based on assessment results, the *Contingency Planning Coordinator* is to notify assessment results to civil emergency personnel (e.g., police, fire) as appropriate.

The Contingency Plan is to be activated if one or more of the following criteria are met:

1. {*System name*} will be unavailable for more than 48 hours; or
2. Facility is damaged and will be unavailable for more than 24 hours; or
3. Other criteria, as appropriate.

- If the plan is to be activated, the *Contingency Planning Coordinator* is to notify all Team Leaders and inform them of the details of the event and if relocation is required.
- Upon notification from the *Contingency Planning Coordinator*, Team Leaders are to notify their respective teams. Team members are to be informed of all applicable information and prepared to respond and relocate if necessary.

- The *Contingency Planning Coordinator* is to notify the *off-site storage facility* that a contingency event has been declared and to ship the necessary materials (as determined by damage assessment) to the *alternate site*.
- The *Contingency Planning Coordinator* is to notify the Alternate site that a contingency event has been declared and to prepare the facility for the *Organization's* arrival.
- The *Contingency Planning Coordinator* is to notify remaining personnel (via notification procedures) on the general status of the incident.

4. RECOVERY OPERATIONS

This section provides procedures for recovering the application at the alternate site, whereas other efforts are directed to repair damage to the original system and capabilities.
The following procedures are for recovering the {*system name*} at *the alternate site*. Procedures are outlined per team required. Each procedure should be executed in the sequence it is presented to maintain efficient operations.

Recovery Goal. *State the first recovery objective as determined by the Business Impact Assessment (BIA). For each team responsible for executing a function to meet this objective, state the team names and list their respective procedures.*

- *{team name}*
  – *Team Recovery Procedures*
- *{team name}*
  – *Team Recovery Procedures*
- *{team name}*
  – *Team Recovery Procedures*

Recovery Goal. *State the second recovery objective as determined by the BIA. For each team responsible for executing a function to meet this objective, state the team names and list their respective procedures.*

- *{team name}*
  – *Team Recovery Procedures*
- *{team name}*
  – *Team Recovery Procedures*
- *{team name}*
  – *Team Recovery Procedures*

Recovery Goal. *State the remaining recovery objectives (as determined by the BIA). For each team responsible for executing a function to meet this objective, state the team names and list their respective procedures.*

5. RETURN TO NORMAL OPERATIONS

This section discusses activities necessary for restoring {*system name*} operations at the {*Organization name*}'s original or new site. When the computer center at the original or new

site has been restored, {*system name*} operations at the alternate site must be transitioned back. The goal is to provide a seamless transition of operations from the alternate site to the computer center.

Original or New Site Restoration

Procedures should be outlined, per necessary team, to restore or replace the original site so that normal operations may be transferred. IT equipment and telecommunications connections should be tested.

- *{team name}*
  – *Team Resumption Procedures*
- *{team name}*
  – *Team Resumption Procedures*

5.1 CONCURRENT PROCESSING

Procedures should be outlined, per necessary team, to operate the system in coordination with the system at the original or new site. These procedures should include testing the original or new system until it is functioning properly and the contingency system is shut down gracefully.

- *{team name}*
  – *Team Resumption Procedures*
- *{team name}*
  – *Team Resumption Procedures*

5.2 PLAN DEACTIVATION

Procedures should be outlined, per necessary team, to clean the alternate site of any equipment or other materials belonging to the organization, with a focus on handling sensitive information. Materials, equipment, and backup media should be properly packaged, labeled, and shipped to the appropriate location(s). Team members should be instructed to return to the original or new site.

- *{team name}*
  – *Team Testing Procedures*
- *{team name}*
  – *Team Testing Procedures*

6. PLAN APPENDICES

The appendices included should be based on system and plan requirements.

- Personnel Contact List
- Vendor Contact List
- Equipment and Specifications
- Service Level Agreements and Memorandums of Understanding

Attachment I

- IT Standard Operating Procedures
- Business Impact Analysis
- Related Contingency Plans
- Emergency Management Plan
- Occupant Evacuation Plan
- Continuity of Operations Plan.

Attachment II

Sample Security Assessment Reporting Form

Attachment II

Sample Security Assessment Reporting Form

To help organizations collect, organize, and report the findings of individual security control assessments for the information system, a sample reporting form is provided below. This sample reporting form is illustrative and is intended to be used for each security control and control enhancement included in the security control assessment. The form is not intended to limit the flexibility of organizations in determining the most appropriate presentation of assessment findings for the purposes of a given security control assessment.

SAMPLE SECURITY ASSESSMENT REPORTING FORM	
SECTION I: INFORMATION SYSTEM AND ASSESSMENT INFORMATION	
Information System Name	**Impact Level** *Low, Moderate, High*
Site(s) Assessed	**Assessment Date(s)**
Information System Components Where Security Control Employed *(e.g., firewall, router, workstation, server, laptop, PDA)*	
SECTION II: SECURITY CONTROL INFORMATION	
Security Control or Control Enhancement *Insert text from security control or control enhancement being assessed as stated in, or as referenced by the approved system security plan.*	
Supplemental Guidance Associated with Security Control or Control Enhancement *Insert text from the supplemental guidance from the security control or control enhancement being assessed as stated in, or as referenced by the approved system security plan.*	
SECTION III: ASSESSMENT FINDINGS	
Assessment Objective *Identify assessment objective (e.g., CP-1.1, associated with the security control or control enhancement described above).*	
Determination Statements *See determination statements below which restate the determinations from the assessment objective, as tailored for this security control assessment (e.g., including organization-specific information, where appropriate).*	**Finding** *(S/O)*
Determination Statement	
Determination Statement	
Determination Statement	

SAMPLE SECURITY ASSESSMENT REPORTING FORM
Assessment Methods and Objects *Identify assessment methods and assessment objects as tailored for this assessment (e.g., the specific version of a specification examined and the nature of the examination performed).*
SECTION IV: ASSESSOR COMMENTS AND RECOMMENDATIONS
Assessor Comments *Explanation of weaknesses or deficiencies noted for each finding of* ***other than satisfied****. Comments may also be included in this section regarding evidence used to support findings of* ***satisfied****.*
Assessor Recommendations *Recommendations for remediation, corrective actions, or improvements in security control implementation or operation.*

Attachment III

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

	State Workforce Authorities																								
Elements	**AL**	**AK**	**AZ**	**AR**	**CA**	**CO**	**CT**	**DE**	**FL**	**GA**	**HI**	**ID**	**IL**	**IN**	**IA**	**KS**	**KY**	**LA**	**ME**	**MD**	**MA**	**MI**	**MN**	**MS**	**MO**	**MT**
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	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			X		
Damage Assessment Procedures					X	X			X						X			X			X			X		
Detailed Recovery Procedures		X							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.

Attachment III

Presence of 17 IT Contingency Plan Elements in UI Systems' Plans (continued) [2]

	State Workforce Authorities																							
Elements	**NE**	**NV**	**NJ**	**NM**	**NC**	**ND**	**OH**	**OK**	**OR**	**PA**	**RI**	**SC**	**SD**	**TN**	**TX**	**UT**	**VT**	**VA**	**WA**	**WV**	**WI**	**WY**	**VI**	**DC**	**PR**
Purpose	X	X		X	X			X		X			X		X			X	X						
Applicability	X	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									
Line of Succession		X								X								X	X						
Responsibilities		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					
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					
Vendor contact information		X			X			X								X				X					
Checklists for system recovery		X			X										X						X				
Equip/System requirements lists		X			X			X			X									X					
Description/Direction to alternative sites					X			X			X										X				

[2] 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.