

EMPLOYMENT AND TRAINING ADMINISTRATION ADVISORY SYSTEM U. S. Department of Labor Washington, D.C. 20210	CLASSIFICATION UI
	CORRESPONDENCE SYMBOL OWS/DUIO
	DATE April 25, 2005

ADVISORY: **FIELD MEMORANDUM NO. 10-05**

TO: **REGIONAL ADMINISTRATORS**

/s/

FROM: **JACK H. RAPPORT**
Administrator
Office of Field Operations

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

1. **Purpose.** To announce the availability of Fiscal Year (FY) 2005 funds to improve UI *Information Technology Security and Internal Security.*

2. **References.** ET Handbook No. 336, 17th Edition, the Unemployment Insurance State Quality Service Planning and Reporting Guidelines, Chapter 1, Section VI, C, SBRs and Chapter 1, Section VII, J, Assurances of Automated Information System Security; Unemployment Insurance Program Letter (UIPL) 24-04 Change 1, Unemployment Insurance Information Technology Security – Additional Information; UIPL 34-87 Unemployment Insurance Internal Security Risk Analysis; FM 05-05 Regional Role in Managing State Grants for the Unemployment Insurance Program; and ETA Handbook 376, Guidelines for Internal Security for UI Operations.

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) has encouraged states to conduct IT security self-assessments as a way to evaluate their security. The results of the self-assessments can be used each year as a basis for states providing assurance of their IT system security as required in the UI State Quality Service Plan. DOL’s Office of Inspector General (OIG) recently conducted IT security audits in seven (7) states. The OIG found security weaknesses in all seven states that need to be addressed. Other states may have similar security weaknesses.

IS reviews and audits, conducted periodically by Federal and/or state staff or under the Single Audit Act, are designed to monitor and strengthen internal controls. States should be conducting

RESCISSIONS None	EXPIRATION DATE April 30, 2006
----------------------------	--

IS reviews and risk assessments/analyses to evaluate the susceptibility of the IT programs to loss by internal fraud, waste, abuse or unauthorized use of UI resources. Tools available for these assessments include Risk Watch or the IS One Technical Assistance Guide, a software program produced by state personnel for the sole purpose of conducting an IS risk assessment or risk analysis. The software (is1tag.exe) may be obtained at: <http://www.centralvermont.com/isnet/>. A similar tool called SWA-Risk Assessment/Analysis may be obtained at: <http://www.centralvermont.com/swarisk/>.

4. Fiscal Year 2005 Funding. DOL will award funds to selected SWAs to address:

- UI IT security weaknesses that have been identified by recent IT security audits (performed within the last three (3) years) or by IT SWA self-assessments that comply with the National Institute of Standards and Technology (NIST) IT security guidelines; and/or
- UI IS weaknesses or vulnerabilities identified within the past three years as part of an overall audit of agency operations or by risk analyses or assessments performed using tools such as the *IS One Technical Assistance Guide*, *Risk Watch*, or another accredited assessment/analysis tool. States should consult with their Regional Office to ensure that the assessment tool on which their request is based will be accepted by the Department before submitting an SBR.

Each IT Security or IS SBR must address a specific security weakness identified by the audit, review, self-assessment or risk analysis and it must address the proposed remediation. SWAs may submit more than one SBR. Each SBR must describe the total cost to complete the proposed project; however, the Federal funding awarded for each successful SBR may not exceed \$150,000. Each SBR award will be based upon the SBR score as well as input provided from the Regional Office. Multiple SBRs from a single state may be funded but each SBR award will be limited to \$150,000. Please note that SBRs should not be duplicated for identical weaknesses that were identified in separate audits, reviews or assessments such as an IT security audit and an IS review or risk assessment/analysis.

All SBR submissions must include the following:

- A copy of the specifications or tools used for the risk assessment or self-assessment;
- A copy of the complete report of the risk assessment/analysis, audit or self-assessment (performed within the last three (3) years), 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 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 is requested, the documentation on type of position, estimated contract staff hours, anticipated costs per hour, and total staffing cost;
- If a SWA staff position is backfilled, the documentation on type of position, estimated staff hours, anticipated costs per hour, and total staffing cost for the backfilled position;
- A timeline for the project; and
- The name, address, telephone number, and e-mail address of a SWA contact person.

5. Confidentiality of Information. Under the provisions of the Freedom of Information Act (FOIA), records received by a Federal agency can be requested by any member of the public. DOL recognizes the states' concern related to disclosure of information about IT security, IS or internal control 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.

6. Evaluation Criteria. A National Office (NO) 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 risk assessment/analysis, security audit or self-assessment report.
- Level of risk of the finding which the SWA proposal addresses. Priority will be given to proposals which address findings with the greatest risk.
- Whether the SWA provides assurance that future audits, self-assessments or risk assessment/analysis 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 OMB Circular A-130, Appendix III, The Federal Information System Controls Audit Manual and the NIST computer security and information processing publications.
- RO recommendation(s).

7. SBR Award Time Lines.

- SWAs submit proposals to RO at a due date set by the RO;
- ROs submit proposals from SWAs to the NO by June 30, 2005;
- Evaluation panel completes evaluation by August 1, 2005;
- Final selection and required notifications made by August 15, 2005;

- Grant awards made to selected SWAs by August 31, 2005.

8. Action Required. Regional Administrators are requested to:

- Provide information contained in this Field Memorandum and attachments to the SWAs;
- Establish regional procedures and timelines for the submission and regional review of the proposals;
- Review the SBRs and provide comments and funding recommendation(s) with the submission to the NO;
- Forward to the NO review panel only those SBRs that meet the basic criteria outlined above.

SBRs that meet the criteria must be received in the NO by June 30, 2005, along with the following documents, which should be sent - Attention: Office of Workforce Security, Division of UI Operations. The RO should ensure that it provides the following:

- Original and two copies of each SBR proposal with supporting documentation.
- RO Checklist and Recommendation Form.
- Completed forms SF 424 (revised 9-2003), 424a and 424b as required in ET Handbook 336, 17th Edition.

9. 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.

10. Attachment. RO Checklist and Recommendation Form