Unemployment Insurance (UI) Benefit Operations Self-Assessment Tool:
Internal Security (IS)

This self-assessment review of the state's Internal Security (IS) functional area will examine IS processes and operations. The reviewer will consult with appropriate staff regarding each operational element, as necessary, to ensure accurate and complete information is reported. This will include Unemployment Insurance (UI) administrators, IT managers, and the IS manager. Depending on how the state's agency is organized, the reviewer may need to consult with staff outside of the UI operations.

Upon completion of this review, the results should be shared with UI administrators and the IS manager. The self-assessment findings can provide a very good analysis of the state's IS operations and can be used to drive process and program-improvement initiatives.

The purpose of this self-assessment review is for the reviewer to exam whether the state agency's IS operations can verify that key IS responsibilities were performed/completed during the review period. It is not expected or intended that the self-assessment reviewer conduct these IS responsibilities.

A comments section is provided for each operational element, which the reviewer should use to document any observations regarding issues identified related to a specific element that is not covered by the questions. In addition, a concluding comments section is provided at the end of the self-assessment to capture any general comments about this functional area. The reviewer can provide information here that Federal reviewers and state UI administrators and managers can use to assess program operations and the state's effectiveness in providing quality services in this functional area.

As used throughout the IS self-assessment tool, the term "state" means the state agency that operates the state's UI program.

Save your entries regularly as you complete the review and when you close the self-assessment to ensure your answers are saved.

SECTION 1: Procedures, Policies, and Confidentiality

The purpose of this section is to review the policies and procedures provided by the agency for staff to use in operating this functional area of the UI program. These are the written (in hard-copy, electronically, or both formats) standards, instructions, and guidelines that staff regularly use in the operation of the program. The reviewer may utilize resources that include manuals, handbooks, desk aids, computer help screens, training guides, organized collections of procedures or policies, or other readily accessible instructions which can help staff do their work correctly. Instructions will normally include general information such as compilations of relevant laws and regulations, as well as detailed instructions for carrying out individual jobs in the agency. Reviewers may need to look in many places to examine all relevant instructions and consult with UI administrators and the state agency's IS manager.

The reviewer will document whether the state agency has policies and procedures sufficient to provide guidance and instruction to staff that are responsible for the state agency's IS program. Existing policies and procedures should be examined to determine whether they are up-to-date and address all law changes, organizational changes and technology changes that occurred during the review period.

Helpful Info.

Question 1a: If the state has a strategic plan or policies and procedures for the IS program, the reviewer will examine all applicable documentation to determine which security practices are covered.

Question 2: The reviewer will consult with the IS manager to verify which areas were covered by the state's disaster recovery plan during the review period.

Question 2b: If the state tested its disaster recovery plan during the review period, the reviewer will document the date and results of the test(s).

Question 3a: The reviewer will consult with the IS manager to verify which areas were covered by the state's business continuity plan during the review period.

- Critical contact information, in this case, refers to having a list of contacts, including their contact phone numbers and email addresses, etc. in the event it is necessary to contact them to implement a disaster recovery plan.
- Upstream applications would be those that feed data to the UI system, such as the state's workforce programs for WPRS and RESEA; Contributions or Revenue systems for wage data, etc.
- Downstream applications are those to which data is sent by the UI system, such as the ICON interstate application; interfaces with the Federal Claims Control Center (FCCC), workforce systems, etc.

Helpful Info. (*continued*)

Question 3c: If the state tested its business continuity plan during the review period, the reviewer will document the date and results of the test(s).

Question 5: The reviewer will consult with the IS manager to determine whether the state conducted a threat assessment during the review period and, if so, document all areas of risk covered by the assessment.

Question 6a: The reviewer will review the state's policies and procedures regarding building access and control of confidential data and documents and indicate all security measures that are covered.

Question 7: The reviewer should review the confidentiality provision of 20 CFR 603 and the state's statute to ensure the state has fully and correctly implemented operating procedures concerning staff handling of confidential UI data and documents.

Question 7b: The reviewer should review UIPL No. 29 - 05 regarding requirements for reporting investigations involving potential internal UI fraud, identity theft, or illegal benefit payments to state UI staff to the US Department of Labor's Office of Inspector General, to determine whether the state's policies and procedures provide adequate guidance on the issue.

Question 8a: If the state pays unemployment benefits by paper warrant/check, the reviewer will consult with UI managers and the IS manager to document the controls the state has in place to ensure returned warrants are properly secured until they are destroyed.

Question 11f: If IS staff has conducted an Internal Security audit of the UI program, the reviewer will document any deficiencies identified during the most recent review.

Question 13: The state should employ work processes that provide checks and balances so that the same employee is not responsible for all phases of work processes, such as cancelling benefit payments, issuing supplemental payments, tax functions and handling of cash, etc.

Question 15: This question refers to UI agency internal computer system access (i.e., state employee access) – it is not asking about the general public.

SECTION 2: Training

Managers/employees should possess and maintain a level of expertise which enables them to accomplish their assigned duties. Training systems should be sufficient to ensure that personnel understand and perform their duties properly. When reviewing IS activities related to training systems, the reviewer should consult with the state's training unit/staff and the IS manager and examine formal training procedures (e.g., the training is conducted using an established schedule and using set guidelines). The state should have procedures for identifying general and specific training needs, for developing a training curriculum and training materials, and for delivering training to IS staff and delivering training on IS matters to UI program staff, as needs are identified.

Helpful Info.

Question 1: The reviewer will document the methods the state uses to provide training to IS staff, including the resources and materials used for training (Question 1 generally means training related to UI program operations, UI data safeguards, security of UI staff, etc., that helps IS staff effectively perform their duties). See Unemployment Insurance Program Letter (UIPL) No. 14-17 at: Link to UIPL 14-17.

Question 2: The reviewer will document who provides training to IS staff and whether the provider is in-agency personnel or an outside resource.

Question 4: The reviewer will identify the state's approach to providing IS training to UI program staff.

SECTION 3: Workload Analysis / Management Controls

The reviewer will examine the state's ability to manage the IS program, and will also review the methods used by the state to identify security vulnerabilities in IT operations and at its physical locations as well as detecting internal fraud and/or abuse. The reviewer will interview UI administrators and the IS manager to document the state's practices for managing its IS program.

Helpful Info.

Question 2: The reviewer will identify offices where UI staff work that were open to the public during the review period. "Open to the public" means that some part of the building is accessible by the public, even though the area where the UI work is performed may be secured.

Question 3: The reviewer will document the methods the state uses to assess all potential vulnerabilities in its locations, for internal and external threats.

Helpful Info. (*continued*)

Question 4: The reviewer will document the methods the state uses to assess all potential vulnerabilities in its computer systems and data security. "Data handling" includes data collection, data storage, data transmission, and data destruction.

Question 6: The reviewer should review UIPL No. 08 - 12 regarding requirements for reporting Internal Security activities and fraud case investigations to determine whether the state's policies and procedures provide adequate guidance.

Question 6a: The reviewer will report whether the state's internal methods for compiling overpayment detection and recovery data for the ETA 227 report are automated.

SECTION 4: Information Technology

When completing this section of the self-assessment, the reviewer should consult with UI and IT administrators and the IS manager. The reviewer will examine in depth the role of the IS unit in evaluating and monitoring IT systems security. The state's disaster recovery plan and its contingency planning for implementation of emergency UI programs with a short lead time will be reviewed here.

Helpful Info.

Question 2d: The reviewer should consult with the IS manager to review the unit's records regarding the most recent IT security test and document the date the test was performed and any deficiencies that were identified.

Question 2f: If security-related deficiencies were identified during the most recent IT security test that have not been corrected at the time of the review, the reviewer should document the reason(s) the deficiencies have not been corrected. It may be necessary to consult with the UI manager and/or the IT manager to obtain this information.

Question 3: The reviewer will identify whether the state's IT security testing includes internal and external security testing.

Question 10a: The reviewer should review and document all security measures the state agency's IT department used in its physical location(s).

Helpful Info. (*continued*)

Question 23c: If the state tested its disaster recovery plan during the review period, the reviewer will document the date and results of the test.

Question 24: The reviewer should review requirements for methods of conducting security self-assessments in compliance with NIST SP 800-53 and NIST SP 800-53A.

SECTION 5: Agency Staff Access & Communication

The reviewer will examine the role of Internal Security staff related to the development and implementation of security policies and procedures. The reviewer will consult with UI administrators and the IS manager when completing this section of the self-assessment.

Helpful Info.

Question 1: The reviewer will document the agency security measures that IS staff was involved in developing or enforcing.

SECTION 6: Operational Efficiency / Resource Allocation

Through interviews with UI administrators and the IS manager, the reviewer will determine whether the state has allocated sufficient resources to training, facilities, staff, etc. to support IS program operations. The reviewer will identify efficiencies and automation the state has used to improve IS operations. The reviewer will identify any areas for improvement in IS operations that will be addressed in the future.

Helpful Info.

Question 1a: The reviewer will document any automated systems the state uses to monitor UI staff computer transactions for fraudulent or unauthorized activity.

Question 4a: The reviewer will document the state's methods for conducting internal investigations regarding suspicious activities and potential breaches of computer security, including which office is responsible for conducting these investigations.

Helpful Info. (*continued*)

Question 5a: If the state conducted any business process analysis efforts during the review period, the reviewer will document all IS initiatives that have been implemented and any results due to the changes.

Question 5b: If the state conducted any business process analysis efforts during the review period, the reviewer will document all IS initiatives that were recommended but have not been implemented, including an explanation of why they have not been implemented.

SECTION 7: Staffing

The reviewer will examine organizational changes that occurred during the review period, if any, and their effect on the state's ability to manage its IS operations. The reviewer should consult with UI administrators, the IS manager, and the state agency's human resource manager when completing this section of the self-assessment.

Helpful Info.

Question 2: Staffing allocations are examined to determine whether IS operations are adequately staffed, based upon state size and FTE allocations. Report the percentage of FTEs in the FY MPU allocation for Internal Security compared to the total FTEs of the UI Benefits operations.

Question 3: The reviewer will report the number of FTEs budgeted for IS during the review period. This will include all positions budgeted by the state after Federal "base" allocations.

Question 4: The reviewer will report the number of FTEs dedicated to IS operations during the review period. Dedicated FTEs means the number of FTEs that were charged to the function.

Question 6: The reviewer will document the state agency's security procedures taken when an IS staff is terminated—for example, computer access is immediately suspended, the individual is escorted from the premises, etc.

Question 10: The reviewer will document whether IS staff follow Federal cost allocation principles when reviewing other programs besides UI to ensure costs are allocated by program.

SECTION 8: Concluding Summary Comments

The reviewer will use the Concluding Summary Comments section to highlight the state's strengths and weaknesses that impact the Internal Security functional areas and to identify issues that have not been addressed in any other section of the self-assessment. These comments are intended to provide Federal reviewers and the state's UI administrators with additional insight into these program areas, focusing on methods that have proven to be successful and can be capitalized upon or areas where corrective measures may be needed.

The first comment area provides the reviewer an opportunity to share any examples of good and/or exemplary operations in this functional area after reviewing each operational element. The reviewer can use this space to identify any policy, procedure or operation that would constitute a successful practice that can be shared with other states.

The second comment area provides the reviewer to document issues detected during the review that are having an adverse impact on the functional area, affecting the state's performance, ability to meet performance standards or customer service. It is also a place to recommend corrective actions for the agency's leadership to consider implementing.

The final comment area in this section provides the reviewer space to share any additional comments, concerns or observations regarding the state's operations in this functional area.