

EMPLOYMENT AND TRAINING ADMINISTRATION ADVISORY SYSTEM U.S. DEPARTMENT OF LABOR Washington, D.C. 20210	CLASSIFICATION UI
	CORRESPONDENCE SYMBOL OUI/DPM
	DATE March 29, 2010

ADVISORY: UNEMPLOYMENT INSURANCE PROGRAM LETTER NO. 19-10

TO: STATE WORKFORCE AGENCIES

FROM: JANE OATES /s/
Assistant Secretary

SUBJECT: Unemployment Insurance (UI) Fiscal Year (FY) 2010 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 2010 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 Contingency Planning; Unemployment Insurance Program Letter (UIPL) 24-04 Change 3, Unemployment Insurance Information Technology Security – Additional Information; Office of Inspector General (OIG) Report No. 23-08-004-03-315¹ and [OIG Report No. 23-09-002-03-315²](http://www.oig.dol.gov/public/reports/oa/2009/23-09-002-03-315.pdf).
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.

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>

RECLASSIFICATIONS None	EXPIRATION DATE March 29, 2011
----------------------------------	--

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 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; 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 2010 Funding. ETA will award selected SWAs funding to improve their UI IT Contingency Plans and UI IT Security. The priority will be to fund UI IT Contingency Plan SBRs first, and then use any remaining funds to fund UI IT Security SBRs.

- a. **UI IT Contingency Plan:** SWAs may submit a SBR to develop or update their UI IT Contingency Plan utilizing the guidelines provided in NIST SP 800-34. Attachment I 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. Upon completion of the plan, SWAs must have an IV&V conducted of their UI IT Contingency Plan based on guidelines provided in the NIST SP 800-34. SWAs must submit a copy of the IV&V certification report to their respective Regional Office (RO).

A UI IT Contingency Plan SBR must address all the key elements deemed as missing in the SWA UI IT Contingency Plan by the OIG Audit and describe the proposed corrections/solutions. See Attachment III, extracted 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. The SBR must include the total cost of the project; however, Federal funding for each 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 SBRs to address the 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 II 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.).

The UI IT Security SBR must also address the proposed remediation for each security weakness identified. Each SWA may submit multiple UI IT Security SBRs. Each SBR must 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. The following information is required to request for the SBRs:

- Specific to a UI IT Contingency Plan SBR, provide a list of the UI IT contingency planning key elements missing in the current plan according to the OIG, including a description of how the proposed remediation addresses these weaknesses. Also, submit a proposal from an independent entity to perform a UI IT Contingency Plan IV&V based on guidelines provided in the NIST SP 800-34;
- Specific to any UI IT Security SBR, submit 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, including 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. Proposals will be evaluated 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 III;
- 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 submit a copy of the IV&V certification report to their respective RO upon completion.

• **UI IT Security:**

Priority will be given to proposals that address the following:

- The specific security weaknesses documented in a recently-conducted security audit or security assessment report;
- Findings with the greatest risk;
- Provide assurance that future audits or security assessments will show that the weaknesses have been resolved or mitigated; and
- Audit 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. The SBR award timeline is as follows:

- SBRs must be submitted electronically, via email to ows.sbr@dol.gov no later than May 14, 2010;
- Award notifications will be made by July 16, 2010;
- Grants will be executed to selected SWAs by July 30, 2010.

9. SBR Funds Expenditure. FY 2010 automation funds must be obligated no later than September 30, 2012, 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 May 14, 2010. The SWA should ensure that the following are provided:

- SBR proposal with supporting documentation.
- Completed forms SF 424 (OMB Approval No. 4040-0004) and SF 424a (OMB Approval No. 4040-0006) 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. Attachments.

- 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