EMPLOYMENT AND TRAINING ADMINISTRATION ADVISORY SYSTEM U.S. DEPARTMENT OF LABOR Washington, D.C. 20210	CLASSIFICATION UI
	CORRESPONDENCE SYMBOL OWS/DPM
	DATE March 4, 2009

ADVISORY: UNEMPLOYMENT INSURANCE PROGRAM LETTER NO. 15-09

TO: STATE WORKFORCE AGENCIES

FROM: DOUGLAS F. SMALL Douglas F. Small
Deputy Assistant Secretary

SUBJECT: Proposed Changes to Employment and Training (ET) Handbook 336, 18th Edition: "Unemployment Insurance (UI) State Quality Service Plan Planning (SQSP) and Reporting Guidelines"

1. **Purpose**. To provide an opportunity for comment on proposed changes to the Assurance of Disaster Recovery Capability and the Assurance of Automated Information Systems Security sections within ET Handbook 336.

2. **References**. ET Handbook No. 336, 18th Edition, "UI SQSP and Reporting Guidelines".

3. **Background**. In FY 2008, the Office of Inspector General (OIG) conducted an audit to determine if the Employment & Training Administration (ETA) provides sufficient oversight of the State Workforce Agencies' (SWAs) Information Technology (IT) contingency planning for the UI program in order to minimize service disruption in the event of a disaster or other situations that may disrupt normal operations. The summary of findings of this OIG audit (OIG Report No. 23-08-004-03-315 issued on September 29, 2008) include: (1) SWAs lack IT contingency plans that can ensure adequate disaster-response capability; (2) ETA has not fully carried out its leadership responsibilities in providing oversight and targeted guidance to the SWAs regarding expectations of an IT disaster-recovery capability.

4. **Additional Guidance**. In response to the audit findings, ETA is providing specific guidance on the requirements of IT security necessary for a viable SWA IT system security program.

   This guidance is incorporated in the following areas of the SQSP:
   - Chapter I, Section VII-H, "Assurance of Contingency Planning", pages I-19 – 20. The title of this assurance is changed from "Disaster Recovery Capability" to "Contingency Planning Capability", since Contingency Planning means to prepare for any uncertain future disruptions, including disasters. The assurance provides guidelines for UI Contingency Planning controls.

RESCISSIONS None	EXPIRATION DATE March 4, 2010

- Chapter I, Section VII-J, "Assurance of Automated Information Systems Security", pages I-20 – 21. The assurance is modified to provide guidelines for having adequate UI information security controls.
- Appendix I, "Planning Forms and Formats". The State Plan Narrative Outline, Section H, "Assurances" is modified for SWAs to provide the dates when their IT Contingency Plan, System Security Plan, and Risk Assessment were implemented, tested, and reviewed/updated.
- Appendix IV, "Information Technology Security Guide". This new appendix provides overview on IT Contingency Planning, Risk Assessment, and System Security Planning security controls.

5. **Action Required**. SWA administrators are requested to review the recommended changes and within 45 days of receiving this advisory, provide any comments electronically to patel.jagruti@dol.gov or by mail to the attention of:

   U.S. Department of Labor
   Office of Workforce Security
   Division of Performance Management
   200 Constitution Avenue, NW
   Washington, DC 20210
   Attention: Jagruti Patel, Room S-4231

   Please be aware that all mail sent via United States Postal Service is irradiated which can delay receipt of comments.

6. **Inquiries**. All inquiries should be directed to the appropriate Regional Office.

7. **Attachments**. ET Handbook 336, 18th Edition, Chapter I
   Appendix I: Planning Forms and Formats
   Appendix IV: Information Technology Security Guidelines

ET HANDBOOK NO. 336

18th Edition

UNEMPLOYMENT INSURANCE

STATE QUALITY SERVICE PLAN

PLANNING AND REPORTING GUIDELINES

TABLE OF CONTENTS

ET HANDBOOK NO. 336

18th Edition

INTRODUCTION

ET HANDBOOK NO. 336
INTRODUCTION

The SQSP Handbook provides guidelines for the completion and submittal of the State Quality Service Plan (referred to as the SQSP or the State Plan) for the Unemployment Insurance (UI) program and the reports and data elements to be used for financial reporting of state UI program activities.

A. Background

The SQSP represents an approach to the UI performance management and planning process that allows for an exchange of information between the Federal and state partners to enhance the ability of the program to reflect their joint commitment to performance excellence and client centered services. The statutory basis for the SQSP is Title III, Section 302 of the Social Security Act, which authorizes the Secretary of Labor to provide funds to administer the UI program and Sections 303(a)(8) and (9) which govern the expenditure of those funds. Plans are prepared annually since funds for UI operations are appropriated each year. The Department of Labor's (DOL's) annual budget request for state UI operations contains workload assumptions for which the state must plan in order for the Secretary to carry out her responsibilities under Section 303(a)(1) of the Social Security Act, which ensures full payment of unemployment compensation when due. DOL issues financial planning targets based on the budget request. States make plans based on such assumptions and targets via this mechanism.

As part of UI Performs, a comprehensive performance management system for the UI program, the SQSP is the principal vehicle that the state UI programs use to plan, record and manage improvement efforts as they strive for excellence in service. UI Performs was officially announced in August 1995. Unemployment Insurance Program Letter (UIPL) No. 41-95, dated August 24, 1995, outlined a construct for a comprehensive performance management system based on the following:

- a significantly improved data collection infrastructure that provides more management information more frequently;
- performance measures that include national core criterioned measures and a menu of non-criterioned measures for states to use in measuring and improving their program performance;
- a dynamic planning process that is state focused; and
- a goal of continuous improvement with responsibility shared by both state and Federal partners.

UIPL No. 14-05, dated February 18, 2005, and UIPL No. 14-05, Change I, dated October 12, 2005, outlined changes to UI Performs as a result of a review of the system. The changes streamlined UI Performs by:

- reducing the number of measures for which performance criteria are set to a few core measures;

- recognizing remaining measures as management information with no set performance criteria; and

- streamlining the SQSP narrative.

The focus of this Handbook is to provide specific guidance regarding the SQSP, which is the implementing document for the performance management system described above. The State Plan is an integral part of UI Performs. It is, therefore, critical to understand the broader context in which the State Plan is developed.

1. The Continuous Improvement Cycle. UI Performs embraces the continuous improvement cycle advocated by quality practitioners which is commonly known as the "Plan-Do-Check-Act" cycle. It also is referred to as a "closed loop" continuous improvement cycle. It incorporates a strategic planning process of identifying priorities; ongoing collection and monitoring of valid data to measure performance; identification of areas of potential improvement; and development of specific action steps to improve performance, followed by use of available data to determine whether the action steps are successful. The cycle continues indefinitely with the opportunity at any point to reassess priorities, performance, and action that can improve performance.

2. The Performance Measurement System. The system includes both criterioned (Core Measures) and non criterioned (Management Information) measures. The Core Measures are indicators of how well State Workforce Agencies (SWAs) perform critical activities. Core Measures include Tax, Benefits, Appeals, and Reemployment measures. Management Information Measures provide additional insight into UI program operations.

3. The Planning Process. UI Performs emphasizes joint responsibility between states and the Employment and Training Administration (ETA) for setting priorities and responding to performance information both annually and on an ongoing basis. The relationship between the states and ETA will include the following shared responsibilities:

- continued tracking and analysis of performance data;

- identification of Federal and state priorities;

- development of planning directions;

- negotiation to determine improvement levels; and

- development and implementation of strategies to maintain acceptable performance.

Accomplishing these ongoing responsibilities requires an interactive and consultative process between states and ETA.

4. <u>The State Quality Service Plan</u>. The State Plan is intended to be a dynamic document that states can use as a management tool - much like a business plan - not only to ensure strong program performance, but also to guide key management decisions, such as where to focus resources. It should focus the states' efforts to ensure well-balanced performance across the range of UI activities. The State Plan also is designed to be flexible to accommodate, among other things, multi-year planning and significant changes in circumstances during the planning cycle. Although it will be developed in cooperation with the Federal partner, the State Plan is state-focused. The Federal role in the process is designed to be constructive and supportive.

Operationally, the State Plan also serves as the programmatic plan portion of the grant document through which states receive Federal UI administrative funding. To serve this purpose, the state is required to submit budget worksheets and various assurances required in the Federal grant agreement.

The annual State Plan is designed to provide the structure for recording the following kinds of information:

- responses to federally identified priorities;
- performance assessment information;
- short and long term strategies for achieving performance targets;
- corrective action plans (CAPs) for failure to meet Core performance criteria; and
- state strategies for evaluating customer satisfaction and gaining customer input to promote performance excellence.

States are required to submit the SQSP electronically and should contact the RO SQSP Coordinator prior to submittal to coordinate specific details.

B. <u>Relationship/Coordination with Other Plans</u>

The UI program does not stand alone. It is the wage replacement component of an overarching effort to return a worker to suitable work. As such, the SQSP should be developed in concert with other plans which also address the same customer (such as the Wagner-Peyser and Workforce Investment Act plans) to insure a coordinated effort and minimal obstacles for the client in moving from program to program. This coordination will most likely be apparent in the State Plan Narrative portion of the SQSP.

C. Partnership Principles

The three following principles form the basis for carrying out Federal and state responsibilities under UI Performs and the SQSP planning process:

- Basing the federal-state relationship on mutual trust and respect will improve the UI system and its service to the American public;

- Working as equal partners with complementary roles will improve the UI system's quality of service and its integrity; and

- By setting high standards and goals and working together as a team, the system will be strengthened and the entire nation will benefit.

The following are examples of the actions and attitudes which are consistent with these principles:

- Fostering a win-win relationship; advocating for and supporting one another;
- Sharing credit, celebrating successes;
- Being willing to acknowledge the existence of problems, and focus on fixing them instead of placing blame;
- Mutually accepting responsibility for resolving problems and overcoming deficiencies;
- Where there are differences between partners—
    - Trying to resolve disputes equitably and fairly, being willing to compromise to achieve consensus; and
    - Seeking early, informal resolution;
- Fostering open, personal communication;
- Clearly defining partner roles, rights and responsibilities;
- Engaging in joint planning and influencing one another's priorities;
- Promoting innovation and creativity;
- Jointly seeking input from customers;
- Sharing information and resources;
- Recognizing the role and importance of other players at the state and national levels;
- Asserting positive and friendly influence on partners to improve performance; and
- Periodically reviewing the principles and roles.

D. Planning Considerations

This section provides information for states to use in developing their SQSPs.

1. State Agency Resource Planning Targets for UI.

a. Financial Guidelines. States will prepare SQSPs according to financial guidelines transmitted with target funding levels provided by the ROs.

b. Final Allocations. Final allocations may contain increases or decreases from the target funding level, which may require some revisions to submitted or approved State Plans.

2. State Flexibility. States have the flexibility to use the total dollars approved by ETA among the various UI program categories as they deem appropriate. However, for purposes of determining certification of above-base funding for workload above the base, the base staff year levels for claims activities as allocated by ETA will be used. Note that this flexibility does not include special allocations which are identified on a case-by-case basis.

3. State Financial Reporting System. ETA does not prescribe the use of any specific accounting and reporting system by the states. States are free to use any accounting system that meets the standards for state grantee financial management systems prescribed by Federal Regulations at 29 CFR 97.20. However, states must be able to report UI financial information in the form and detail described in Chapter II of this Handbook.

E. OMB Approval

The Office of Management and Budget (OMB) has approved ET Handbook No. 336 for use through June 30, 2008, in accordance with the Paperwork Reduction Act of 1995, under OMB No.1205-0132.

Persons are not required to respond to this collection of information unless it displays a currently valid OMB control number. Respondents' obligation to reply to these reporting requirements is mandatory (20 CFR 97.42). Public reporting burden for this collection of information is estimated to average 3 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to the U.S. Department of Labor, Office of Workforce Security, Room S4231, Washington, D.C. 20210 (Paperwork Reduction Project 1205-0132.)

ET HANDBOOK NO. 336

18th Edition

CHAPTER I - PLANNING

ET HANDBOOK NO. 336
CHAPTER I - PLANNING

I. INTRODUCTION

Chapter I of the SQSP Handbook provides guidelines for the completion and submittal of the state SQSP for the UI program and instructions for the SBR process for extraordinary funding.

II. OVERVIEW OF PROCESS

While the SQSP process is ongoing throughout the year, the formal plan submittal occurs once each year in conjunction with the funding cycle and utilizes the following process:

A. Schedule. The significant activities and dates relating to the submittal and subsequent approval of the annual SQSP are estimated to be:

Activity	Approximate Date
National Office (NO) issues Annual Call Memo	Late May
ROs send financial guidelines and planning targets to states States submit SF 424, 424A (as necessary), 424B	Late June At RO request or with SQSP at the latest
States electronically submit the SQSP to ROs.	August/September per RO requirement
ROs notify states of SQSP approval	Late September
ROs notify NO of approved SQSPs	No later than September 25
NO Grant Officer transmits UI Annual Funding Agreement to states for signature	Mid September
Execution of UI Annual Funding Agreement with first funding increment	Early October
States submit UI-1 (UI Staff Hours)	October 1

B. Annual Call Memorandum. Each year, formal SQSP submittal will be initiated with a UIPL (Call Memo). States should carefully review the annual Call Memo. This memo will specify the dates relevant to the SQSP process for the approaching fiscal year; summarize Federal Program Emphasis for the year; and identify any special planning requirements in effect for the fiscal year. It also will explain opportunities for increased, targeted funding made available on an annual basis in the President's budget if such opportunities exist.

1. Federal Program Emphasis. The Federal Program Emphasis summarizes the primary areas in which the Federal partner will focus attention and resources for the planning year. The six-year DOL Strategic Plan and the annual DOL Performance Budget form the basis for the Federal Program Emphasis. Required by Congress under the Government Performance and Results Act (GPRA), the Federal plans are an integral part of the Federal budget process. They establish program performance goals and outcomes and identify strategies and performance objectives to attain them. Accordingly, states will want to review the current versions of these planning documents before developing their annual SQSPs. These documents may be found under the "Budget, Performance & Planning" section of the DOL webpage, http://www.dol.gov/dol/aboutdol/main.htm.

2. Special Planning Requirements. Any special planning considerations or requirements for the planning year will be identified in the Call Memo.

C. Financial Guidelines and Planning Targets. Each year the ROs provide preliminary allocations, any special financial instructions for the year, and the deadline for plan submission.

D. Performance Measures. UI Performs incorporates two types of performance measures (Core and Management Information). States are encouraged to routinely monitor performance data on both Core and Management Information Measures and to achieve continuous improvement in overall unemployment compensation performance by establishing improvement targets for as many measures as possible.

1. Core (Criterioned) Measures. Core Measures are those measures that are considered to be critical indicators of the overall performance of the program. If acceptable levels of performance (ALPs) for them are not met, it signals fundamental impairment in program operations, and triggers corrective action planning. Core Measures are comparable among SWAs and have ALP criteria assigned to them. SWAs are expected to submit corrective action plans (CAPs) if performance falls below the ALPs. See Appendix III, Performance Measures, for a list of the Core Measures and associated criteria.

2. Management Information (Non-Criterioned) Measures. Management Information Measures, like Core Measures, are routinely reported by the state using Federal definitions found in ETA Handbook 401, but, with the exception of the Secretary's Standards[1], have no nationally established Federal criteria for determining the adequacy of the state's performance. Some Management Information Measures are subsets or components of data included in Core Measures, such as timeliness of Unemployment Compensation for ex-Service Members (UCX) benefit payments, those claiming benefits on an interstate basis, or the individual Tax Performance System (TPS) components of the tax quality measure. These data alert state and Federal managers to performance issues that could result in lower

[1] The criteria for measures of Secretary's Standards are currently in regulation and will remain in effect until the regulation is replaced.

performance on Core Measures and are useful for performance analysis. However, as provided in Federal UI law, the Secretary of Labor retains full authority to address cases of conspicuously poor performance in a state.

E. Performance Assessment

1. Continuous Assessment. In the SQSP process, both the Federal partner and the state will routinely access performance data to monitor program performance and initiate corrective action when warranted. CAPs are plans developed in response to data showing state performance below the ALPs established for Core Measures. Also, if a state's performance in one or more Management Information Measures is so conspicuously poor that a state's compliance with Federal law requirements is in question, DOL would require corrective action. Although performance may be viewed at specific points in time (e.g. monthly, quarterly, annually, etc.), each assessment reviews performance over time and focuses not only on performance for the period in question, but also on the trend of performance over the period reviewed (e.g., was performance declining or improving, sustained or erratic).

2. Annual Assessment. An annual assessment will augment the ongoing continuous improvement process, and will form the basis for corrective action planning for the SQSP. This annual assessment will utilize the most recent 12 months of performance data. For data reported monthly or quarterly, the assessment will include the 12 months ending March 31 of each year. For data reported annually, the assessment will be based on data reported for the most recent complete calendar year (or other full 12-month period, per reporting requirements).

ETA will make all relevant data available to the states for SQSP purposes, but states have continuous direct access to the data resident on the state SUN computer system, or through the Office of Workforce Security website at http://www.ows.doleta.gov. Subsequent performance data that become available during the plan development period (e.g., April, May, June data) should be utilized to refine plans before final submission and approval.

3. State/Regional Negotiations. Before the annual SQSP is signed, states and regional administrators must agree on the specific areas for which the state will submit CAPs in the SQSP. These negotiations encompass performance below the established ALPs for Core Measures. CAPs are expected to be submitted if performance is unsatisfactory and an effective plan is not already in place for Core Measures or for improper administration of BAM or BPC activities.

F. State Plan Preparation. States must prepare and transmit an annual SQSP in accordance with the instructions in this Handbook and in the annual SQSP Call Memo. The SQSP, with its CAPs and Narratives, is the state's formal plan and schedule for improving performance. An

acceptable SQSP must have state management approval and must authorize the resources necessary to conduct the actions planned.

G. SQSP Review and Approval. ROs shall review SQSPs for completeness, and to make sure that they are in accordance with the instructions and that they reflect negotiated agreements. This review may result in the RO initiating additional discussion or obtaining clarification. A plan that the regional administrator deems unsatisfactory, i.e., failing to meet the requirements identified in this Handbook, shall be returned to the state for revision without approval.

III. CONTENT AND SUBMITTAL OF SQSP

A. Content of the SQSP. The Annual SQSP must contain a transmittal letter, State Plan Narrative, Corrective Action Plans, Budget Worksheets, Organizational Chart, and Signature Page. Each element/document is described below.

1. Transmittal Letter. State administrators must prepare and send a cover letter to the appropriate RO transmitting all the required SQSP documents.

2. State Plan Narrative. The State Plan Narrative is a vital element of the SQSP that provides a vehicle for sharing with the Federal partner state-specific efforts that affect the administration of the UI Program. The State Plan Narrative allows the state to designate elements on which it intends to focus in the coming year, and describe how those elements are incorporated into a cohesive and comprehensive plan for administration of the UI Program.

Section IV, State Plan Narrative, provides a detailed description and instructions for the format and content of the Narrative. An outline of the Narrative is contained in Appendix I.

3. Corrective Action Plans. States are expected to complete and submit CAPs for the following:

a. Performance that did not meet ALPs for Core Measures for the annual measurement period and remains uncorrected prior to the preparation of the SQSP; and

b. Failure to administer Benefits Accuracy Measurement (BAM) or Benefit Payment Control (BPC) activities properly resulting in an overpayment detection rate above 95%.

The CAP format is found in Appendix I.

4. Budget Worksheets. States must complete required budget forms and plan for administration based on projected allocations received from the Federal partner.

All states must complete Worksheet UI-1 and SF 424, and SF 424B. States must complete the SF 424A only if they vary the quarterly distribution of base claims activity staff years.

States must submit the Worksheets UI-1 by October 1 of each year separately from the SQSP submittal. States must include SF 424, SF 424A (if necessary), and SF 424B in the SQSP submittal, if not submitted previously in August at the RO's request.

Completion instructions and facsimiles of these forms are located in Appendix I.

5. Organizational Chart. The state must submit a new organizational chart if its organizational structure has changed in the last year. This organization chart must conform to the requirement for delivery of service through public employment offices, or such other designated providers as the Secretary may authorize; show the state's configuration from the Governor of the state down to the point of Employment Service and UI customer service delivery; and provide sufficient detail to show each organizational unit involved and the title of the unit manager.

6. Signature Page. State administrators must sign and date the Signature Page located in Appendix I. By signing the Signature Page, the state administrator certifies that the state will comply with all the assurances contained in the SQSP guidelines. Therefore, it is not necessary for states to include written assurances with their SQSP submittals.

B. Submittal of the SQSP. States must submit the SQSP to their RO by the date the Region has specified. The SQSP Content Checklist located at the end of this chapter shows all the documents that comprise the entire SQSP. Each state must include a completed Checklist to insure that those documents appropriate to its plan are submitted, and to minimize the potential for a delay in the approval and funding process. Electronic transmittal of the SQSP is required in a format specified by the RO. States must provide their RO with an original SQSP signature page; however, states may submit the signature page electronically, if state law permits.

IV. STATE PLAN NARRATIVE

Of necessity, states engage in an annual planning process and set priorities for the coming year. The State Plan Narrative provides a vehicle for sharing the results of that process with the Federal partner. In addition, it provides an opportunity to report on the integration and coordination with other internal and external plans which serve the same client.

A. Description. The State Plan Narrative consists of a description of major planning elements the state plans to focus on during the fiscal year. The Narrative should be concise, as a more

detailed discussion with RO staff already may have occurred, or may occur as a follow-up. However, in order to develop RO and NO support for its objectives, the state needs to provide a minimum amount of information relative to the categories defined in a format that allows for follow-up and tracking.

Below are the components to be included in the State Plan Narrative. These components should be addressed in a manner that best describes the state's direction and plans:

- The strategic direction the state has adopted to ensure continuous program improvement, including the basis for the state's choice of areas to emphasize in the planning year, and the actions planned to support performance improvement during the year;

- Assessment of program performance in prior program years;

- Responses to the Secretary of Labor's areas of program emphasis;

- State performance in comparison to the GPRA goals for the U.S. Department of Labor;

- Actions planned to correct the following types of deficiencies regarding program reviews and reporting requirements including:

    - **Program Review Deficiencies.** Uncorrected deficiencies identified in program reviews conducted by the state, or ETA. Examples of such program reviews include Federal programs (Unemployment Insurance for Federal Employees (UCFE), UCX, etc.), BPC, Internal Security, UI Automation Support Account (UIASA) monitoring, and State Audits.

    - **Reporting Deficiencies.** Consistent failure to timely or accurately submit any federally-required reports.

    - **BAM Requirement Deficiencies.** Failure to meet Federal requirements identified in BAM which remain uncorrected. The RO will notify the states when, based on the annual BAM administrative determination, states must describe in the narrative the steps to be taken for correcting the problems in question and provide projected dates for the completion of each step. The BAM requirements are contained at 20 CFR Part 602 and in the Benefits Accuracy Measurement State Operations Handbook (ET Handbook No. 395).

    - **TPS Requirement Deficiencies.** Failure to fully complete all parts of TPS as required in ET Handbook No. 407, Revenue Quality Control, must be addressed in the narrative.

- **Data Validation Deficiencies.** Failure to fully complete all parts of Data Validation must be addressed in the narrative. In addition, states must address Data Validation population failures.

- Information on the state strategy for evaluating customer satisfaction and including customer input to promote continuous improvement; (optional)

- State's specific requests for technical assistance from the Federal partner; and

- Information on the state's approach to maintaining solvency of the state's unemployment fund.

B. Format and Instructions. The State Plan Narrative outline is contained in Appendix I. The format is intended to provide states flexibility in conveying their overall direction and emphasis while providing for electronic transmittal. States are requested to address each area of the outline, including entering N/A (Not Applicable) where appropriate.

V. CORRECTIVE ACTIONS PLANS

A. Description. These plans consist of a narrative section and milestone summary completed and submitted in the format in Appendix I. Each CAP must be titled as listed in Appendix III.

States are expected to complete and submit CAPs for the following:

1. Performance Deficiencies. Performance that did not meet ALPs established for Core Measures for the annual measurement period and remains uncorrected prior to the preparation of the SQSP is considered deficient.

In many instances, performance deficiencies will have been identified prior to the annual assessment with a CAP already in existence to remedy the problem. Accordingly, the SQSP will not, in many instances, result in the development of a new CAP, unless progress on an existing plan is not on target or does not adequately address milestones for the plan year. Such CAPs (i.e., adequate, existing CAPs) will be incorporated into the SQSP submission along with revised CAPs and CAPs addressing newly identified deficiencies.

2. Improper Administration of BAM or BPC Activities. If improper administration of BAM or BPC activities results in an overpayment detection rate above 95%, the state must submit a CAP designed to produce valid data for the Overpayment Detection Measure. A CAP is required because the administration of BAM and BPC has a direct bearing on this Core Measure.

3. Conspicuously Poor Performance. If a state's performance in one or more Management Information Measures is so conspicuously poor that a state's compliance with Federal law requirements is in question, DOL would require corrective action.

B. CAP Format Completion. When developing a CAP, states should complete all data elements in the prescribed format. A sample format is contained in Appendix I.

1. Summary. This section must:

a. Explain the reason(s) for the deficiency;
b. Provide a brief description of the actions/activities which will be undertaken to improve performance.
c. If a plan was in place the previous fiscal year and performance has not improved as specified in the plan, provide an explanation of why the actions contained in that plan were not successful in improving performance, and an explanation of why the actions now specified are expected to be more successful.
d. Provide a brief description of plans for monitoring and assessing accomplishment of planned actions and for controlling quality after achieving performance goals.

If the desired improvement will not be accomplished by the end of the fiscal year for which the plan is submitted, the state should provide a multi-year plan which must include: (1) an estimate of where performance will be at the end of the fiscal year; (2) major actions remaining to be taken in subsequent fiscal years; and (3) a projection as to when the performance goal will be achieved.

2. Milestones. The state must list both specific milestones (key corrective action or improvement activities) and the completion date for each milestone in the space provided. Milestones must be established for each element of the state's corrective action plan and be of sufficient number and frequency to facilitate state and regional plan oversight and assessment during the fiscal year. It is anticipated that one or more milestones for each quarter would permit such progress tracking and assessment during the fiscal year through state and regional follow-up schedules.

NOTE. Milestones should be concise and should specify key actions to be accomplished throughout the planning year to implement the state's proposals for achieving its corrective action goals. States also may wish to identify performance milestones that reflect the performance level they anticipate will result from completion of planned activities.

3. Assembly. CAPs must use the identical labels and be arrayed in the same order in which they appear in the lists of Measures (see Appendix III).

VI. BUDGET WORKSHEETS AND INSTRUCTIONS

This section contains instructions states will need to follow to prepare resource requests for administering the UI program during the Fiscal Year. Budget worksheets are in Appendix I. Only two UI program operation worksheets (UI-1 and SF 424) are required. State agencies must prepare and submit the UI-1 (via Unemployment Insurance Required Reports (UIRR)) for staff hour estimates, and the SF 424 for base level planning and supplemental grant requests.

A. Worksheet UI-1, UI Staff Hours. A facsimile of Worksheet UI-1 and associated form completion instructions are found in Appendix I. These data are required for the development of annual base planning targets. The UI-1 worksheet is due by submission via the UIRR to the National Office (Attn.: Office of Workforce Security, Division of Fiscal and Actuarial Services) by October 1 of each year.

B. SF 424, Application for Federal Assistance. The regulation at 29 CFR 97.10 requires the use of the OMB Standard Form (SF) 424, Application for Federal Assistance, or other forms approved by OMB under the Paperwork Reduction Act of 1995, for an application for grant funds by state grantees. ETA requires that states use the SF 424 for submitting applications for UI base grants and SBRs. The SF 424 must be filled out according to its instructions.

1. Procedures for Submission. States must submit a separate SF 424 and SF 424B for each request for base funding and each SBR. A separate SF 424A also may be required as described in sub-paragraph 2.b. below. In addition, states which submit SBRs must provide supporting justification and documentation. SF 424s are due as requested, or with the SQSP at the latest, for base grants and throughout the year as necessary for SBRs.

2. Form Completion Instructions. States must follow the standard instructions in completing SFs 424, 424A and 424B; however, states are not required to complete all items on the SF 424 and 424A. A facsimile of these forms and completion instructions are found in Appendix I. The following are specific guidelines for completing SFs 424 and 424A.

a. SF 424. States are not required to complete Items 3, 4, 9, 12, and 14 for base grants and SBRs. States must complete the remaining items. In Item 8, all SBRs are considered to be revisions. In Item 12, the title of the project must refer to either the base grant or SBR title and number. SBRs must be numbered sequentially within the fiscal year, e.g., 00-1, 00-2, etc.

b. SF 424A. States must complete Items 1, 6, and 16 for SBRs. States are not required to complete this form for base grants, unless they vary the number of base

claims activity staff years paid by quarter; states that do so must show the quarterly distribution in Item 23 (Remarks).

C. Supplemental Budget Requests (SBRs). ETA may on occasion award supplemental funds for specific items not funded in the base allocations.

1. Allowable/Unallowable Costs

a. Allowable Costs. States may submit SBRs only for one-time costs that are not a part of base or above base. SBR funds may be used only for the purposes identified in the SBR and/or any modifications to the original agreement approved by ETA.

b. Unallowable Costs. SBR funds may not be used for ongoing costs, such as maintenance of software and hardware, or ongoing communications costs. In addition, SBRs may not be used to pay for salary increases, even when these increases are caused by a law change.

2. Guidelines for Preparing SBR Supporting Documentation. ETA will evaluate and approve all SBRs on the basis of supporting documentation and the justification provided. Insufficient justification may delay processing and result in partial or total disapproval of the SBR.

a. Supporting Documentation. SBRs may address a variety of projects whose scope cannot be fully anticipated. At a minimum, the SBR supporting documentation must contain the following five elements; however, these guidelines will not perfectly fit every SBR. States should use them as a starting point.

1) Summary. The SBR should contain a summary that explains what the funds will accomplish. It should identify major capital expenditures, including hardware, software, and telecommunications equipment; staff in excess of base staff; contract staff; and other purchases. It should also state what the final product or results will be when the funds have been expended.

2) Commitment to Complete Project. ETA cannot assure the availability of future Federal supplemental funds. Applicants must agree to continue efforts to complete the SBR project, and to supply any additional funds necessary to complete the project in a timely manner. This assurance is necessary to ensure that projects begun with Federal funds are not abandoned due to a lack of additional Federal funding.

3) Schedule. If the project activities have not been completed, the SBR must include a projected schedule. The schedule should provide the projected dates for significant activities from start to completion.

4) Amount of Funding Requested. The total dollar amount of the SBR must be included. The costs of specific program modules or tasks must also be listed.

5) Description of the Proposed Fund Usage. The SBR must contain a full description of how the funds are to be used and why the proposed expenditures represent the best use of funds for the state. For each specific program module or task, the SBR must include costs for:

(a) Staff. The request must identify both one-time state staff needs (in excess of base staff) and contract staff needs. Staff needs must include the type of position (e.g., program analysts), the expected number of staff hours, and the projected hourly cost per position.

(1) State Staff. Any staff costs are allowable only for additional staff, not staff previously funded by the state's base grant. Costs incurred by regular state staff assigned to the project on a temporary basis may not be funded by the SBR unless those positions are "back-filled." The request may include costs for staff that conduct training; however, personal services (PS) and personal benefit (PB) costs for staff attending training are not allowable unless those positions are back-filled. Unless otherwise justified, regular, Administrative Staff and Technical Services (AS&T), and above base staff year costs must be based on the state PS and PB rate approved for the current year's UI grant. If not itemized in the SBR, standard add-on costs for support and AS&T staff must be based on the rates approved for the current year's base allocation.

(2) Contractor Staff. For contract staff, the state must supply documentation including the estimated positions and hours, and the anticipated costs. States electing to negotiate with the Information Technology Support Center (ITSC) or other available sources for technical assistance must supply the same information normally requested for all contract staff, including the type of position, the expected staff hours, and the costs.

(b) Non-Personal Services (NPS). States may identify itemized one-time state NPS needs or may calculate staff-related NPS costs by formula. If not itemized in the SBR, staff-related NPS costs (excluding data processing and other needs) must be based on the rates approved for the current year's base allocation.

(1) Hardware, Software, and Telecommunications Equipment. This section must include any hardware, software, and/or telecommunications

equipment purchases that are a part of the request. Descriptions must show that the sizing and capabilities of the proposed purchases are appropriate for the state. States that receive SBR funds for specific items, and subsequently determine that other items are more suitable, may substitute those items if they submit an amendment to the SBR documenting the appropriateness of the purchase, and ETA approves the substitution. Substitutions must be in line with the overall goals of the project.

SBRs sometimes include requests for items covered under the definition of automation acquisition in Chapter II. The obligation and expenditure periods for these funds are longer than the periods for regular UI base and above base funds. States must clearly identify automation acquisition items in the SBR.

(2) Travel. The request may include NPS travel costs; however, PS and PB costs for staff while on travel are not allowable.

(3) Other. The request may include one-time costs for other activities, not identified above, anticipated to be obtained from vendors, such as telephone companies, Internet service providers, and telecommunications providers.

b. Additional Required Items for Law Change SBRs. SBRs for law changes must contain the following information:

1) The specific bill number of enactment, and effective date of law change.

2) Relevant provisions as an attachment.

3) Costs per legislative provision and a narrative explaining why costs were or will be incurred for each provision, e.g., implementing tax rate changes; increasing the maximum benefit amount; or creating an alternative base period.

4) If a legislative provision benefits both UI and non-UI activities, the SBR must contain a statement certifying that the request is consistent with the state's approved cost allocation plan and is only for costs which, under Federal law, may be funded from UI grants.

c. Supplementary Items. Some SBRs are for large-scale, complex projects that may be accomplished over a period of years. The following items are not required, but would be helpful in the SBR evaluation process:

1) Use of Technology. If applicable, the request should describe how the state will use technology in this project**,** including the technical appropriateness of the

hardware, software, and/or telecommunications equipment for integration with the state's current operating systems**.**

2) Strategic Design. The SBR should include a description of the strategic design of the project as evidence of a well-thought-out analysis of operations.

3) Measurable Improvements Expected in UI Operations. The request should identify the areas in which services could be improved through implementation of the proposed project. Measurable improvements may include accomplishing necessary work using fewer steps, doing work more quickly, incorporating work steps which are not currently accomplished, or reducing the amount of error which presently occurs in the work product.

4) Supporting Materials. States may attach any additional materials which they believe will enhance the content of the SBR.

VII. ASSURANCES

The State administrator, by signing the SQSP Signature Page, certifies that the state will comply with the following assurances, and that the state will institute plans or measures to comply with the following requirements. A facsimile of the Signature Page appears in Appendix I. The assurances are identified and explained in Paragraphs A. through K. below.

A. Assurance of Equal Opportunity (EO). As a condition to the award of financial assistance from ETA, the state must assure that the operation of its program, and all agreements or arrangements to carry out the programs for which assistance is awarded, will comply with the following laws:

- Title VI of the Civil Rights Act of 1964, as amended;
- Sections 504 and 508(f) of the Rehabilitation Act of 1973, as amended;
- Age Discrimination Act (ADA) of 1975, as amended,
- Section 188 of the Workforce Investment Act; and
- Title IX of the Education Amendments of 1972, as amended

Further, the state must assure that it will establish and adhere to Methods of Administration that give a reasonable guarantee of compliance with the above equal opportunity and nondiscrimination laws and regulations regarding the program services it provides and in its employment practices. These Methods of Administration must, at a minimum, include the following:

1. Designation of an Equal Opportunity Officer. The state must designate a senior-level individual to coordinate its EO responsibilities. The person designated must report to the

top official on equal opportunity and nondiscrimination matters and be assigned sufficient staff and resources to ensure the capability to fulfill the agency's equal opportunity and nondiscrimination obligations.

2. Equal Opportunity Notice and Communication. The state must take affirmative steps to prominently display the *Equal Opportunity is the Law* poster in all of its facilities and inform applicants for programs, participants, applicants for employment, and employees:

- **a.** that the state does not discriminate in admission, access, treatment, or employment; and
- **b.** of their right to file a complaint and how to do so.

Other than the *Equal Opportunity is the Law* poster, methods of notification of this information may include placement of notices in offices and publication of notices in newsletters, newspapers, or magazines.

3. Assurances. The state must develop and implement procedures for transferring nondiscrimination and EO obligations in sub-contracts and sub-agreements.

4. Universal Access. The state must take appropriate steps to ensure that they are providing universal access to their programs. These steps should include reasonable efforts to include members of both sexes, various racial and ethnic groups, individuals with disabilities and individuals in differing age groups.

5. Compliance with Section 504. The state must take the necessary measures to ensure access to its programs and facilities for persons with disabilities, as well as make certain communication with persons with disabilities is as effective as that with others.

6. Data Collection and Recordkeeping. The state must collect such data and maintain such records in accordance with procedures prescribed by the Director of the U.S. Department of Labor's Civil Rights Center. These characteristics data (e.g., race, sex, national origin, age, disability) are utilized to determine whether the state and its local office are in compliance with Federal nondiscrimination and equal opportunity statutes and regulations.

7. Monitoring. The state must establish a system for periodically monitoring the delivery of program services for compliance.

8. Discrimination Complaint Procedures. The state must develop and follow procedures for handling complaints of discrimination covering all of the regulations applicable to it as a recipient of Federal financial assistance.

9. Corrective Actions and Sanctions. The state must establish procedures for taking prompt corrective action regarding any noncompliance finding relating to the administration, management, and operation of its programs and activities.

B. Assurance of Administrative Requirements and Allowable Cost Standards. The State must comply with administrative requirements and cost principles applicable to grants and cooperative agreements as specified in 20 CFR Part 601 (Administrative Procedure), 29 CFR Part 93 (Lobbying Prohibitions), 29 CFR Part 96 and Part 99 (Audit Requirements), 29 CFR Part 97 (Uniform Administrative Requirements for Grants and Cooperative Agreements to State and Local Governments), and OMB Circular A-87 (Revised), 2 CFR 225 (Cost Principles for State, Local, and Indian Tribal Governments), and with administrative requirements for debarment and suspension applicable to sub-grants or contracts as specified in 29 CFR Part 98 (Debarment and Suspension). The state assures that state staff will attend mandatory meetings and training sessions, or return unused funds.

States that have subawards to organizations covered by audit requirements of 29 CFR Part 99 (Audit of States, Local Governments, and Non-Profit Organizations) must (1) ensure that such subrecipients meet the requirements of that circular, as applicable, and (2) resolve audit findings, if any, resulting from such audits, relating to the UI program.

The state also assures that it will comply with the following specific administrative requirements:

1. Administrative Requirements

a. Program Income. Program income is defined in 29 CFR 97.25 as gross income received by a grantee or subgrantee directly generated by a grant supported activity, or earned only as a result of the grant agreement during the grant period. States may deduct costs incidental to the generation of UI program income from gross income to determine net UI program income. UI program income shall be added to the funds committed to the grant by ETA. The program income must be used only as necessary for the proper and efficient administration of the UI program. Any rental income or user fees obtained from real property or equipment acquired with grant funds from prior awards shall be treated as program income under this grant.

b. Budget Changes. Except as specified by terms of the specific grant award, ETA, in accordance with regulations, waives the requirements in 29 CFR 97.30(c)(1)(ii) that states obtain prior written approval for certain types of budget changes.

c. Real Property Acquired with Reed Act Funds. The requirements for real property acquired with Reed Act or other non-Federal funds and amortized with UI grants are in UIPL 39-97, dated September 12, 1997; 29 CFR 97.31, to the extent

amortized with UI grants; and in TEGL 7-04, Issues Related to Real Property Used for ETA Program Purposes.

d. Equipment Acquired with Reed Act Funds. The requirements for equipment acquired with Reed Act or other non-Federal funds and amortized with UI grants are in UIPL 39-97, and UIPL 39-97 Changes 1 and 2, and in 29 CFR 97.31, to the extent amortized with UI grants.

e. Real Property, Equipment, and Supplies

1) Real property, equipment, and supplies acquired under prior awards are transferred to this award and are subject to the relevant regulations at 29 CFR Part 97.

2) For computer systems and all associated components which were installed in states for the purpose of Regular Reports, BAM, and other UI Activities, the requirements of 29 CFR Part 97 apply. The National Office reserves the right to transfer title and issue disposition instructions in accordance with paragraph (g) of Federal regulations at 29 CFR 97.32. States also will certify an inventory list of system components which will be distributed annually by ETA.

2. Exceptions and Expansions to Cost Principles. The following exceptions or expansions to the cost principles of OMB Circular No. A-87 (Revised) are applicable to states:

a. Employee Fringe Benefits. As an exception to OMB Circular A-87 (Revised) with respect to personnel benefit costs incurred on behalf of state employees who are members of fringe benefit plans which do not meet the requirements of OMB Circular No. A-87 (Revised), Attachment B, item 11, the costs of employer contributions or expenses incurred for state fringe benefit plans are allowable, provided that:

1) For retirement plans, all covered employees joined the plan before October 1, 1983; the plan is authorized by state law; the plan was previously approved by the Secretary; the plan is insured by a private insurance carrier which is licensed to operate this type of plan in the applicable state; and any dividends or similar credits because of participation in the plan are credited against the next premium falling due under the contract.

2) For all state fringe benefit plans other than retirement plans, if the Secretary granted a time extension after October 1, 1983, to the existing approval of such a plan, costs of the plan are allowable until such time as the plan is comparable in cost and benefits to fringe benefit plans available to other similarly employed

state employees. At such time as the cost and benefits of an approved fringe benefit plan are equivalent to the cost and benefits of plans available to other similarly employed state employees, the time extension will cease and the cited requirements of OMB Circular A-87 (Revised) will apply.

3) For retirement plans and all other fringe benefit plans covered in (1) and (2) of this paragraph, any additional costs resulting from improvements to the plans made after October 1, 1983, are not chargeable to UI grant funds.

b. UI Claimant's Court Appeals Costs. To the extent authorized by state law, funds may be expended for reasonable counsel fees and necessary court costs, as fixed by the court, incurred by the claimant on appeals to the courts in the following cases:

1) Any court appeal from an administrative or judicial decision favorable in whole or in part for the claimant;

2) Any court appeal by a claimant from a decision which reverses a prior decision in his/her favor;

3) Any court appeal by a claimant from a decision denying or reducing benefits awarded under a prior administrative or judicial decision;

4) Any court appeal as a result of which the claimant is awarded benefits;

5) Any court appeal by a claimant from a decision by a tribunal, board of review, or court which was not unanimous;

6) Any court appeal by a claimant where the court finds that a reasonable basis exists for the appeal.

c. Reed Act. Payment from the state's UI grant allocations, made into a state's account in the Unemployment Trust Fund for the purpose of reducing charges against Reed Act funds (Section 903(c)(2) of the Social Security Act, as amended (42 U.S.C. 1103(c)(2)), are permitted provided that the charges against the grant are allowable costs under OMB Circular A-87 and provided that

1) The charges against Reed Act funds were for amounts appropriated, obligated, and expended for the acquisition of automated data processing installations or for the acquisition or major renovation of state-owned buildings, but not land; and

2) With respect to each acquisition or improvement of property, the payments are accounted for as credit against equivalent amounts of Reed Act funds previously withdrawn under the respective appropriation.

d. Prior Approval of Equipment Purchases. As provided for in OMB Circular No. A-87 (Revised), Attachment B, item 19, the requirement that grant recipients obtain prior approval from the Federal grantor agency for all purchases of equipment (as defined in 29 CFR 97.31) is waived and approval authority is delegated to the state administrator.

e. Federal Cash Transaction Report. The state is exempt from submission of the SF 272, Federal Transactions Report, and the SF 272A, Continuation Sheet, per 29 CFR 97.41 (c) discretion.

C. Assurance of Management Systems, Reporting, and Record Keeping. The state assures that:

1. Financial systems provide fiscal control and accounting procedures sufficient to permit timely preparation of required reports, and the tracing of funds to a level of expenditure adequate to establish that funds have not been expended improperly (29 CFR 97.20).

2. The financial management system and the program information system provide federally-required reports and records that are uniform in definition, accessible to authorized Federal and state staff, and verifiable for monitoring, reporting, audit, and evaluation purposes.

3. It will submit reports to ETA as required in instructions issued by ETA and in the format ETA prescribes.

4. It will retain all financial and programmatic records, supporting documents, and other required records at least three years as specified in 29 CFR 97.42(b).

5. The financial management system provides for methods to insure compliance with the requirements applicable to procurement and grants as specified in 29 CFR Part 98 (Debarment and Suspension), and for obtaining the required certifications under 29 CFR 98.510(b) regarding debarment, suspension, ineligibility, and voluntary exclusions for lower tier covered transactions.

D. Assurance of Program Quality. The state assures that it will administer the UI program in a manner that ensures proper and efficient administration. "Proper and efficient administration" includes performance measured by ETA through Core measures, Management Information Measures, program reviews, and the administration of the UI

BAM, Benefits Timeliness and Quality (BTQ) measures, Data Validation (DV), and TPS program requirements.

E. Assurance on Use of Unobligated Funds. The state assures that non-automation funds will be obligated by December 31 of the following fiscal year, and liquidated within 90 days thereafter. ETA may extend the liquidation date upon written request. Automation funds must be obligated by end of the 3rd fiscal year, and liquidated within 90 days thereafter. ETA may extend the liquidation date upon written request. Failure to comply with this assurance may result in disallowed costs from audits or review findings.

Note. Travel costs for state agency personnel are considered obligated when the travel is actually performed.

F. Assurance of Prohibition of Lobbying Costs. The state assures and certifies that, in accordance with the DOL Appropriations Act(s), no UI grant funds will be used to pay salaries or expenses related to any activity designed to influence legislation or appropriations pending before the Congress of the United States. (29 CFR Part 93)

G. Drug-Free Workplace. The state assures and certifies that it will comply with the requirements at this part. (29 CFR Part 98)

H. Assurance of Contingency Planning. The state must establish, effectively implement, and maintain plans for emergency response, backup operations, and post-disaster recovery for the UI systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

The state assures that, at a minimum, the following formally written and tested procedures of Contingency Planning are in place:

- procedures for sustaining essential business operations while recovering from a significant disruption
- procedures and capabilities for recovering information technology (IT) system, such as a major application or general support system
- procedures to facilitate recovery of capabilities at an alternate site
- procedures and capabilities to sustain an organization's essential, strategic functions at an alternate site for up to 30 days
- procedures for recovering business operations immediately following a disaster
- procedures for disseminating status reports to personnel and the public
- strategies to detect, respond to, and limit consequences of malicious cyber incident
- procedures for minimizing loss of life or injury and protecting property damage in response to a physical threat.

The National Institute of Standards and Technology (NIST) provides guidelines for IT

Contingency Planning. An overview of these guidelines is provided in Appendix IV. It is recommended that the state follow state or departmental guidelines for business related procedures, such as business continuity, continuity of operations, or business recovery after a disaster.

I. Assurance of Conformity and Compliance. The state assures that the state law will conform to, and its administrative practice will substantially comply with, all Federal UI law requirements, and that it will adhere to DOL directives.

J. Assurance of Automated Information Systems Security. The state must establish and implement an information security program. The state must ensure that it is providing adequate IT security and that it is commensurate to the level of risk associated with the UI program and the UI IT environment. The state must ensure that appropriate safeguards are put in place to protect both tangible and intangible resources and employees.

The state should develop, disseminate, and periodically review/update: (1) formal, documented policies for Risk Assessment and System Security Planning that address purpose, scope, roles, responsibilities, management commitment, coordination among all entities, and compliance; and (2) formal, documented procedures to facilitate the implementation of these policies and associated controls.

The state assures that it has the following Risk Assessment controls for UI systems in place:

1. Risk Assessments of the UI systems to assess the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and other systems that support the operations and assets of the state.

2. Updates to the Risk Assessment at least once every three years or whenever there are significant changes to any of the UI systems, facilities where they reside, or other conditions that may affect the security status of the system.

3. Scans for vulnerabilities in the UI systems as deemed necessary or when significant new vulnerabilities potentially affecting the system are identified and reported.

The state assures that it has the following System Security Planning controls for UI systems in place:

1. A System Security Plan for the UI systems that provides an overview of the security requirements for the systems and a description of the security controls in place or planned for meeting those requirements. The plan should be approved by the officials designated by the state.

2. An annual review of the system security plan for the UI systems. Revisions to the plan should address system/organizational changes or problems identified during plan implementation and/or security control assessments.

3. A set of rules that describes users' responsibilities and expected behavior with regard to UI information and information system usage. A signed acknowledgement (Rules of Behavior) from users indicating that they have read, understood, and agreed to abide by a set of Rules of Behavior, before authorizing access to the information system and its resident information.

An overview of Risk Management and System Security Planning for an information system is provided in Appendix IV.

K. Assurance of Confidentiality. The state will keep confidential any business information, as defined at 29 CFR 90.33 and any successor provision(s), it obtains or receives in the course of administering the Trade Adjustment Assistance or Alternative Trade Adjustment Assistance programs under this Agreement. The state shall not disclose such information to any person, organization, or other entity except as authorized by applicable state and Federal laws.

VIII. SQSP CONTENT CHECKLIST

The SQSP Content Checklist shows all the documents which comprise the entire SQSP listed by submittal and in order of assembly. Each state must insure that those documents appropriate to its plan are submitted to minimize the potential for a delay in the approval and funding process.

A. SQSP Submittal

AUGUST SUBMITTAL (Main)

1. Transmittal Letter
2. CAPs
   - Deficient Core Performance
   - Improper Administration of BAM or BPC Activities
3. State Plan Narrative
   - A. Overview
   - B. Federal Emphasis (GPRA goals)
   - C. Program Review Deficiencies
     - (a) Federal Program Reviews (UCFE, UCX, etc.)
     - (b) BPC Reviews
     - (c) Internal Security Reviews
     - (d) Data Validation

(e) Automation Grants
(f) BAM Requirement Deficiencies
1) Organization
2) Authority
3) Written Procedures
4) Format
5) Sample Selection and Investigation
6) Case Completion Timeliness
(g) TPS Requirement Deficiencies
(h) Other

D. Program Deficiencies
E. Reporting Requirements
F. Customer Service Surveys (optional)
G. Other

4. Budget Worksheets/Forms
SF 424, SF 424 (A) & (B) - Application for Federal Assistance (as necessary)
5. Organization Chart
6. Signature Page

OCTOBER SUBMITTAL
UI-1 - UI Staff Hours

B. SBR SUBMITTAL (As Appropriate)

1. Transmittal Letter
2. Budget Worksheets/Forms
SF 424, SF 424 (A) & (B) - Application For Federal Assistance
3. Supporting Documentation
Summary
Commitment to Complete Project
Schedule
Description of Proposed Fund Usage
Amount of Funding Requested
Expenditures
4. Additional SBR Documentation (Law Change SBRs only)
Bill Number and Effective Date
Relevant Provisions
Costs & Narrative by Legislative Provision
UI only Statement
5. Optional Supplementary Items (Large-scale, Complex Projects)
Technical Approach
Strategic Design

Measurable Improvements Expected
Supporting Materials

ET HANDBOOK NO. 336

18th Edition

APPENDIX I

PLANNING FORMS AND FORMATS

CORRECTIVE ACTION PLAN

State:	**Federal Fiscal Year:**
MEASURE/PROGRAM AREA: *(For Core Measures use descriptor contained in Appendix III of the SQSP Handbook)*	**Performance Level:** *(most recent 4 quarters)* **Current 12/31 3/31 6/30 9/30** *(Identify the performance level as a percentage)*

SUMMARY:

Provide:
A. the reason(s) for the deficiency;
B. a description of the actions/activities which will be undertaken to improve performance and;
C. if a plan was in place the previous fiscal year, an explanation of why the actions contained in that plan were not successful in improving performance, and an explanation of why the actions now specified will be more successful; and
D. a brief description of plans for monitoring and assessing accomplishment of planned actions and for controlling quality after achieving performance goals.

If the desired improvement will not be accomplished by the end of the current fiscal year, also indicate the major actions remaining to be taken in subsequent fiscal years, and a projection as to when the performance goal will be achieved.

MILESTONES: (Number sequentially)	**Completion Date***			
	12/31	**03/31**	**06/30**	**09/30**
Milestones should be established for each core element of the state's corrective action plan and be of sufficient number and frequency to facilitate state and regional plan oversight and assessment during the fiscal year. It is anticipated that one or more milestones for each quarter would permit such progress tracking and assessment during the fiscal year through state and Regional follow-up schedules. *States also may wish to identify performance milestones that reflect the performance level they anticipate will result from completion of planned activities.* {} If continued, check box				

* check the quarter milestone is expected to be completed.

STATE PLAN NARRATIVE OUTLINE

STATE PLAN NARRATIVE
(State Name - FY xxxx)

A. Overview

1. State priorities and the strategic direction the state has adopted to ensure continuous improvement.
2. Assessment of past performance and expected future performance. Includes, at state discretion, a discussion of external factors that may have performance implications.
3. Coordination with other plans.

B. Federal emphasis (GPRA goals)

1. State performance compared to the GPRA goals.
2. Actions taken to improve performance in GPRA goals.

C. Program review deficiencies

1. Causes for failures to conduct required reviews/activities, e.g., Benefit Payment Control, Internal Security, Benefit Accuracy Measure, Tax Performance System, and Data Validation.
2. Plans to conduct the reviews as required.

D. Program Deficiencies

1. Plans to correct deficiencies identified through required program reviews, e.g., deficiencies identified during an internal security review.
2. Core Measure transition performance improvement acknowledgments, e.g., new Core Measure for tax quality.

E. Reporting requirements

Actions to correct reporting deficiencies. Reporting deficiencies are defined as missing reports, or reports submitted late more than 50 percent of the time (7 of 12 months for monthly reports; 3 of 4 quarters for quarterly reports).

F. Customer Service Surveys (optional)

G. Other (e.g., approach to maintaining solvency, requests for technical assistance)

H. Assurances:

a. Assurance of Equal Opportunity (EO).
b. Assurance of Administrative Requirements and Allowable Cost Standards.
c. Assurance of Management Systems, Reporting, and Recordkeeping.
d. Assurance of Program Quality.
e. Assurance on Use of Unobligated Funds.
f. Assurance of Prohibition of Lobbying Costs (29 CFR Part 93).
g. Drug-Free Workplace (29 CFR Part 98).
h. Assurance of Contingency Planning.
Provide the most recent dates for the following:
- **Information Technology Contingency Plan Implemented: _____**
- **Information Technology Contingency Plan Updated: _____**
- **Information Technology Contingency Plan Tested: _____**

i. Assurance of Conformity and Compliance.
j. Assurance of Automated Information Systems Security.
Provide the most recent dates for the following:
- **Risk Assessment Conducted: _____**
- **System Security Plan Updated: _____**

k. Assurance of Confidentiality.

U.S. Department of Labor

SQSP SIGNATURE PAGE

OMB Approval No. 1205-0132 Expires 06/30/08

U.S. DEPARTMENT OF LABOR Employment and Training Administration	**FEDERAL FISCAL YEAR**	**STATE**

UNEMPLOYMENT INSURANCE
STATE QUALITY SERVICE PLAN
SIGNATURE PAGE

This Unemployment Insurance State Quality Service Plan (SQSP) is entered into between the Department of Labor, Employment and Training Administration, and

_____

(STATE'S NAME)

The Unemployment Insurance SQSP is part of the State's overall operating plan and, during this Federal fiscal year, the State agency will adhere to and carry out the standards set forth in Federal UI Law as interpreted by the DOL, and adhere to the Federal requirements related to the use of granted funds.

All work performed under this agreement will be in accordance with the assurances and descriptions of activities as identified in the SQSP Handbook and will be subject to its terms.

TYPED NAME AND TITLE	**SIGNATURE**	**DATE**
STATE ADMINISTRATOR		
DOL APPROVING OFFICIAL		

U.S. DEPARTMENT OF LABOR
Employment and Training Administration

Exp. Date 6/30/2008
OMB Approval #1205-0132

WORKSHEET UI-1	UI STAFF HOURS	
State	Fiscal Year	Date

Annual Hours Per Staff Year and Quarterly Distribution

Hours Per Staff Year	**Annual**	**First**	**Second**	**Third**	**Fourth**
a. Hours Worked					
b. Hours Paid					

Comments

ETA 8623A (July 2003)

INSTRUCTIONS FOR THE UI-1

Please type or print legibly. The following general instructions explain how to use the form itself.

Item	Entry
a.	Enter the annual staff year hours worked and distribution by quarter. The annual hours for this item must equal the annual hours worked from the planning targets.
b.	Enter the annual staff year hours paid and distribution by quarter. The annual hours for this item must equal the annual hours for the number of standard hours.

ETA 8623A (July 2003) Back

APPENDIX IV

INFORMATION TECHNOLOGY SECURITY GUIDELINES[1]

1 The information in this appendix is attributed to National Institute of Standards and Technology (NIST) Special Publications (SP) and Federal Information Processing Standards (FIPS). These publications can be found on the NIST website, http://csrc.nist.gov/publications/PubsSPs.html, and http://csrc.nist.gov/publications/PubsFIPS.html, respectively. Web links of the key NIST documents are provided below:

NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems, 2006 February;*
NIST SP 800-30, *Risk Management Guide for Information Technology Systems, 2002 July;*
NIST SP 800-34, *Contingency Planning for Information Technology Systems, 2002 June;*
NIST SP 800-100, *Information Security Handbook: A Guide for Managers, 2006 October;*
FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems, 2004 February;*
FIPS Pub 200, *Minimum Security Requirements for Federal Information and Information Systems, 2006 March;*

INFORMATION TECHNOLOGY (IT) CONTINGENCY PLANNING

Contingency planning for information systems is a required process for developing general support systems (GSS) and major applications (MA) with appropriate backup methods and procedures for implementing data recovery and reconstitution against IT risks. Risks to information systems may be natural, technological, or human in nature.

Contingency planning refers to interim measures to recover IT services following an emergency or system disruption. Interim measures may include the relocation of IT systems and operations to an alternate site, the recovery of IT functions using alternate equipment, or the performance of IT functions using manual methods.

The capability to recover and reconstitute data should be integral to the information system design concept during the Initiation phase of Software Development Life Cycle of a system. Recovery strategies should be built into the architecture of the system during the Development phase. The contingency processes should be tested and maintained during the Implementation phase; contingency plans should be exercised and maintained during the Operations/Maintenance phase.

NIST SP 800-34, *Contingency Planning for Information Technology Systems*, details a seven-step methodology for developing an IT contingency process and plan. These seven steps are summarized below:

Step 1: Develop Contingency Planning Policy Statement

A formal department or agency policy provides the authority and guidance necessary to develop an effective contingency plan. The statement should define the agency's overall contingency objectives; identify leadership, roles and responsibilities, resource requirements, test, training, and exercise schedules; and develop maintenance schedules and determine the minimum required backup frequency.

Step 2: Conduct Business Impact Analysis

A business impact analysis (BIA) is a critical step to understanding the information systems components, interdependencies, and potential downtime impacts. The BIA helps to identify and prioritize critical IT systems and components. Contingency plan strategy and procedures should be designed in consideration of the results of the BIA.

A BIA is conducted by identifying the system's critical resources. Each critical resource is then further examined to determine how long functionality of the resource could be withheld from the information system before an unacceptable impact is experienced. The impact may be something that materializes over time or may be tracked across related resources and dependent systems (e.g., cascading domino effect). The time identified is

called a maximum allowable outage (MAO). Based on the potential impacts, the amount of time the information system can be without the critical resource then provides a recourse recovery priority around which an organization can plan recovery activities. The balancing point between the MAO and the cost to recover establishes the information system's recovery time objective (RTO). Recovery strategies must be created to meet the RTO. The strategy must also address recovering information system critical components within a priority, as established by their individual RTOs.

Step 3: Identify Preventive Controls

In some cases, implementing preventive controls might mitigate outage impacts identified by the BIA. Preventive controls are measures that detect, deter, and/or reduce impacts to the system. When cost-effective, preventing an impact is desired over implementing recovery strategies (and therefore risking data loss and impact to the organization). Preventive measures are specific to individual components and the environment in which the components operate. Common controls include:

- Uninterruptible power supply (UPS);
- Fire suppression systems;
- Gasoline or diesel-powered generators;
- Air conditioning systems with excess capacity to permit failure of certain components;
- Heat-resistant and waterproof containers for backup media and vital non-electronic records; and
- Frequent, scheduled data backups.

Step 4: Develop Recovery Strategies

When a disruption occurs despite the preventive measures implemented, a recovery strategy must be in place to recover and restore data and system operations within the RTO period. The recovery strategy is designed from a combination of methods, which together address the full spectrum of information system risks. The most cost-effective option, based on potential impact, should be selected and integrated into the information system architecture and operating procedures.

System data must be backed up regularly; therefore, all IT contingency plans should include a method and frequency for conducting data backups based on system criticality. Data that is backed up may need to be stored offsite and rotated frequently, depending upon the criticality of the system.

Major disruptions to system operations may require restoration activities to be implemented at an alternate site. The type of alternate site selected must be based on RTO requirements and budget limitations. Equipment for recovering and/or replacing the information system must be provided as part of the recovery strategy. Cost, delivery time, and compatibility factors must also be considered when determining how to provide the necessary equipment. Agencies must also plan for an alternate site that, at a

minimum, provides workspace for all contingency plan personnel, equipment, and the appropriate IT infrastructure necessary to execute IT contingency plan and system recovery activities.

The recovery strategy requires personnel to implement the procedures and test operability. Generally, a member of the organization's senior leadership is selected to activate the plan and lead overall recovery operations. Appropriate teams of personnel (at least two people to ensure there is a primary and alternate available to execute procedures) are identified to be responsible for specific aspects of the plan. Personnel should be chosen to staff the teams based on their normal responsibilities, system knowledge, and availability to recover the system on an on-call basis. A line of succession should be defined to ensure that someone could assume the role of senior leadership if the plan leader is unable to respond.

Step 5: Develop IT Contingency Plan

Procedures for executing the recovery strategy are outlined in the IT contingency plan. The plan must be written in a format that will provide the users (recovery team leadership and members) the context in which the plan is to be implemented and the direct procedures, based on role, to execute.

The NIST SP 800-34, *Contingency Planning for Information Technology Systems* presents a sample format for developing an IT contingency plan. The format defines three main phases that govern the actions to be taken following a system disruption. The **Notification/Activation** phase describes the process of notifying recovery personnel and performing a damage assessment. The **Recovery** phase discusses a suggested course of action for recovery teams and personnel to restore IT operations at an alternate site or using contingency capabilities. The final phase, **Reconstitution**, outlines actions that can be taken to return the system to normal operating conditions. Additionally, the format contains the Supporting Information and Appendices components, which provide supplemental information necessary to understand the context in which the plan is to be used and gives additional information that, may be necessary to execute procedures (e.g., emergency contact information and the BIA).

Step 6: Plan Testing, Training, and Exercises

Personnel selected to execute the IT contingency plan must be trained to perform the procedures, the plan must be exercised, and the system strategy must be tested.

Plan testing should include:

• System recovery on an alternate platform from backup media	• System performance using alternate equipment
• Coordination among recovery teams	• Restoration of normal operations
• Internal and external connectivity	• Notification procedures

Personnel training should include:

• Purpose of the plan	• Security requirements
• Cross-team coordination and communication	• Team-specific processes
• Reporting procedures	• Individual responsibilities

Plan exercises should be designed to examine, individually and then collectively, various components of the entire plan. Exercises may be conducted in a classroom setting: discussing specific components of the plan and/or impact issues; or they may be functional exercises: simulating the recovery using actual replacement equipment, data, and alternate sites.

Step 7: Plan Maintenance

The IT contingency plan must always be maintained in a ready state for use immediately upon notification. Periodic reviews of the plan must be conducted to ensure that key personnel and vendor information, system components and dependencies, the recovery strategy, vital records, and operational requirements are up to date. While some changes may be obvious (e.g., personnel turnover or vendor changes), others will require analysis. The BIA should be reviewed periodically and updated with new information to identify new contingency requirements and priorities. Changes made to the plan are noted in a record of changes, dated, and signed or initialed by the person making the change. The revised plan, or plan sections are circulated to those with plan responsibilities. Because of the impact that plan changes may have on interdependent business processes or information systems, the changes must be clearly communicated and properly annotated in the beginning of the document.

Risk Management

An effective risk management process is an important component of a successful information security program. The principal goal of an organization's risk management process is to protect the organization and its ability to perform its mission, not just its information assets. Risk Management is an essential management function of the organization that is tightly woven into the system development life cycle (SDLC). Because risk cannot be eliminated entirely, the risk management process allows information security program managers to balance the operational and economic costs of protective measures and achieve gains in mission capability. By employing practices and procedures designed to foster informed decision-making, agencies help protect their information systems and the data that support their own mission.

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, provides for the development of an effective risk management program.

Risk management is an aggregation of three processes:

1. Risk Assessment,
2. Risk Mitigation, and
3. Evaluation and Assessment.

These three processes are summarized below:

Risk Assessment

The goal of the risk assessment process is to identify and assess the risks to a given environment. The depth of the risk assessment performed can vary greatly and is determined by the criticality and sensitivity of the system, as applied to confidentiality, integrity, and availability. To meet the goal of the risk assessment, a process is divided into following steps:

Step 1: System Characterization

Characterizing an information system establishes the scope of the risk assessment effort, delineates the operational authorization boundaries, and provides information. This step begins with the identification of the information system boundaries, resources, and information.

When characterizing the system, the mission criticality and sensitivity are described in sufficient terms to form a basis for the scope of the risk assessment. Various techniques, such as questionnaires, interviews, documentation reviews, and automated scanning tools, can be used to collect the information needed to characterize the system completely. At a minimum, the system characterization describes the following individual system components:

- Hardware;
- Software;
- External interfaces to other systems;
- Data; and
- People.

In addition to the component descriptions, the system characterization describes other factors with the potential to affect the security of the system, such as:

- System functional requirements;
- Organizational security policy and architecture;
- System network topology;
- Information flows throughout the system;
- Management, operational, and technical security controls implemented or planned to be implemented for the system; and
- Physical and environmental security mechanisms.

Step 2: Threat Identification

Threat identification consists of identifying threat sources with the potential to exploit weaknesses in the system. The threat statement must be tailored to the individual organization and its processing environment (e.g., end-user computing habits), which is accomplished by performing a threat evaluation, using the system characterization as the basis, for the potential to cause harm to the system.

There are common threat sources that typically apply, regardless of the system, and should be evaluated. These common threats can be categorized into three areas:

- Natural threats (e.g., floods, earthquakes, tornadoes, landslides, avalanches, electrical storms),
- Human threats (intentional or unintentional), and
- Environmental threats (e.g., power failure).

In general, information on natural threats (e.g., floods, earthquakes, storms) should be readily available, as known threats have been identified by many government and private sector organizations. Intrusion detection tools also are becoming more prevalent, and government and industry organizations continually collect data on security events, thereby improving the ability to assess threats realistically.

Step 3: Vulnerability Identification

Vulnerability is defined as "a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy". Vulnerabilities can be identified using a combination of a number of techniques and sources. Reviews of such sources as previous risk assessments, audit

reports, vulnerability lists, and security advisories can be used to begin the process of vulnerability identification. System security testing, using methods such as automated vulnerability scanning tools; security, test, and evaluation (ST&E); and penetration testing can be used to augment the vulnerability source reviews and identify vulnerabilities that may not have been previously identified in other sources.

In addition, developing a security requirements checklist based on the security requirements specified for the system during the conceptual, design, and implementation phases of the SDLC can be used to provide a 360-degree inspection of the system. The checklist developed must ensure the inclusion of appropriate questions in the areas of management, operational and technical security controls. The results of the checklist can be used as input for evaluating compliance and noncompliance, which in turn identifies system, process, and procedural weaknesses that represent potential vulnerabilities.

Step 4: Risk Analysis

The risk analysis is a determination (or estimation) of risk to the system, an analysis that requires the consideration of closely interwoven factors, such as the security controls in place for the system under review, the likelihood that those controls will be either insufficient or ineffective protection of the system, and the impact of that failure. The following four steps—control analysis, likelihood determination, impact analysis, and risk determination—are, in a practical sense, performed simultaneously or nearly simultaneously because they are so tightly linked to each other.

1. Control Analysis

As previously discussed, the analysis of controls in place to protect the system can be accomplished using a checklist or questionnaire, which is based on the security requirements for the system. The checklist also provides guidance on testing security controls. The results are used to strengthen the determination of the likelihood that a specific threat might successfully exploit a particular vulnerability.

2. Likelihood Determination

Likelihood determination considers a threat source's motivation and capability to exploit vulnerability, the nature of the vulnerability, the existence of security controls, and the effectiveness of mitigating security controls. Likelihood ratings are described in the qualitative terms of high, moderate, and low, and are used to describe how likely a successful exploitation of a vulnerability is by a given threat. For example, if a threat is highly motivated and sufficiently capable, and controls implemented to protect the vulnerability are ineffective, then it is highly likely that the attack would be successful. In this scenario, the appropriate likelihood rating would be high. The likelihood ratings of moderate and low are similarly defined to successively lesser degrees.

3. Impact Analysis

The third factor used in determining the level of risk to a system is impact. A proper overall impact analysis considers the following factors: impact to the systems, data, and the organization's mission. Additionally, this analysis should also consider the criticality and sensitivity of the system and its data for the three security domains of confidentiality, integrity, and availability. Tools such as mission-impact reports, asset criticality assessment reports, and business impact analyses results in a rating describing the estimated impact to the system and organization should a threat successfully exploit vulnerability. While impact can be described using either a quantitative or qualitative approach, in the context of information technology (IT) systems and data, impact is generally described in qualitative terms. As with the ratings used to describe likelihood, impact levels are described using the terms of high, moderate, and low. NIST SP 800-30 provides definitions for the impact ratings of low, medium, and high.

4. Risk Determination

Once the ratings for likelihood and impact have been determined through appropriate analyses, the level of risk to the system and the organization can be derived by multiplying the ratings assigned for threat likelihood (e.g., probability) and threat impact. NIST SP 800-30 provides how to calculate an overall risk rating using inputs from the threat likelihood and impact categories.

Step 5: Control Recommendations

The goal of the control recommendations is to reduce the level of risk to the information system and its data to a level the organization deems acceptable. These recommendations are essential input for the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented. This step is designed to help agencies identify and select controls appropriate to the organization's operations and mission that could mitigate or eliminate the risks identified in the preceding steps. The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks:

Effectiveness of recommended options (e.g., system compatibility):

- Legislation and regulation;
- Organizational policy;
- Operational impact; and
- Safety and reliability.

Step 6: Results Documentation

The risk assessment report is the mechanism used to report the results formally of all risk assessment activities. The intended function of this report is to describe and

document the risk posture of the system while it is operating in its stated environment (as described in the system characterization) and to provide organization managers with sufficient information so that they can make sound, risk-based decisions, such as resources that must be allocated to the risk mitigation phase. Lastly, the agency should ensure that the results of the risk assessment are appropriately reflected in the system's Plan of Action and Milestones (POA&M) and System Security Plan.

At a minimum, the risk assessment report should describe the following:

- Scope of the assessment based on the system characterization;
- Methodology used to conduct the risk assessment;
- Individual observations resulting from conducting the risk assessment; and
- Estimation of the overall risk posture of the system.

The risk assessment process is usually repeated at least every three years. However, risk assessments should be conducted and integrated into the SDLC for information systems.

Risk Mitigation

The second phase of the risk management process is risk mitigation. Because it is impractical, if not impossible, to eliminate all risk from a system, risk mitigation strives to prioritize, evaluate, and implement the appropriate risk-reducing controls recommended from the risk assessment process. Managers may use several options to reduce the risk to a system. These options are risk assumption; risk avoidance; risk limitation; risk planning, research, and acknowledgement; and risk transference.

A straightforward strategy can be used to determine whether risk mitigation actions are necessary. Working from each risk identified and analyzed in the first process—risk assessment—managers must then decide whether the risk is acceptable or unacceptable and, subsequently, whether to implement additional controls or not to mitigate unacceptable risks. Once the decision has been made on which risks are to be addressed in the risk mitigation process, a seven-step approach is used to guide the selection of security controls:

1. Prioritize actions;
2. Evaluate recommended control options;
3. Conduct cost-benefit analyses;
4. Select controls;
5. Assign responsibility;
6. Develop a safeguard implementation plan; and
7. Implement selected control(s).

The process of selecting controls to mitigate identified risks to an acceptable level is based on the security categorization of the system. For new systems, once the security controls for the system have been identified and refined and an initial risk assessment conducted, the selected controls must be implemented. For legacy systems, the security

controls that are selected are verified.

Organizations can leverage controls used among multiple systems by designating them as common controls where implementation, assessment, and monitoring is conducted at an organizational level or by areas of specific expertise (e.g., human resources, physical security, building management). The system owner must understand who is responsible for implementing these controls and identify the risk that this extension of trust will generate.

Because it is impracticable to eliminate all risk, it is important to note that even after the controls have been selected and implemented, some degree of residual risk will remain. The remaining residual risk should be analyzed to ensure that it is at an acceptable level. After the appropriate controls have been put in place for the identified risks, the authorizing official should sign a statement accepting any residual risk. Either the official should authorize the operation of the new information system or request continued processing of the existing information system. If the residual risk has not been reduced to an acceptable level, the risk management cycle must be repeated to identify a way of lowering the residual risk to an acceptable level.

Evaluation and Assessment

The third and final phase in the risk management process is evaluation and assessment. The art of risk management in today's dynamic and constantly changing IT environments must be ongoing and continuously evolving. Systems are upgraded and expanded, components are improved, and architectures are constantly evolving.

The evaluation and assessment of security controls' effectiveness must be performed. The results are used to provide an Authorizing Official with the essential information needed to make a credible, risk-based decision on whether to authorize the operation of the information system. The reuse of assessment data will not only save valuable resources, but also provide the most up-to-date risk information for the authorizing official.

Many of the risk management activities are conducted during a snapshot in time—a static representation of a dynamic environment. All the changes that occur to systems during normal, daily operations have the potential to affect the security of the system adversely in some fashion, and it is the goal of the risk management evaluation and assessment process to ensure that the system continues to operate in a safe and secure manner. This goal can be partially reached by implementing a strong configuration management program. In addition to monitoring the security of an information system on a continuous basis, agencies must track findings from the security control assessment to ensure they are addressed appropriately and do not continue to pose or introduce new risks to the system.

System Security Planning

The objective of system security planning is to improve the protection of information system resources. The protection of a system must be documented in a system security plan. The purpose of the system security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system. It should reflect input from various managers with responsibilities concerning the system.

NIST SP 800-18 *Guide for Developing Security Plans for Federal Information Systems*, provides basic information on how to prepare a system security plan in accordance with applicable federal requirements, and it is easily adaptable to a variety of organizational structures.

Program managers, system owners, and security personnel in the organization must understand the system security planning process. In addition, users of the information system and those responsible for defining system requirements should also be familiar with the system security planning process, as the system security plan is an important deliverable in the SDLC process. Those responsible for implementing and managing information systems must participate in addressing security controls to be applied to their systems.

Applications

All information systems must be covered by a system security plan. Systems can be labeled as a major application (MA) or general support system (GSS). MA is defined as an application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. GSS is defined as an interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people. A minor application is an application, other than major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a GSS.

Security Planning Roles and Responsibilities

Agencies should develop policy on the system security planning process. System security plans are living documents that require periodic review, modification, and plans of action and milestones (POA&M) for implementing security controls. Procedures should be in place outlining who reviews the plans, keeps the plan current, and follows up on planned security controls.

The roles and responsibilities in this section are specific to information system security planning.

Chief Information Officer

The chief information officer (CIO) is the agency official responsible for developing and maintaining an agency-wide information security program and has the following system security planning responsibilities:

Designating a Senior Agency Information Security Officer (SAISO) who shall carry out the CIO's responsibilities for system security planning such as:

- Developing and maintaining information security policies, procedures, and control techniques to address system security planning;
- Managing the identification, implementation, and assessment of common security controls;
- Ensuring that personnel with significant responsibilities for system security plans are trained;
- Assisting senior agency officials with their responsibilities for system security plans; and
- Identifying and developing common security controls for the agency.

Information System Owner

The information system owner is the agency official responsible for the overall procurement, development, integration, modification, and operation and maintenance of the information system. The information system owner has the following responsibilities related to system security plans:

- Developing the system security plan in coordination with information owners, the system administrator, the information system security officer (ISSO), the SAISO, and functional "end users";
- Maintaining the system security plan and ensuring that the system is deployed and operated according to the agreed-upon security requirements; and
- Ensuring that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior) and assisting in the identification, implementation, and assessment of the common security controls.

Information Owner

The information owner is the agency official with statutory or operational authority for specified information and is responsible for establishing the controls for information generation, collection, processing, dissemination, and disposal. The information owner has the following responsibilities related to system security plans:

- Establishing the rules for the appropriate use and protection of the subject data/information (rules of behavior);
- Providing input to information system owners on the security requirements and security controls for the information systems where the information resides;
- Deciding who has access to the information system and determining what types of privileges or access rights; and
- Assisting in identifying and assessing the common security controls where the information resides.

Senior Agency Information Security Officer

The SAISO is the agency official responsible for serving as the CIO's primary liaison to the agency's information system owners and ISSOs. The SAISO has the following responsibilities related to system security plans:

- Carrying out the CIO's responsibilities for system security planning;
- Coordinating the development, review, and acceptance of system security plans with information system owners, ISSOs, and the authorizing official;
- Coordinating the identification, implementation, and assessment of the common security controls; and
- Possessing professional qualifications, including training and experience, required to develop and review system security plans.

Information System Security Officer

The ISSO is the agency official assigned responsibility by the SAISO, authorizing official, management official, or information system owner for ensuring that the appropriate operational security posture is maintained for an information system or program. The ISSO has the following responsibilities related to system security plans:

- Assisting the SAISO in identifying, implementing, and assessing the common security controls; and
- Actively supporting the development and maintenance of the system security plan, to include coordinating system changes with the information system owner and assessing the security impact of those changes.

Rules of Behavior

The rules of behavior should clearly delineate responsibilities and expected behavior of all individuals with access to the system. The rules should state the consequences of inconsistent behavior or noncompliance and be made available to every user prior to receiving authorization for system access. It is required that the rules contain a signature page for each user to acknowledge receipt, indicating that they have read, understand, and agree to abide by the rules of behavior. Electronic signatures are acceptable for use in acknowledging the rules of behavior.

Following lists the examples of what should be covered in typical rules of behavior:

- Delineate responsibilities, expected use of system, and behavior of all users
- Describe appropriate limits on interconnections
- Define service provisions and restoration priorities
- Be clear on consequences of behavior not consistent with rules

It covers the following topics:

- Work at home
- Dial-in access
- Connection to the Internet
- Use of copyrighted work
- Unofficial use of government equipment
- Assignment and limitations of system privileges and individual accountability
- Password usage
- Searching databases and divulging information

Agencies can incorporate, by reference, the agency body of policies and procedures governing information security and other applicable policies in the text of the rules of behavior.

System Security Plan Approval

Organizational policy should clearly define who is responsible for system security plan approval and procedures developed for plan submission, including any special memorandum language or other documentation required by the agency.

System Boundary Analysis and Security Controls

Before the system security plan is developed, the information system as well as the information itself should be categorized based on impact analysis. NIST issued FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* to develop standards for categorizing information and information systems. Refer to FIPS Publication 199 for more information on system categorization. Then a determination can be made as to which systems in the inventory can be logically grouped into GSSs or MAs. The FIPS 199 impact levels should be considered when the system boundaries are drawn and when selecting the initial set of security controls (e.g., control baseline). The baseline security controls can then be tailored based on an assessment of risk and local conditions, including organization-specific security requirements, specific threat information, cost-benefit analyses, the availability of compensating controls, or special circumstances. Common security controls, which is one of the tailoring considerations, must be identified prior to system security plan preparation to identify those controls covered at the agency level that are not system-specific. These common security controls can then be incorporated into the system security plan by reference.

Security Controls

FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems* provides seventeen minimum-security requirements for the information systems. The requirements represent a broad-based, balanced information security program that addresses the management, operational, and technical aspects of protecting the confidentiality, integrity, and availability of the information and information systems. An agency should meet the minimum-security requirements in this standard by applying security controls selected in accordance with NIST SP 800-53, *Recommended Security Control for Federal Information Systems* and the designated impact levels of the information systems. An agency has the flexibility to tailor the security control baseline in accordance with the terms and conditions set forth in the standard. Tailoring activities include:

(1) the application of scoping guidance,
(2) the specification of compensating controls, and
(3) the specification of agency-defined parameters in the security controls, where allowed. The system security plan should document all tailoring activities.

Scoping Guidance

Scoping guidance provides an agency with specific terms and conditions on the applicability and implementation of individual security controls in the security control baselines defined in NIST SP 800-53. System security plans should clearly identify which security controls used scoping guidance. In addition, system security plans should include a description of the type of considerations that were made.

Compensating Controls

Compensating security controls are the management, operational, or technical controls used by an agency in lieu of prescribed controls in the low, moderate, or high security control baselines, which provide equivalent or comparable protection for an information system. Compensating security controls for an information system should be used by an agency only under the following conditions:

(1) The agency selects the compensating controls from the security control catalog in NIST SP 800-53;
(2) The agency provides a full and complete rationale and justification for how the compensating controls provide an equivalent security capability or level of protection for the information system; and
(3) The agency assesses and formally accepts the risk associated with using the compensating controls in the information system.

Common Security Controls

An agency-wide view of the information security program facilitates the identification of

common security controls that can be applied to one or more agency information systems. Common security controls can apply to all agency information systems; a group of information systems at a specific site; or common information systems, subsystems, or applications (i.e., common hardware, software, and/or firmware) deployed at multiple operational sites. Common security controls are typically identified during a collaborative agency-wide process that involves the CIO, SAISO, authorizing officials, information system owners, and ISSOs.

For efficiency in developing system security plans, common security controls should be documented once and then inserted or imported into each system security plan for the information systems within the agency.

Security Control Selection

An agency should meet the minimum-security requirements in FIPS 199 by selecting the appropriate security controls and assurance requirements as described in NIST SP 800-53. The process of selecting the appropriate security controls and assurance requirements for agency information systems to achieve adequate security is a multifaceted, risk-based activity involving management and operational personnel within the agency. Subsequent to the security categorization process, an agency must select an appropriate set of security controls for their information systems that satisfy the minimum-security requirements set forth in FIPS 200. The selected set of security controls must be one of three security control baselines from NIST SP 800-53 (see Table below) that are associated with the designated impact levels of the agency information systems as determined during the security categorization process.

FIPS 199 Categorization

Potential Impact			
Security Objective	**Low**	**Moderate**	**High**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Completion and Approval Dates

The completion date of the system security plan should be provided. The completion date should be updated whenever the plan is periodically reviewed and updated. The system security plan should also contain the date the authorizing official or the designated approving authority approves the plan.

Ongoing System Security Plan Maintenance

Once the information system security plan is approved, it is important to periodically assess the plan; review any change in system status, functionality, design, etc.; and ensure that the plan continues to reflect the correct information about the system. This documentation and its accuracy are imperative for system recertification and reaccreditation activity. All plans should be reviewed and updated, if appropriate, at least annually. Some items to include in the review are:

- Change in information system owner;
- Change in information security representative;
- Major change in system architecture;
- Change in system status;
- Additions/deletions of system interconnections;
- Change in system scope; and
- Change in authorizing official.

SAMPLE PLAN FORMATS

SAMPLE IT CONTINGENCY PLAN FORMAT

This sample format provides a template for preparing an information technology (IT) contingency plan. The template is intended to be used as a guide, and the Contingency Planning Coordinator should modify the format as necessary to meet the system's contingency requirements and comply with internal policies. Where practical, the guide provides instructions for completing specific sections. Text is added in certain sections; however, this information is intended only to suggest the type of information that may be found in that section. The text is not comprehensive and should be modified to meet specific agency and system considerations. The IT contingency plan should be marked with the appropriate security label, such as *Official Use Only*.

IT CONTINGENCY PLAN

1. INTRODUCTION

1.1 PURPOSE

This {*system name}* Contingency Plan establishes procedures to recover the {*system name}* following a disruption. The following objectives have been established for this plan:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
  - *Notification/Activation phase* to detect and assess damage and to activate the plan
  - *Recovery phase* to restore temporary IT operations and recover damage done to the original system
  - *Reconstitution phase* to restore IT system-processing capabilities to normal operations.
- Identify the activities, resources, and procedures needed to carry out {*system name}* processing requirements during prolonged interruptions to normal operations.
- Assign responsibilities to designated *{Organization name}* personnel and provide guidance for recovering {*system name}* during prolonged periods of interruption to normal operations.
- Ensure coordination with other *{Organization name}* staff who will participate in the contingency planning strategies. Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

1.2 APPLICABILITY

The {*system name}* Contingency Plan applies to the functions, operations, and resources necessary to restore and resume {*Organization name}'s* {*system name}* operations as it is installed at *primary location name, City, State*. The {*system name}* Contingency Plan applies to *{Organization name}* and all other persons associated with *{system name}* as identified under Section 2.3, Responsibilities.
The *{system name}* Contingency Plan is supported by *plan name,* which provides the *purpose of plan.* Procedures outlined in this plan are coordinated with and support the *plan name*, which provides *purpose of plan.*

1.3 SCOPE

1.3.1 Planning Principles

Various scenarios were considered to form a basis for the plan, and multiple assumptions were made. The applicability of the plan is predicated on two key principles:

- *The {Organization name}'s* facility in *City, State,* is inaccessible; therefore, *{Organization name}* is unable to perform {*system name}* processing for the *Department*.
- A valid contract exists with the alternate site that designates that site in City, State, as the {Organization name}'s alternate operating facility.
  - {Organization name} will use the alternate site building and IT resources to recover {system name} functionality during an emergency that prevents access to the original facility.
  - The designated computer system at the alternate site has been configured to begin processing {system name} information.
  - The alternate site will be used to continue {system name} recovery and processing throughout the period of disruption, until the return to normal operations.

1.3.2 Assumptions

Based on these principles, the following assumptions were used when developing the IT Contingency Plan:

- The {system name} is inoperable at the {Organization name} computer center and cannot be recovered within 48 hours.
- Key {system name} personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the {system name} Contingency Plan.
- Preventive controls (e.g., generators, environmental controls, waterproof tarps, sprinkler systems, fire extinguishers, and fire department assistance) are operational at the time of the disaster.
- Computer center equipment, including components supporting {system name}, are connected to an uninterruptible power supply (UPS) that provides 45 minutes to 1 hour of electricity during a power failure.
- {system name} hardware and software at the {Organization name} original site are unavailable for at least 48 hours.
- Current backups of the application software and data are intact and available at the offsite storage facility.
- The equipment, connections, and capabilities required to operate {system name} are available at the alternate site in City, State.
- Service agreements are maintained with {system name} hardware, software, and communications providers to support the emergency system recovery.

The {system name} Contingency Plan does not apply to the following situations:

- **Overall recovery and continuity of business operations.** The Business Resumption Plan (BRP) and Continuity of Operations Plan (COOP) are appended to the plan.
- **Emergency evacuation of personnel.** The Occupant Evacuation Plan (OEP) is appended to the plan.
- *Any additional constraints should be added to this list*.

1.4 REFERENCES/REQUIREMENTS

This {system name} Contingency Plan complies with the {Organization name}'s IT contingency planning policy as follows:

The organization shall develop a contingency planning capability to meet the needs of critical supporting operations in the event of a disruption extending beyond 72 hours. The procedures for execution of such a capability shall be documented in a formal contingency plan and shall be reviewed at least annually and updated as necessary. Personnel responsible for target systems shall be trained to execute contingency procedures. The plan, recovery capabilities, and personnel shall be tested to identify weaknesses of the capability at least annually.

The {system name} Contingency Plan also complies with the following federal and departmental policies:

- The Computer Security Act of 1987
- OMB Circular A-130, Management of Federal Information Resources, Appendix III, November 2000.
- Federal Preparedness Circular (FPC) 65, Federal Executive Branch Continuity of Operations, July 1999
- Presidential Decision Directive (PDD) 67, Enduring Constitutional Government and Continuity of Government Operations, October 1998
- PDD 63, Critical Infrastructure Protection, May 1998
- Federal Emergency Management Agency (FEMA), The Federal Response Plan (FRP), April 1999
- Defense Authorization Act (Public Law 106-398), Title X, Subtitle G, "Government Information Security Reform," October 30, 2000
- Any other applicable federal policies should be added
- Any other applicable departmental policies should be added.

1.5 RECORD OF CHANGES

Modifications made to this plan since the last printing are as follows:

Record of Changes			
Page No.	**Change Comment**	**Date of Change**	**Signature**

2. CONCEPT OF OPERATIONS

2.1 SYSTEM DESCRIPTION AND ARCHITECTURE

Provide a general description of system architecture and functionality. Indicate the operating environment, physical location, general location of users, and partnerships with external organizations/systems. Include information regarding any other technical considerations that are important for recovery purposes, such as backup procedures. Provide a diagram of the architecture, including security controls and telecommunications connections.

2.2 LINE OF SUCCESSION

The *{organization name}* sets forth an order of succession, in coordination with the order set forth by the *department* to ensure that decision-making authority for the {*system name*} Contingency Plan is uninterrupted. The Chief Information Officer (CIO), {*organization name*} is responsible for ensuring the safety of personnel and the execution of procedures documented within this {*system name*} Contingency Plan. If the CIO is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the Deputy CIO shall function as that authority. *Continue description of succession as applicable.*

2.3 RESPONSIBILITIES

The following teams have been developed and trained to respond to a contingency event affecting the IT system.

The Contingency Plan establishes several teams assigned to participate in recovering *{system name}* operations. The *{team name}* is responsible for recovery of the *{system name}* computer environment and all applications. Members of the *team name* include personnel who are also responsible for the daily operations and maintenance of *{system name}*. The *team leader title* directs the *{team name}.*

Continue to describe each team, their responsibilities, leadership, and coordination with other applicable teams during a recovery operation.

The relationships of the team leaders involved in *system* recovery and their member teams are illustrated in Figure XX below.

> *(Insert hierarchical diagram of recovery teams. Show team names and leaders; do not include actual names of personnel.)*

Describe each team separately, highlighting overall recovery goals and specific responsibilities. Do not detail the procedures that will be used to execute these responsibilities. These procedures will be itemized in the appropriate phase sections.

3. NOTIFICATION AND ACTIVATION PHASE

This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to {*system name*}. Based on the assessment of the event, the plan may be activated by the Contingency Planning Coordinator.

> **In an emergency, the {*Organization name*}'s top priority is to preserve the health and safety of its staff before proceeding to the Notification and Activation procedures.**

Contact information for key personnel is located in Personnel Contact list appendix. The notification sequence is listed below:

- The first responder is to notify the *Contingency Planning Coordinator*. All known information must be relayed to the *Contingency Planning Coordinator*.
- The systems manager is to contact the *Damage Assessment Team Leader* and inform them of the event. The *Contingency Planning Coordinator* is to instruct the *Team Leader* to begin assessment procedures.
- The *Damage Assessment Team Leader* is to notify team members and direct them to complete the assessment procedures outlined below to determine the extent of damage and estimated recovery time. If damage assessment cannot be performed locally because of unsafe conditions, the *Damage Assessment Team* is to follow the outline below.

Damage Assessment Procedures:

(Detailed procedures should be outlined to include activities to determine the cause of the disruption; potential for additional disruption or damage; affected physical area and status of physical infrastructure; status of IT equipment functionality and inventory, including items that will need to be replaced; and estimated time to repair services to normal operations.)

- Upon notification from the *Contingency Planning Coordinator*, the *Damage Assessment Team Leader* is to …
- The *Damage Assessment Team* is to ….

Alternate Assessment Procedures:

- Upon notification from the *Contingency Planning Coordinator*, the *Damage Assessment Team Leader* is to …
- The *Damage Assessment Team* is to ….
  - When damage assessment has been completed, the *Damage Assessment Team Leader* is to notify the *Contingency Planning Coordinator* of the results.
  - The *Contingency Planning Coordinator* is to evaluate the results and determine whether the contingency plan is to be activated and if relocation is required.
  - Based on assessment results, the *Contingency Planning Coordinator* is to notify assessment results to civil emergency personnel (e.g., police, fire) as appropriate.

The Contingency Plan is to be activated if one or more of the following criteria are

met:

1. {*System name*} will be unavailable for more than 48 hours
2. Facility is damaged and will be unavailable for more than 24 hours
3. Other criteria, as appropriate.

- If the plan is to be activated, the *Contingency Planning Coordinator* is to notify all Team Leaders and inform them of the details of the event and if relocation is required.
- Upon notification from the *Contingency Planning Coordinator*, Team Leaders are to notify their respective teams. Team members are to be informed of all applicable information and prepared to respond and relocate if necessary.
- The *Contingency Planning Coordinator* is to notify the *off-site storage facility* that a contingency event has been declared and to ship the necessary materials (as determined by damage assessment) to the *alternate site*.
- The *Contingency Planning Coordinator* is to notify the Alternate site that a contingency event has been declared and to prepare the facility for the *Organization's* arrival.
- The *Contingency Planning Coordinator* is to notify remaining personnel (via notification procedures) on the general status of the incident.

4. RECOVERY OPERATIONS

This section provides procedures for recovering the application at the alternate site, whereas other efforts are directed to repair damage to the original system and capabilities. The following procedures are for recovering the {*system name*} at *the alternate site*. Procedures are outlined per team required. Each procedure should be executed in the sequence it is presented to maintain efficient operations.

Recovery Goal. *State the first recovery objective as determined by the Business Impact Assessment (BIA). For each team responsible for executing a function to meet this objective, state the team names and list their respective procedures.*

- *{team name}*
  − *Team Recovery Procedures*
- *{team name}*
  − *Team Recovery Procedures*
- *{team name}*
  − *Team Recovery Procedures*

Recovery Goal. *State the second recovery objective as determined by the BIA. For each team responsible for executing a function to meet this objective, state the team names and list their respective procedures.*

- *{team name}*
  − *Team Recovery Procedures*
- *{team name}*

- *Team Recovery Procedures*
- *{team name}*
  - *Team Recovery Procedures*

Recovery Goal. *State the remaining recovery objectives (as determined by the BIA). For each team responsible for executing a function to meet this objective, state the team names and list their respective procedures.*

5. RETURN TO NORMAL OPERATIONS

This section discusses activities necessary for restoring {*system name*} operations at the {*Organization name*}'s original or new site. When the computer center at the original or new site has been restored, {*system name*} operations at the alternate site must be transitioned back. The goal is to provide a seamless transition of operations from the alternate site to the computer center.

Original or New Site Restoration

Procedures should be outlined, per necessary team, to restore or replace the original site so that normal operations may be transferred. IT equipment and telecommunications connections should be tested.

- *{team name}*
  - *Team Resumption Procedures*
- *{team name}*
  - *Team Resumption Procedures*

5.1 CONCURRENT PROCESSING

Procedures should be outlined, per necessary team, to operate the system in coordination with the system at the original or new site. These procedures should include testing the original or new system until it is functioning properly and the contingency system is shut down gracefully.

- *{team name}*
  - *Team Resumption Procedures*
- *{team name}*
  - *Team Resumption Procedures*

5.2 PLAN DEACTIVATION

Procedures should be outlined, per necessary team, to clean the alternate site of any equipment or other materials belonging to the organization, with a focus on handling sensitive information. Materials, equipment, and backup media should be properly packaged, labeled, and shipped to the appropriate location(s). Team members should be instructed to return to the original or new site.

- *{team name}*
  - *Team Testing Procedures*
- *{team name}*
  - *Team Testing Procedures*

6. PLAN APPENDICES

The appendices included should be based on system and plan requirements.

- Personnel Contact List
- Vendor Contact List
- Equipment and Specifications
- Service Level Agreements and Memorandums of Understanding
- IT Standard Operating Procedures
- Business Impact Analysis
- Related Contingency Plans
- Emergency Management Plan
- Occupant Evacuation Plan
- Continuity of Operations Plan.

Sample Information System Security Plan Template

The following sample has been provided ONLY as one example. Agencies may be using other formats and choose to update those to reflect any existing omissions based on this guidance. This is not a mandatory format; it is recognized that numerous agencies and information security service providers may have developed and implemented various approaches for information system security plan development and presentation to suit their own needs for flexibility. The template instructions, which are separate from the template, will assist the user when completing the sections of the plan.

Information System Security Plan

1. Information System Name/Title:
2. Information System Categorization:

	LOW		**MODERATE**		**HIGH**

3. Information System Owner:
4. Authorizing Official:
5. Other Designated Contacts:
6. Assignment of Security Responsibility:
7. Information System Operational Status:

	Operational		**Under Development**		**Major Modification**

8. Information System Type:

	Major Application		**General Support System**

9. General System Description/Purpose

10. System Environment

11. System Interconnections/Information Sharing

System Name	Organization	Type	Agreement (ISA/MOU/MOA)	Date	FIPS 199 Category	C&A Status	Auth. Official

12. Related Laws/Regulations/Policies

13. Minimum Security Controls

CONTROL FAMILY	DESCRIPTION	CLASS
Access Control (AC)		**Technical**
Awareness and Training (AT)		**Operational**
Audit and Accountability (AU)		**Technical**
Certification, Accreditation, and Security Assessments (CA)		**Management**
Configuration Management (CM)		**Operational**
Contingency Planning (CP)		**Operational**
Identification and Authentication (IA)		**Technical**
Incident Response (IR)		**Operational**
Maintenance (MA)		**Operational**
Media Protection (MP)		**Operational**
Physical & Environmental Protection (PE)		**Operational**
Planning (PL)		**Management**
Personnel Security (PS)		**Operational**
Risk Assessment (RA)		**Management**
System and Services Acquisition (SA)		**Management**
System and Communications Protection (SC)		**Technical**
System and Information Integrity (SI)		**Operational**

14. Information System Security Plan Completion Date: _____

15. Information System Security Plan Approval Date: _____

Template Instructions

1. Information System Name/Title

- Unique identifier and name given to the system.

2. Information System Categorization

- Identify the appropriate FIPS 199 categorization.

3. Information System Owner

- Name, title, agency, address, email address, and phone number of person who owns the system.

4. Authorizing Official

- Name, title, agency, address, email address, and phone number of the senior management official designated as the authorizing official.

5. Other Designated Contacts

- List other key personnel, if applicable; include their title, address, email address, and phone number.

6. Assignment of Security Responsibility

- Name, title, address, email address, and phone number of person who is responsible for the security of the system.

7. Information System Operational Status

- Indicate the operational status of the system. If more than one status is selected, list which part of the system is covered under each status.

8. Information System Type

- Indicate if the system is a major application or a general support system.

9. General System Description/Purpose

- Describe the function or purpose of the system and the information processes.

10. System Environment

- Provide a general description of the technical system. Include the primary hardware, software, and communications equipment.

11. System Interconnections/Information Sharing

- List interconnected systems and system identifiers (if appropriate), provide the system, name, organization, system type (major application or general support system), indicate if there is an ISA/MOU/MOA on file, date of agreement to interconnect, FIPS 199 category, C&A status, and the name of the authorizing official.

12. Related Laws/Regulations/Policies

- List any laws or regulations that establish specific requirements for the confidentiality, integrity, or availability of the data in the system.

13. Minimum Security Controls

- Provide a thorough description of how the minimum controls in the applicable baseline are being implemented or planned to be implemented. The controls should be described by control family and indicate whether it is a system control, hybrid control, common control, scoping guidance is applied, or a compensating control is being used.

14. Information System Security Plan Completion Date

- Enter the completion date of the plan.

15. Information System Security Plan Approval Date

- Enter the date the system security plan was approved and indicate if the approval documentation is attached or on file.