EMPLOYMENT AND TRAINING ADMINISTRATION ADVISORY SYSTEM U.S. DEPARTMENT OF LABOR Washington, D.C. 20210	CLASSIFICATION UI
	CORRESPONDENCE SYMBOL OUI/DUIO
	DATE March 23, 2017

ADVISORY: UNEMPLOYMENT INSURANCE PROGRAM LETTER NO. 14-17

TO: STATE WORKFORCE AGENCIES

FROM: BYRON ZUIDEMA /s/
Deputy Assistant Secretary

SUBJECT: States' Responsibilities for Internal Security in the Unemployment Insurance Program

1. **Purpose.** To reissue and update guidance provided in General Administration Letter (GAL) No. 4-88, *Unemployment Insurance (UI) Internal Security (IS) Policy*, for use by the states in carrying out their responsibilities related to IS for UI operations.

2. **References.**
   - Section 303 of the Social Security Act (42 U.S.C. 503) – Grants to States for Unemployment Compensation Administration; State Laws;
   - 20 C.F.R. 601.6 – Grants for Administration of Unemployment Compensation Laws and Employment Service;
   - 20 C.F.R. Part 603 – Federal-State Unemployment Compensation (UC) Program; Confidentiality and Disclosure of State UC Information;
   - Unemployment Insurance Program Letter (UIPL) No. 12-01, *Outsourcing of Unemployment Compensation Functions*;
   - UIPL No. 12-01, Change 1, *Outsourcing of Unemployment Compensation Administrative Functions – Claims Taking;*
   - UIPL No. 29-05, *Memorandum of Understanding Regarding Unemployment Insurance Criminal Investigations Between the U.S. Department of Labor's Office of Inspector General and the Employment and Training Administration*;
   - UIPL No. 8-12, *Consolidation of the Employment and Training Administration (ETA) 9000 and ETA 227 Reports;*
   - UIPL No. 8-12, Change 1, *Consolidation of the Employment and Training Administration (ETA) 9000 and ETA 227 Reports*;
   - Employment and Training (ET) Handbook No. 376, *Guidelines for Internal Security in Unemployment Insurance Operations*;
   - ET Handbook No. 336, 18th Edition, *Unemployment Insurance State Quality Service Plan (SQSP) Planning and Reporting Guidelines*; and
   - ET Handbook No. 407, 4th Edition, *Tax Performance System.*

RESCISSIONS	EXPIRATION DATE
GAL No. 4-88, UIPL 42-87, UIPL 42-87 Change 1	Continuing

3. **Background.** Preventing and detecting internal fraud and abuse is a top priority for UI program administrators. States are responsible for creating policies, procedures, and internal controls that effectively protect the integrity and security of UI program staff, program operations and systems, UI funds, UI data, and other state assets.

   Internal controls are policies, procedures, techniques, and mechanisms designed to help protect state assets including, but not limited to, confidential information, UI funds, systems, business processes, and procedures used to transmit, process, and/or store UI data and information. These controls must ensure the integrity of the systems and resources (including human capital) of UI and workforce services provided through the state UI agency. States need to develop guidelines related to internal controls such as separation of duties, reviews of program areas at the functional and/or activity level to assess adherence to policies/procedures, and individual accountability for the safeguarding of information created, stored, accessed or transmitted through UI systems or equipment. See Attachment to this UIPL.

   The purpose of state IS programs is to ensure that all appropriate internal controls and processes are in place, and are adequate to ensure program integrity and security and minimize program vulnerabilities and faulty procedures. State IS staff must continuously review adequacy of internal controls and make recommendations to executive management for the implementation of internal controls where none exist and the strengthening of controls where weaknesses are detected.

   States are required, as a condition of receiving Federal UI administrative grants, to provide in their laws for "[s]uch methods of administration…as are found by the Secretary of Labor to be reasonably calculated to insure full payment of unemployment compensation when due," and "the expenditure of all [UI grant] moneys…solely for the purposes and in the amounts found necessary by the Secretary of Labor for the proper and efficient administration of such State law." 42 U.S.C. 503(a)(1) and (8). Monitoring UI operations and safeguarding UI assets are important components of these requirements. UI programs, such as Benefit Accuracy Measurement (BAM), Benefit Payment Control (BPC), Benefit Timeliness and Quality (BTQ), and Tax Performance Systems (TPS), have been implemented to monitor unique aspects of each state's UI operations. IS programs, are designed to assess internal risks and threats as well as threats to the entire UI system and to provide recommendations and remedies to safeguard UI assets. Therefore, it is a fundamental requirement for states to have an active and effective IS program.

   State IS staff activities include conducting risk assessments and audits, reviewing procedures or processes, conducting investigations of alleged internal violations by state staff (acting alone or in collusion with other perpetrators), and conducting IS reviews of UI operations, (i.e., operations performed by UI program or other staff that serve to accomplish the mission of the UI program). Examples of state IS activities are provided throughout this guidance.

4. **State Responsibilities.** The UI Annual Funding Agreement and the State Quality Service Plan (SQSP), ET Handbook No. 336, 18th Edition, outline the administrative and program

requirements, funding restrictions, and public policy assurances and attestations that must be certified annually. States are responsible for ensuring internal controls are adequate to protect the integrity and security of state assets including, but not limited to, confidential information, UI funds, and systems and business processes used to create, transmit, process, and/or store UI data. State staff that perform IS duties must be:

- Responsible to officials at a sufficiently high level to permit the independent review and monitoring of UI program operations and system(s) integrity;
- Supervised by an official other than a UI Chief of Benefits, UI Chief of Tax, the Chief of Information Technology (IT), UI program managers other than the IS Program Manager, or any individual or organization having direct responsibility for UI tax or benefit payments, certifications, or processing operations; and
- Authorized to perform reviews, assessments, and audits on a regular and ongoing basis. See Section 6 of this UIPL for an overview of IS staff responsibilities.

In addition, there are important areas that must be examined as part of the IS process. Key areas to be reviewed, assessed, and/or audited by IS staff must include:

- **Organization and Management**: Organization and management refers to the human resource functions of management. States are responsible to ensure appropriate separation of duties between functional areas within the UI program, including both Benefits and Tax operations. Examples of functions that must be assessed include:
  - Performance management;
  - Fiscal activities;
  - Security of personnel, equipment and agency records, including identification and monitoring of restricted work areas;
  - Personnel practices relating to internal security, including background checks for certain positions; and
  - IT operations related to key internal controls.

- **Safeguarding UI Funds**: Safeguarding UI funds means protecting the funds coming into the program, (such as grants awarded to states to administer the UI program, tax contributions and overpayment collections) and UI funds going out, (such as benefit payments and tax refunds). Examples of functions assessed to safeguard the funds include data cross matches (e.g., matching UI benefit payments against employee names/addresses), and processes for disbursing electronic and/or paper check payments.

- **Tax Operations**: Tax operations involve all tax-related functions within the UI program. State IS reviews should complement, but not duplicate, the reviews performed as a part of UI TPS review. Examples of tax functions to be reviewed and assessed include processes and procedures for employer contributions/tax receipts and reports, field audits, wage credits, employer accounts, procedures for employer refunds, access control policies and procedures, and essential separation of duties between appropriate functional areas (e.g., prohibiting the same staff member from establishing employer accounts and processing

UI claims; prohibiting the same staff member from collecting UI employer contributions and posting payment details to employer accounts).

- **Benefit Operations**: Benefit operations involve all benefit claim functions, activities and security in UI claims call/contact centers and other claims processing centers/offices. Examples of these functions include claims taking and claims processing procedures, debit card and direct deposit functions, benefit payment procedures, benefit audit cross matches, records management of information used to establish, recover, waive, litigate, offset, and write off benefit overpayments, access control policies and procedures, and essential separation of duties between appropriate functional areas (e.g., prohibiting the same staff member from establishing employer accounts and processing UI claims).

- **Information Technology (IT) Security**: State IT security refers to the processes and procedures used to protect the state's UI IT systems and electronic data. Examples include verification of:
  - Authorized user authentication;
  - Authorized user/system access (on-site, remote, third party);
  - System permissions;
  - Password policy;
  - Change control procedures;
  - Event logs;
  - Firewalls;
  - Data encryption;
  - Secure data connections;
  - Information systems and data security;
  - Safeguards for proprietary data and data shared or secured through joint agreements;
  - Safeguards to protect the confidentiality of information obtained or housed on state information systems;
  - An updated and tested disaster recovery plan;
  - The existence of antivirus software;
  - Physical computer security and policies for updating the master benefit/tax file(s);
  - User training and security awareness;
  - System and data integrity;
  - Contingency and disaster recovery planning; and
  - Access control policies and procedures for IT staff.

- **Physical Security**: Physical security refers to essential actions necessary to safeguard people and state assets (e.g., agency employees, visitors on state property, agency records, buildings, equipment and other physical property owned or used for the administration of the UI program, including electronic data, standard operating procedures, business methodologies, and contingency plans) of the UI agency. Physical security also refers to actions taken by the state agency to safeguard the confidentiality of claimant and employer information and to control access to areas where UI data is created, stored, processed or disseminated.

5. **Management Responsibilities**. The state executive management team and program managers have overall responsibility for the protection of UI program assets and operations. These responsibilities include:
    - Ensuring the development and operation of an effective IS function that provides for an assessment/review of the state's internal controls on an ongoing basis;
    - Implementing, as appropriate, IS staff recommendations that will help to ensure that IS strategies, corrections, and controls are enforced and/or established if none exist and corrected when weaknesses are found in the UI program;
    - Ensuring employees understand the importance of IS;
    - Ensuring employees understand their internal fraud prevention and reporting responsibilities;
    - Ensuring that orientation training for new state staff includes IS-related information;
    - Providing information to staff about unacceptable behavior while handling UI-related information and requiring signed acknowledgment of receipt of such information;
    - Providing memoranda/information outlining sanctions imposed if an employee commits a fraudulent act;
    - Ensuring that all relevant/necessary information and records are made available to IS staff upon request for IS reviews and investigations;
    - Ensuring that IS staff understand and carry out their roles, responsibilities, and job duties;
    - Ensuring that only merit staff make determinations of an individual's UI eligibility and/or determine an employer's liability for UI coverage in accordance with guidance contained in UIPL No. 12-01;
    - Limiting, to the greatest extent possible, the amount of personally identifiable information displayed on communications to employers and UI claimants; and
    - Ensuring that the state complies with the assurances outlined in ET Handbook No. 336, 18th Edition, and in the State Quality Service Plan (SQSP).

6. **IS Staff Responsibilities.** State IS staff must conduct, on a periodic basis, reviews and audits of internal controls within the UI program operations, including operations within the state's central office, call/contact centers, American Job Centers, and for other UI-related activities and operations, as appropriate. State IS staff also conducts reviews stemming from duly authorized requests for reviews, investigations, or audits to address identified or suspected fraud, waste, abuse and/or problem areas. States have flexibility in how to organize and operate their individual IS program; however, the scope of work, generally, should include the following actions in addition to other required audits and reviews:

    - Plan, conduct, and/or oversee a review of internal controls in the state's UI operations at least once every four years;
    - Plan, conduct, and/or oversee a risk assessment covering all UI program operations every three years. The purpose of a risk assessment is to identify risks, and identify ways to mitigate or manage the risks. Thus, IS staff working with IT staff can examine

appropriate risk assessment software or develop software/processes to conduct these assessments and help eliminate the risks;

  - States may choose to combine their review of internal controls and risk assessments. If these reviews are combined, the review must be conducted at least once every three years.

- Conduct a combined review within one year of any significant program change (including changes to internal controls) or any IT change to help ensure vulnerabilities are addressed;
- Consult with appropriate staff when there are changes to benefit payment procedures or other internal controls;
- Consult with IT staff and confirm that standards for internal controls for the IT system(s) comply with nationally accepted standards (e.g., National Institute of Standards and Technology, Government Accountability Office Standards for Internal Controls in the Federal Government). An IT risk assessment must be conducted at least once every three years or within one year when there are significant changes to any UI systems (e.g., IT platform changes, system enhancements, automation of systems or business processes, changes to facilities where IT processing or storage systems reside, or other conditions that may affect the security status of the system as stated in ET Handbook No. 336, 18th Edition);
- Consult with and make recommendations, as needed, when IT systems are updated and modernized to ensure appropriate internal controls are included and, as appropriate, for procedural and IT system changes to strengthen internal controls in UI operations and to ensure proper and authorized access to systems;
- Review the results of any state UI program accountability process or review (e.g., a self-assessment review) to identify any IS weaknesses or breaches identified by a self-assessment review;
- Consult with the BAM staff to mitigate any IS weaknesses or breaches identified by BAM reviews;
- Consult with the TPS reviewer to mitigate any IS weaknesses or breaches identified by TPS system reviews;
- Review the state's single audit reports related to UI and consult with appropriate agency leadership to mitigate any internal control weaknesses identified;
- Consult with IT staff to verify that the state is complying with the IT assurances outlined in ET Handbook No. 336, 18th Edition and in the SQSP;
- Assess and, as appropriate, conduct investigations of reported allegations of employee fraud;
- Report known or substantive allegations of malfeasance, criminal misconduct, and large-scale fraud promptly to the Office of Inspector General through the appropriate ETA Regional Office and in accordance with UIPL No. 29-05 and/or with appropriate officials in the state as required by state laws or regulations;
- Report any overpayments/cases of agency employee benefit fraud, the number of fraud cases referred for prosecution related to agency employee fraud, and the number of convictions due to employee fraud on the ETA 227, Overpayment Detection and Recovery report, as stated in UIPL No. 8-12;

- Verify that the agency has a current disaster recovery/contingency plan that is periodically tested; and
- Prepare periodic written reports to state management on IS risk analyses, reviews, investigations, and audits conducted, and include recommendations for corrective actions, as appropriate.

7. **Action Requested.** State Administrators should provide the information in this UIPL to appropriate staff.

8. **Inquiries.** All questions or inquiries should be referred to the appropriate Regional Office.

9. **Attachment**. Internal Security Guidelines for Unemployment Insurance Programs.