

EMPLOYMENT AND TRAINING ADMINISTRATION ADVISORY SYSTEM U. S. Department of Labor Washington, D.C. 20210	CLASSIFICATION UI
	CORRESPONDENCE SYMBOL OWS/DUIO
	DATE April 4, 2007

ADVISORY: UNEMPLOYMENT INSURANCE PROGRAM LETTER NO. 16-07

TO: STATE WORKFORCE AGENCIES

**FROM: EMILY STOVER DeROCCO /s/
Assistant Secretary**

SUBJECT: Solicitation for Unemployment Insurance (UI) Supplemental Budget Requests (SBRs) to Improve Information Technology (IT) Security

- 1. Purpose.** To announce the availability of Fiscal Year (FY) 2007 funds to improve UI Information Technology Security.
- 2. References.** ET Handbook No. 336, 18th Edition, the Unemployment Insurance State Quality Service Planning and Reporting Guidelines, Chapter 1, Section VI, C., SBRs and Chapter 1, Section VII, J., Assurance of Automated Information Systems Security; and Unemployment Insurance Program Letter (UIPL) 24-04 Change 2, Unemployment Insurance Information Technology Security – Additional Information and Self-Evaluation Tool.
- 3. Background.** As states continue to implement new technologies to operate their UI programs, there is an increasing need to monitor and improve the security of IT systems. The U.S. Department of Labor (DOL) encourages states to conduct IT security self-assessments. The results of the self-assessments can be used each year as a basis for states to provide “assurance” of their IT system security as required in the UI State Quality Service Plan. DOL’s Office of the Inspector General (OIG) recently conducted IT security audits in seven states. The OIG found security weaknesses in all seven states, and other states may have similar security weaknesses.
- 4. Fiscal Year 2007 Funding.** DOL will award funds to selected State Workforce Agencies (SWA) to address the UI IT security weaknesses that have been identified by recent IT security audits (performed within the last three years from the date of this UIPL) or by SWA IT self-assessments that comply with the National Institute of Standards and Technology (NIST) IT security guidelines. Each IT security SBR must address a specific security

RESCISSIONS None	EXPIRATION DATE September 30, 2009
----------------------------	--

weakness identified by the audit or self-assessment, and it must address the proposed remediation. Each state may submit multiple 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. All SBR submissions must include the following:

- A copy of the specifications or tools used for the audit or self-assessment;
- A copy of the complete audit report or self-assessment (performed within the last three years from the date of this UIPL) which outlines the finding(s) related to the UI program weakness being addressed;
- A description of how the proposed remediation addresses the security weakness;
- A projected cost breakout (including any additional costs to be covered by the SWA);
- A detailed cost proposal for any equipment, hardware, software, etc., to be purchased to address the security weakness;
- A detailed product description and specifications for any equipment, hardware, software, etc., to be purchased to address the security weakness;
- If contract staff are 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. DOL recognizes the states' concern related to disclosure of information about IT security weaknesses that are submitted to support their SBRs. DOL will protect the states' 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 that the state is requesting be held confidential should be clearly marked as "confidential."

Should DOL receive a FOIA request related to the security material submitted as part of this SBR, it will notify the relevant state, 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:

- How well the SWA's proposal addresses the specific security weaknesses documented in a recently-conducted security audit or self-assessment report.
- Level of risk of the finding which the SWA proposal addresses. Priority will be given to proposals that address findings with the greatest risk.
- Whether the SWA provides assurance that future audits or self-assessments will show that the weaknesses have been resolved or mitigated.
- Whether the audit and findings of UI IT security 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 to the National Office (NO) postmarked by May 25, 2007.
- Evaluation panel completes evaluation by June 22, 2007.
- Final selection and required notifications made by July 06, 2007.
- Grant awards made to selected SWAs by July 20, 2007.
- Deadline for UI IT Security grant obligation is September 30, 2009, and the deadline for expenditure is 90 days later.

9. Action Required. State Administrators are requested to distribute this advisory to appropriate staff. SBRs that meet the above criteria must be sent to the NO postmarked by May 25, 2007. Please be aware that all the SBRs that are mailed via United States Postal Service are irradiated which can delay receiving the SBRs. It is highly recommended that the SBRs be sent via a commercial carrier. Send these SBRs and the required documents to the attention of: U.S. Department of Labor, Office of Workforce Security/Division of UI Operations (Attn: Jagruti Patel), 200 Constitution Avenue, NW, Room S-4231, Washington, DC 20210. The state should ensure that the following are provided:

- Original and three copies of each SBR proposal with supporting documentation
- State Checklist Form
- Completed forms SF 424 (revised 9-2003), 424a and 424b as required in ET Handbook 336, 18th Edition

10. 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.

11. Attachment. State Checklist Form

STATE CHECKLIST FORM

UNEMPLOYMENT INSURANCE INFORMATION TECHNOLOGY SECURITY SUPPLEMENTAL BUDGET REQUEST

STATE:

DATE:

PROPOSAL AMOUNT:

(The total amount of the proposal cannot exceed \$100,000)

STATE CONTACT:

Name:

Telephone Number:

Email Address:

CHECKLIST:

All SBR submissions must include the following. Please check each item that has been submitted for the UI IT Security SBR. Any items that are not included may result in the failure of the proposal to be considered for possible funding.

- Original and three copies of each UI IT Security SBR proposal with supporting documentation.
- Completed forms SF 424 (revised 9-2003), 424a and 424b as required in ET Handbook 336, 18th Edition.
- Copy of the audit or self-assessment specifications or tools used.
- Complete report of the audit or self-assessment (performed within the last three years from the date of this UIPL) which outlines the finding(s) related to the UI program weakness being addressed.
- Description of how the proposed remediation addresses the security weakness (multiple solutions from which the state will later choose will not be funded).
- Projected Cost breakout (including any additional costs to be covered by the SWA).
- Detailed cost proposals for any equipment, hardware, software, etc. to be purchased to address the security weakness.
- Detailed product description and specifications for any equipment, hardware, software, etc. to be purchased to address the security weakness.
- All requested expenditures for staff identified by position title, number of hours, cost per hour and total cost.
- Timeline for the project.