U.S. Department of Labor

Employment and Training Administration
Sam Nunn Atlanta Federal Center
Room 6M12 - 61 Forsyth Street, S.W.
Atlanta, Georgia 30303

SWA ISSUANCE NO. 05-04

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) No. 24-04, Change 1, Unemployment Insurance Information Technology Security – Additional Information; UIPL No. 34-87, Unemployment Insurance Internal Security Risk Analysis; and ET Handbook No. 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 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 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 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. If there are questions, states should consult with the 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 (RO). 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 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 an 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 an 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' concerns 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 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 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 by close of business (COB) June 20, 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. SWA Administrators are requested to:

- Provide information contained in this Issuance and attachments to appropriate staff;

? Submit the following documents to the RO by COB June 20, 2005, ATTN: Office of Workforce Support:

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

9. Inquiries. Direct questions to Chuck Vantreese at 404-562-2122 or Vantreese.Charles@dol.gov or Dianna Milhollin at 404-562-2122 or Milhollin.Dianna@dol.gov

10. Expiration Date. April 30, 2006.

Helen N. Parker
HELEN N. PARKER
Regional Administrator

Attachment

STATE WORKFORCE AGENCY (SWA) CHECKLIST

UNEMPLOYMENT INSURANCE INFORMATION TECHNOLOGY SECURITY / INTERNAL SECURITY SUPPLEMENTAL BUDGET REQUEST

STATE:

DATE:

SWA CONTACT:
(Name, Telephone Number and Email Address)

CHECK ONE: ___ Information Technology Security
___ Internal Security

PROPOSAL AMOUNT:

THE TOTAL AMOUNT OF THE PROPOSAL CANNOT EXCEED $150,000:

CHECKLIST:

Please check each item that has been submitted for the Unemployment Insurance (UI) Information Technology (IT) Security/Internal Security (IS) Supplemental Budget Request (SBR). Any items that are not included may result in the failure of the proposal to be considered for possible funding.

___ SWA Checklist for UI Information Technology Security or Internal Security SBR.

___ Original and two copies of each UI IT Security/IS SBR proposal with supporting documentation.

___ Completed Forms SF 424 (revised 9-2003), 424a and 424b as required in ET Handbook No. 336, 17th Edition.

___ Copy of the risk assessment/analysis, audit or self-assessment specifications or tools used.

___ Complete report of the risk assessment/analysis, audit or self-assessment (performed within the last three years), which outlines the finding(s) related to the UI program weakness being addressed.

___ Description of how the proposed remediation addresses the security weakness.

___ 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 are identified by position title, number of hours, cost per hour and total cost.

___ The proposal does not contain multiple solutions from which the state will later choose but clearly identifies the state's proposed system.

___ Timeline for the project is provided.