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 /s/
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. <u>Information Required</u>.

- 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