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

REVIEW PERIOD: Begins _____ **Ends** _____

Unless otherwise noted, all questions are applicable to the review period.

SECTION 1: Procedures, Policies, and Confidentiality

Resources may include manuals, handbooks, desk aids, computer help screens, training guides, organized collections of procedures or policies, or other readily accessible instructions that can help IS staff do their work and conduct reviews. 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 besides the IS unit to examine all relevant instructions.

1. Does the state have a strategic plan or written policies and procedures for its Internal Security program?
Select Answer

1a. If yes, does the strategic plan and/or written policies include policies and procedures regarding the following Internal Security practices related to the UI program? (*check all that apply*)

- ☐ Security risk management
- ☐ Critical asset identification
- ☐ Physical security
- ☐ System and network management
- ☐ Authentication and authorization
- ☐ Access control
- ☐ Vulnerability management
- ☐ Incident management
- ☐ Awareness and training
- ☐ Ethical responsibilities
- ☐ Privacy
- ☐ Encryption of Internet transactions and all data transmitted from remote locations

Question 1a check boxes continue on next page

☐ Other (*explain*)

2. During the review period, did Internal Security staff verify that the state has a disaster recovery plan that covers the following areas affecting the UI program? (*check all that apply*)

Select Answer

- ☐ The identification of possible disasters that could interrupt access to systems
- ☐ Directions to off-site storage locations
- ☐ Business recovery location
- ☐ Disaster recovery organization chart/list – action team call tree for internal contacts and their locations
- ☐ Hardware and other required inventory needed in the event of a disaster
- ☐ Software application(s) and other required inventory needed in the event of a disaster
- ☐ Operating system and other required inventory needed in the event of a disaster
- ☐ Vendor name(s) and contact information, as appropriate
- ☐ Media, records, and documentation needed for restoration
- ☐ Recovery procedures and priority of servers, applications, and other dependent systems
- ☐ Time frames for restoring systems to ensure required transaction processing
- ☐ Critical files and work in process assessment report
- ☐ Recovery status report
- ☐ Other (*explain*)

Question 2 check boxes continue on next page

☐ Other (*explain*)

2a. If yes, has the state tested the UI operations disaster recovery plan?

Select Answer

2b. If yes (to question 2a), what was the date of the most recent test?

2c. If yes (to question 2a), what was the result of the most recent test?

2d. If no (to question 2a), explain. (e.g., has the state planned or scheduled a test)

3. During the review period, did Internal Security staff verify that the state has a business continuity plan that covers the UI program?

Select Answer

3a. If yes, indicate which of the following preparedness functions are addressed in the business continuity plan. (*check all that apply*)

Procedures for response and recovery that contain predetermined prioritized actions on how to:

- ☐ Respond to a disruptive event
- ☐ Activate the plan
- ☐ Recover critical business processes
- ☐ Restore the business back to its state before the incident or disaster occurred

☐ Alternate work locations and work procedures (if necessary) have been identified in case the primary site is unavailable

☐ Procedures to equip the alternate work site (telecommunication systems, PCs, and other devices), and contracts with third parties

☐ Procedures to safeguard and reconstruct the home site

☐ Procedures to safeguard the alternate site

☐ Reconstruction plans for the recovery of all systems resources at the original location

☐ Critical information on continuity teams, affected staff, and suppliers

☐ Major upstream / downstream applications that contain information system groups that may be affected, and critical contact information

☐ Time frames for restoring systems to ensure required transaction processing times are met and disruption time is minimized

☐ Other (*explain*)

3b. If yes, has Internal Security staff verified that the state tested the business continuity plan?

Select Answer

3c. If yes, what was the date of the most recent test?

3d. If yes, what was the result of the most recent test?

3e. If no, explain (e.g., has the state planned or scheduled a test).

4. Are the state agency's disaster recovery and continuity plans coordinated with or a part of a larger state government plan?

Select Answer

4a. If yes, does the state UI agency participate in a state government-wide plan and activities?

Select Answer

5. During the review period, did Internal Security staff verify whether the state conducted a threat assessment for the UI program for each of the following areas of risk? (*check all that apply*)

- ☐ Fire
- ☐ Floods and other water damage
- ☐ Earthquakes
- ☐ Tornadoes
- ☐ Power outages
- ☐ A/C or heating failure
- ☐ Theft/Robbery/Unauthorized access
- ☐ Other (*explain*)

6. During the review period, did Internal Security staff verify state policies and procedures regarding building access and the control of confidential or sensitive data and documents in its UI offices and associated offices such as Job Centers?

Select Answer

6a. If yes, do the policies and procedures address the following areas? (*check all that apply*)

- ☐ Building access
- ☐ Security guards controlling entrances and exits of the building, as needed
- ☐ Sign-in sheets for visitors, as appropriate
- ☐ Secure area for equipment, document storage, etc.
- ☐ Record retention
- ☐ Documents that contain confidential information that are slated for destruction
- ☐ Other (*explain*)

7. During the review period, did the state have policies and procedures that ensure Internal Security practices comply with the confidentiality provision of 20 CFR 603 and the state's statute?

Select Answer

7a. If yes, do the policies and procedures address the following areas? (*check all that apply*)

- ☐ Confidentiality agreements related to sensitive data
- ☐ Documents containing confidential information that must be concealed when an employee is away from his/her workstation
- ☐ Storing documents that contain confidential information
- ☐ Logging off computers whenever employees are away from their workstation
- ☐ Computers must be logged-off by the employee at the end of each day
- ☐ Security warnings at log-in screens
- ☐ Security protocols for employees that work remotely
- ☐ Transmission of confidential data via email
- ☐ Other (*explain*)

- ☐ N/A

7b. Do Internal Security policies and procedures provide for engagement of the US Department of Labor's Office of Inspector General, as appropriate, related to investigations of potential internal UI fraud, identity theft or illegal benefit payments to state UI staff, or collusion of UI staff to improperly pay benefits to others? (Reference UIPL No. 29 - 05)

Select Answer

8. If the state pays benefits by paper warrant/check, does Internal Security staff verify that the state has and follows policies and procedures for handling returned warrants?

Select Answer

8a. If yes, what controls does the state use for handling returned warrants (e.g., establish a chain of custody from the mailroom to Benefits staff)?

9. If the state pays benefits by paper warrant/check, does Internal Security staff verify that the state has and follows policies and procedures for handling cancelled warrants?

Select Answer

9a. If yes, what controls does the state use for handling cancelled warrants (e.g., establish a chain of custody, proper storage of warrants until destroyed)?

10. Is there a standard report form used by the agency to document security incidents (including breach of confidentiality incidents)?

Select Answer

10a. If yes, which office receive(s) these reports?

10b. How many incidents, if any, have been reported during the review period?

11. Do the state's policies and procedures require regularly scheduled Internal Security reviews of key UI program functions?

Select Answer

11a. If yes, what programs are covered by these Internal Security audits? (*check all that apply*)

- ☐ Benefits
- ☐ Benefit Payment Control
- ☐ Benefit Accuracy Measurement
- ☐ Appeals
- ☐ Fiscal – benefits, tax accounts, and grant management
- ☐ Information Technology
- ☐ Other (*explain*)

☐ N/A

11b. If yes, how often are these reviews conducted?

☐ Quarterly ☐ Semi-annually ☐ Annually ☐ Biennially ☐ As needed

☐ Other (*explain*)

☐ N/A

11c. If yes, when was the last review conducted?

11d. If yes, does the review cover the following areas?

☐ All policies, procedures, practices, and documentation related to security

☐ Systems: hardware, software, operations systems, applications

☐ Security tools and reported security incidents

☐ User access methods - user identification, user authentication, account removal

☐ Password protocols: password aging, protection and encryption methods and standards

☐ Remote access procedures

☐ Other (*explain*)

☐ N/A

11e. If yes, which office/staff receives a report of the review results and findings, if any?

11f. What, if any, deficiencies were identified during the most recent review?

11g. Describe any identified deficiencies that still need to be addressed.

12. During the review period, did Internal Security staff verify that the state has policies and procedures to prohibit employees from providing services (e.g., processing unemployment claims, tax payments, overpayment transactions, etc.) for relatives and acquaintances?

Select Answer

13. During the review period, did the Internal Security staff verify that the state enforces the principle of separation of duties (e.g., making adjustments to claims, or tax functions and any handling of cash, etc.)?

Select Answer

14. During the review period, did Internal Security staff verify that the state has confidentiality agreements with all state, Federal, and private entities with which they share or exchange data?

Select Answer

14a. If yes, did they verify that the confidentiality agreements were up-to-date?

Select Answer

14b. Which office is the custodian of these agreements?

14c. Is there an established method available for these organizations to report data security issues to the agency?

Select Answer

15. During the review period did Internal Security staff verify the state policies and procedures for cancelling an individual's computer system access and email account?

Select Answer

16. During the review period did Internal Security staff verify the state policies and procedures, as appropriate, for restricting staff access to the premises upon separation from employment?

Select Answer

17. Does the Internal Security staff verify the state policies and procedures for cancelling computer access and email accounts and restricting access to the premises when contractors are terminated or their engagement with the agency ends?

Select Answer

SECTION 1: Comments

Document any issues that were identified when completing this section. This comment section may also be used to provide additional information relating to any specific question(s) in this section.

SECTION 2: Training

Managers/employees should possess and maintain a level of expertise that enables them to accomplish their assigned duties while ensuring the necessary level of security and confidentiality is maintained. Training systems should be sufficient to ensure that personnel understand and practice proper security procedures. When reviewing IS activities related to training systems, reviewers must consider formal training procedures, e.g., the training is conducted using an established schedule and using set guidelines. There should be procedures for identifying general and specific training needs and for delivering training as needed.

1. How is Internal Security staff trained?

2. What office is responsible for delivering this training?

3. Does the state have a "refresher" training plan to provide continuing training to Internal Security staff?

Select Answer

3a. If yes, how often is the continuing training conducted?

☐ Monthly ☐ Quarterly ☐ Annually ☐ On an as-needed basis

Question 3a check boxes continue on next page

☐ Other (*explain*)

4. How are UI staff members provided training on Internal Security matters? *(check all that apply)*

☐ IS training provided as part of new employee orientation
☐ IS training provided to UI staff annually
☐ IS training provided to UI staff on an as-needed basis
☐ Other (*explain*)

☐ N/A

5. Does the state offer "refresher" training on Internal Security matters to UI staff?

Select Answer

5a. If yes, how often is the continuing training conducted?

☐ Monthly ☐ Quarterly ☐ Annually ☐ On an as-needed basis
☐ Other (*explain*)

5b. Do internal security staff members participate in conducting this training?

Select Answer

SECTION 2: Comments

Document any issues that were identified when completing this section. This comment section may also be used to provide additional information relating to any specific question(s) in this section.

SECTION 3: Workload Analysis / Management Controls

The state's ability to assess and manage its integrity and security systems as well as safety procedures—particularly when a threat exists against agency data, resources, or personnel—is analyzed. Methods used to mitigate such threats should be reviewed for effectiveness after any incident. Reviewers will address the IS activities in promoting process-improvement initiatives aimed at improving response and resolution processes.

1. How many physical locations did the state have for UI operations during the review period?

2. How many of those locations were open to the public?

2a. During the review period, did the state encounter any security threats or incidents related to staff or property at any of the locations?

Select Answer

2b. For locations open to the public, has the state determined whether there is a need for security guards?

3. What measures does Internal Security take to identify potential vulnerabilities in its physical locations?

3a. During the review period, were any vulnerabilities identified that were not resolved?

Select Answer

3b. If yes, what issues were identified but not resolved? (*explain why not*)

4. What, if any, measures does Internal Security staff take to identify potential vulnerabilities in the state's computer systems, data handling, and storage methods?

4a. During the review period, were any vulnerabilities identified that were not resolved?

Select Answer

4b. If yes, what issues were identified but not resolved? (*explain why*)

5. During the review period, did Internal Security staff conduct any cross matches or investigations to prevent or identify incidences of internal fraud/abuse (e.g., matching agency employee addresses against addresses in UI claim records)?

Select Answer

5a. If yes, were any changes recommended as a result of those activities?

Select Answer

5b. If yes, what (if any) changes were recommended but not made? (*explain why*)

6. Does the state have procedures that ensure compliance with the required reporting of Internal Security activities and fraud cases investigated? (Reference UIPL No. 08 - 12 related to the ETA-227 Report)?
Select Answer

6a. Is the required reporting (i.e., ETA 227 Report) for Internal Security activities automated?
Select Answer

6b. During the review period, did the state UI agency report any overpayment activity due to employee fraud?
Select Answer

6c. During the review period, did the state fail to report any UI internal fraud case(s) on the ETA 227?
Select Answer

6d. If yes, explain.

6e. What unit or office is responsible for preparing the ETA 227 report, (specifically, for reporting cases of agency employee benefit fraud?

SECTION 3: Comments

Document any issues that were identified when completing this section. This comment section may also be used to provide additional information relating to any specific question(s) in this section.

SECTION 4: Information Technology (IT)

The state's IT systems must be tested routinely to ensure data security. The reviewer will assess the state's IS activities to verify the state's delivery of programming and technical support in a secure environment. Having a disaster recovery plan as well as contingency planning to implement emergency procedures with a short lead time is vital to continued operations under extreme conditions. IS staff should not be expected to duplicate efforts by the IT staff that help implement IT security controls, but IS staff can verify that these IT controls are in place.

1. What organization is responsible for the operation of the UI agency's computer system? *(check all that apply)*

- ☐ State UI agency
- ☐ Centralized state IT department
- ☐ Other (*explain*)

1a. If the state UI agency's computer system is part of a centralized state computer system, does the Internal Security manager/staff have any authority or responsibilities for IT systems security?

Select Answer

1b. If not, does the Internal Security staff have a way to provide input to management staff about system vulnerabilities that may have been detected or reported?

Select Answer

If the answer to questions 1a. and 1b. is *No*, skip to question 10. Questions 2-9 should be addressed if the UI agency has responsibility for IT operations, or if the response to Question 1a. or 1b. is *Yes*.

2. During the review period, did the Internal Security staff verify that regularly scheduled IT security tests for the state's IT systems and operations were conducted for UI IT programs and applications?

Select Answer

2a. Do Internal Security staff verify the frequency of tests that are conducted?

Select Answer

2b. If yes, what is the frequency of such tests?

☐ Quarterly ☐ Semi-annually ☐ Annually ☐ Biennially

☐ Other (*explain*)

☐ N/A

2c. If yes, which office receives a report of the test results?

2d. According to the Internal Security records, when was the last IT security test performed and what, if any, deficiencies were identified?

2e. If deficiencies or vulnerabilities were identified, did Internal Security staff verify that they have been corrected or are being addressed?

Select Answer

2f. If no, explain.

3. During the review period, did Internal Security staff verify that the state's IT security testing includes external security testing (from outside the organization's security perimeter) and Internal Security testing (from within the internal network)?

Select Answer

4. During the review period, did Internal Security staff verify the type of IT security testing the state conducts? If so, which of the following are addressed? (*check all that apply*)

- ☐ Overt security testing (performed with the knowledge and consent of IT staff)
- ☐ Covert security testing (taking an adversarial approach to testing without the knowledge and consent of IT staff)
- ☐ Other (*explain*)

5. During the review period, did Internal Security staff verify that the state's IT security testing included a documentation review to ensure the technical aspects of policies and procedures are current and comprehensive for the following areas? If so, which of the following are addressed? (*check all that apply*)

- ☐ Security policies
- ☐ Architectures
- ☐ Requirements
- ☐ Standard operating procedures
- ☐ System security plans
- ☐ Authorization agreements
- ☐ Memoranda of understanding
- ☐ Agreements for system interconnections
- ☐ Incident response plans

6. During the review period, did Internal Security staff verify that the state's IT security testing included all wired and wireless network functions to ensure security of data transmissions, including enforcement of encryption protocols?

Select Answer

7. During the review period, did Internal Security staff verify that the state conducted vulnerability scanning to identify hosts/host attributes and associated vulnerabilities?

Select Answer

8. During the review period, did Internal Security staff verify that the state's IT security testing included penetration testing (i.e., conducting real attacks using techniques most commonly used by attackers to identify vulnerabilities in applications, systems or networks)?

Select Answer

9. During the review period, did Internal Security staff verify that the state's IT security testing covered the following data handling areas? If so, which of the following are addressed? (*check all that apply*)

- ☐ Data collection
- ☐ Data storage
- ☐ Data transmission
- ☐ Data destruction

10. During the review period, did Internal Security staff verify that the agency's IT department enforced the following security procedures?

Select Answer

10a. If N/A, explain.

10b. If yes, indicate which of the following security procedures are addressed? *(check all that apply)*

- ☐ Building access
- ☐ Sign-in sheets for visitors
- ☐ Secure area for equipment, document storage, etc.

Question 10b check boxes continue on next page

- ☐ Documents that contain confidential information that are slated for destruction must be stored in locked containers
- ☐ Documents that contain confidential information must be shredded
- ☐ Manage user account, including identification, authentication, and account removal
- ☐ Password security, including aging, encryption methods and standards
- ☐ Other (*explain*)

11. During the review period, did Internal Security staff verify that the state creates an audit trail for UI transactions that contains the following? If so, which of the following are addressed? (*check all that apply*)

- ☐ Type of event
- ☐ Date/time the event occurred
- ☐ User ID associated with the event
- ☐ Program or Command used to initiate the event
- ☐ Other (*explain*)

- ☐ N/A

12. During the review period, did Internal Security staff verify that the state controlled staff access to confidential data through job duties, job titles, etc.?

Select Answer

12a. If N/A, explain.

13. During the review period, did Internal Security staff verify that the state maintained appropriate mechanisms for user authentication and authorization when using network access from inside and outside the organization?

Select Answer

13a. If N/A, explain.

14. If the state issues paper benefit warrants/checks, does Internal Security staff verify that the warrant stock is kept locked in a secure location?

Select Answer

14a. If yes, do they verify that access to the warrant stock is restricted to authorized personnel?

Select Answer

14b. If yes, do they verify that the restriction is enforced?

Select Answer

15. If the state uses a document management system (including electronic scanning), does Internal Security staff verify that controls are in place to safeguard the hard-copy documents that contain claimant and employer information from time of receipt until destruction?

Select Answer

16. During the review period, did Internal Security staff verify that some type of encryption is used for transmission of data outside the agency/state network?

Select Answer

17. During the review period, did Internal Security staff verify when the state's data encryption was last updated?

Select Answer

17a. If yes, how often is the state's data encryption updated?

17b. During the review period, did Internal Security staff verify that UI benefit programs used this data encryption, as needed?

Select Answer

17c. If yes, indicate which programs were included? (*check all that apply*)

- ☐ Benefits
- ☐ Benefit Payment Control
- ☐ Benefit Accuracy Measurement
- ☐ Appeals
- ☐ Other (*explain*)

- ☐ N/A

18. During the review period, did the Internal Security staff verify that the state enforced restrictions on email content, including confidential claimant and employer data?

Select Answer

19. During the review period, did Internal Security staff verify that the state conceals or truncates social security numbers on documents that are mailed through the U.S. Postal Service?

Select Answer

20. During the review period, did Internal Security staff verify that the state provided a secure access to individuals authorized to access the computer system remotely—for example via VPN, secured network, etc.?

Select Answer

21. During the review period did Internal Security staff verify that the computer system(s) has detection software to monitor for possible illegal activity based upon a user's id or IP address? (e.g., authorizing an inordinate number of payments, releasing large payment amounts, etc.)

Select Answer

22. During the review period, did Internal Security staff verify that the state generates a daily report of large benefit payments that are released?

Select Answer

22a. If yes, do Internal Security records indicate which office receives these reports?

23. During the review period, did Internal Security staff verify that the state's disaster recovery plan includes a full-system backup of its IT systems?

Select Answer

23a. If yes, what type of facility does the state use? (*check all that apply*)

- ☐ State-owned backup site
- ☐ Third-party vendor backup site

Question 23a check boxes continue on next page

☐ Other (*explain*)

☐ N/A

23b. If yes, has Internal Security staff verified that the state tested the plan?

Select Answer

23c. If yes, what was the date of the most recent test and results of the test?

24. During the review period, did Internal Security staff conduct security self-assessments that comply with NIST SP 800-53 and NIST SP 800-53A?

Select Answer

24a. If yes, when was the last self-assessment conducted?

SECTION 4: Comments

Document any issues that were identified when completing this section. This comment section may also be used to provide additional information relating to any specific question(s) in this section.

SECTION 5: Agency Staff Access & Communication

The role of Internal Security staff related to staff security and access to confidential data is reviewed. The role of Internal Security staff would generally also include receiving and acting on reported allegations of fraud/abuse.

1. During the review period did Internal Security staff have a role in setting and/or enforcing UI agency practices for the following security controls? (*check all that apply*)

- ☐ Configuration requirements for strong passwords
- ☐ Password expiration
- ☐ Remote access to confidential data
- ☐ Identity validation protocols
- ☐ Workstation security
- ☐ Personal Identification Number (PIN) reset requirements
- ☐ System access levels

2. Does the UI staff have access to appropriate management or Internal Security staff or other resources, as needed, to answer questions related to Internal Security procedures, policies, laws and regulations?

Select Answer

3. Does the UI staff have access to appropriate management or Internal Security staff or other staff to report suspected fraud or abuse?

Select Answer

3a. If no, explain.

SECTION 5: Comments

Document any issues that were identified when completing this section. This comment section may also be used to provide additional information relating to any specific question(s) in this section.

SECTION 6: Operational Efficiency / Resource Allocation

The reviewer will document how the state conducts security inspections, monitors IT system usage, and handles internal investigations regarding suspicious staff activities and potential breaches of security.

1. During the review period, did the Internal Security unit use automated systems for monitoring UI staff computer transactions?

Select Answer

1a. If yes, what automated processes are being used?

2. During the review period, did Internal Security staff receive reports of routine audits or tests of the IT system?

Select Answer

3. During the review period, did the Internal Security staff conduct regular security inspections of all UI facilities?

Select Answer

3a. If no, explain.

3b. If yes, how often are these inspections conducted?

☐ Quarterly ☐ Semi-annually ☐ Annually

☐ Other (*explain*)

☐ N/A

3c. Are written reports available after the security inspections?

Select Answer

3d. If yes, what office receives copies of the reports?

4. Does the Internal Security manager/staff lead internal investigations regarding suspicious staff activities and potential breaches of computer security?

Select Answer

4a. If no, how are these investigations handled?

5. During the review period, did the state conduct any business process analysis efforts to identify issues and recommend improvements of Internal Security processes to increase efficiency?

Select Answer

5a. If yes, what changes have been made and what was the result of those changes?

5b. If yes, what (if any) changes were recommended but not made? (*explain why not*)

SECTION 6: Comments

Document any issues that were identified when completing this section. This comment section may also be used to provide additional information relating to any specific question(s) in this section.

SECTION 7: Staffing

Staffing levels and organizational changes all can affect the state's ability to manage its Internal Security operations.

1. Does the state have a full-time Internal Security manager?

Select Answer

1a. If no, does a staff person(s) have Internal Security managerial or other duties in additional to other responsibilities?

Select Answer

1b. If N/A, explain.

2. What is the percentage of the state UI staff that is allotted (FTE allocation) for Internal Security?

_____ %

3. How many FTEs were budgeted for Internal Security during the review period? _____

4. How many FTEs were dedicated to Internal Security during the review period? _____

5. What security clearance is required for Internal Security staff?

6. What, if any, security procedures are conducted at termination of employment of Internal Security staff?

7. Does the agency's legal staff provide support for investigation of internal fraud related cases?

Select Answer

8. Does the agency's legal staff provide support for prosecution of internal fraud related cases?

Select Answer

9. During the review period, did personnel actions occur that impacted staffing levels of Internal Security program staff? (*check all that apply*)

- ☐ Hiring freeze(s)
- ☐ Temporary or permanent staff reductions
- ☐ Retirement/buyouts
- ☐ Other (*explain*)

9a. If the state implemented a hiring freeze, when did it occur and how long did it last?

9b. What negative impact, if any, did the hiring freeze have on Internal Security operations?

9c. If the state underwent temporary or permanent staff reductions, how many Internal Security program staff were affected, when did the action occur, and how long did it last?

9d. If the state experienced retirements in Internal Security or had a retirement buyout during the review period, provide the number of Internal Security staff that left due to retirement.

9e. What percentage of the overall Internal Security staff was impacted as a result of a temporary or permanent staff reduction and/or retirement? _____ %

9f. If the state experienced turnover, what percentage of the Internal Security positions remain vacant? _____ %

10. During the review period, did the state follow the Federal cost allocation principles if/when Internal Security staff reviewed other programs besides UI, ensuring costs were allocated by program?

Select Answer

SECTION 7: Comments

Document any issues that were identified when completing this section. This comment section may also be used to provide additional information relating to any specific question(s) in this section.

SECTION 8: Concluding Summary Comments for Internal Security

For the following sets of questions, consider the overall operations related to Internal Security. This is an opportunity to identify successful practices and/or any needed corrective action measures along with any other general comments or observations concerning this functional area of UI Benefits. Additional space for comments and reviewer notes is available on pages 43 and 44.

1. Provide any observations of good and/or exemplary performance in the state's Internal Security policies, procedures, or operations that would constitute successful practices to share with other states.

2. Document any issues detected in Internal Security that adversely affects the state's operations. Identify any corrective action measures that should be taken to improve the state's performance regarding any weaknesses identified.

3. Add any additional comments or observations regarding the state's performance or operations in this area that have not been addressed elsewhere and should be noted.

Additional Comments and Reviewer Notes:

Reviewer Information:

REVIEWER

Name:	
Title:	
Email:	
Phone No.:	

ADDITIONAL REVIEW TEAM MEMBER

Name:	
Title:	
Email:	
Phone No.:	