

OFFICE OF THE INSPECTOR GENERAL



CONTINGENCY PLANNING FOR THE SOCIAL SECURITY ADMINISTRATION

**-- WARNING --
THIS REPORT CONTAINS RESTRICTED
INFORMATION FOR OFFICIAL USE.
DISTRIBUTION LIMITED TO AUTHORIZED
OFFICIALS.**

James G. Huse, Jr. – ACTING INSPECTOR GENERAL

September 1999

A-13-98-12022

EXECUTIVE SUMMARY

THIS REPORT CONTAINS INFORMATION THAT IS SENSITIVE AND CONFIDENTIAL. FOR SECURITY REASONS, WE RECOMMEND THAT DISTRIBUTION OF THIS REPORT BE LIMITED TO THOSE WITH A NEED TO KNOW.

OBJECTIVE

The objective of this audit was to assess the effectiveness of the Social Security Administration's (SSA) contingency planning program to mitigate the impact of unexpected events that could interrupt service delivery throughout SSA.

BACKGROUND

We initiated this audit to determine whether SSA had addressed contingency planning weaknesses identified in previous audits.¹ Contingency planning ensures the continuity of data processing operations in the event of interruptions in normal processing activities. As defined by the National Institute of Standards and Technology (NIST), contingency planning should address all resources needed to perform a function, regardless of whether they directly relate to a computer. Effective planning protects Federal information resources against loss, damage, or unavailability.

Development of a contingency planning policy within SSA is the responsibility of the Division of Systems Security under the Deputy Commissioner for Finance, Assessment, and Management. SSA's contingency planning policy is published in the *Systems Security Handbook* (Handbook). The primary component of SSA's Contingency Planning Program is its Backup and Recovery Plan (BRP).² The BRP provides for the movement of NCC processing activity to a remote contract facility equipped to process critical SSA workloads. It defines the support role for each Deputy Commissioner's component in the event of a disaster at the National Computer Center (NCC). The

¹ *Review of the Back-Up and Recovery Procedures at the National Computer Center*, (A-13-96-11052), June 1997; and *Social Security Accountability Report for Fiscal Year 1997*, Price Waterhouse, November 1997.

² Officially entitled, *Backup Plan for National Computer Center Operations*, SSA staff commonly refer to it as the *Backup and Recovery Plan*, *Backup and Recovery Plan for the National Computer Center (NCC) Operations*, and *Disaster and Recovery Plan*.

Emergency Response Procedure (ERP) establishes the actions to be taken by key SSA offices and personnel after a catastrophic event that threatens the data processing operations at the NCC.

SSA depends on the NCC and its communications network to accomplish its mission of service to beneficiaries. The NCC is a large data processing facility located in Baltimore, Maryland. The NCC transmits, receives, processes, and/or stores about 20 million programmatic transactions per day. These transactions contain sensitive beneficiary data submitted by SSA's nationwide network supporting over 1,300 field offices.

Customer service performance measures set by SSA in the SSA Business Plan establish the expectation of prompt service to millions of beneficiaries. The availability of SSA's systems is critical to the achievement of these goals. To meet this expectation on a continued basis, service continuity controls must be in place and functioning to reasonably prevent or mitigate the occurrence of denied availability of systems processing capability or unexpected loss of information resources.

We assessed SSA's contingency planning process to determine its compliance with the requirements of the Computer Security Act. In addition, we compared SSA's planning documents to its contingency plan to determine if there were inconsistencies. We reviewed applicable regulatory criteria and SSA policy, evaluated contingency planning and risk assessment documentation, observed contingency planning meetings, and interviewed SSA staff involved in contingency planning activities. We conducted our audit field work from April through June 1998 at SSA Headquarters and the NCC in Baltimore, Maryland.

RESULTS OF REVIEW

Although SSA had established a disaster recovery program, significant improvement is needed in SSA's overall contingency planning program. The program was fragmented, and contingency activities were not adequately documented for SSA or all of its components. We have categorized the major areas of concern, as follows.

- **SSA'S CONTINGENCY PLANNING PROGRAM LACKED FUNDAMENTAL INFRASTRUCTURE ELEMENTS**
- **CONTROLS WITHIN SSA'S CONTINGENCY PLANNING PROGRAM WERE INADEQUATE**
- **SSA HAD NOT RESOLVED OPEN ACTIONS FROM PREVIOUS AUDIT REPORTS**

CONCLUSIONS AND RECOMMENDATIONS

Based on our findings, we question the effectiveness of SSA's contingency planning program to mitigate the impact of unexpected events that could interrupt service delivery throughout SSA. Although SSA has some service continuity controls in place, it still needs to ensure the protection of all general support systems and major applications from service interruptions of any magnitude. To achieve this goal, SSA must improve the development and testing of its contingency plans. Without adequate development and a system to fully test contingency plans, we believe SSA will likely be unable to provide an acceptable level of service to the public in the event of disruptions of any kind. To improve its contingency planning program, we recommend that SSA:

- Establish and communicate to SSA staff, a formal infrastructure for SSA's contingency planning program.
- Adopt NIST guidance for contingency planning; address accountability for the contingency planning process functions; define the organizational roles and responsibilities for the process functions; and provide for training of SSA staff in contingency planning duties.
- Adopt and communicate a distinct definition of contingency planning so responsible staff understands the concept.
- After a defined infrastructure is in place, develop a contingency plan and individual component contingency plans, compliant with NIST guidance. This effort needs to address and document plans for all SSA general support systems and major applications located throughout the SSA complex, including Central Office components as well as regional office elements, such as area offices, field offices, and disability determination services.
- Ensure the BRP is kept current.
- Document a contingency planning policy consistent with NIST guidance. The policy should address the established SSA contingency planning infrastructure, define explicit roles and responsibilities of specific SSA components, and be clearly communicated to all SSA staff.
- Ensure that requirements and references within the Handbook are kept current, and add the current definition of Office of Management and Budget (OMB) Circular A-130 categories of general support systems and major applications to the Handbook to ensure proper security plan documentation.

- Institute in written policy the NIST standard for risk management of Federal information systems and perform a risk assessment of the NCC that complies with the requirements of OMB Circular A-130, the Handbook, and NIST guidance.
- Ensure that all general support systems and major applications have current and compliant risk assessments documented.
- Ensure that the ERP is kept current.
- Update the ERP to reflect sound planning assumptions, to ensure current key personnel contact information is included and to include complete information regarding team contact rosters. Specifically, SSA needs to update the ERP to include detailed procedures to be followed by the various teams involved in the event of activation of the ERP.
- Update the ERP to reflect staffing requirements that correlate to staffing requirements in the BRP, and consider the requirement of more experienced personnel at the hot-site³ in the event of ERP activation.
- Ensure SSA's contingency planning document(s) support the strategy for increased reliance upon automated systems reflected in the Business Plan.
- Emphasize the importance of contingency planning in all levels of the Agency to ensure service performance goals established in the Business Plan would be achieved in the event of contingency.
- Proactively promote awareness within SSA's organizational components of the importance of contingency planning for SSA systems.
- Encourage and support attendance by their staff at the weekly and monthly planning and status meetings.
- Include SSA Systems Security staff in contingency planning, since their office establishes the policy for SSA's contingency planning program.
- Continue corrective actions identified in prior OIG audit recommendations. Specifically, SSA needs to begin planning for a long-term outage and detail the transition steps from disaster recovery back to normal operations.

³ A hot-site is a remote facility already fully equipped for data processing that several users share.

- Perform a cost-benefit analysis to determine the feasibility of processing death notices as a critical workload.
- Document a policy for handling walk-in clients while the systems are being recovered at the hot-site.

AGENCY COMMENTS AND OIG RESPONSE

With the exception of the following comments, SSA concurred with our findings and recommendations. (See Appendix B for the full text of SSA's comments.)

- SSA did not agree with the portion of our eighth recommendation suggesting that SSA perform a risk assessment of the NCC. SSA contends that it has a program in place, which would normally call for a contractor to perform a risk assessment of the NCC on a regular 5-year cycle. However, the Agency has suspended its risk assessment efforts in an attempt to address concerns previously identified by OIG and its contract auditors. SSA believes it would be cost-beneficial to correct the vulnerabilities already identified before engaging a contractor for further risk assessment.
- With respect to our 19th recommendation, since June 1998, when we concluded our field work, SSA has completed corrective action and included death notices as a critical workload.

In addition, SSA provided general comments explaining the increased focus the Agency has placed on contingency planning. As such, the Agency recommended that references made to the Division of Systems Security be changed to the Office of Systems Security.⁴ SSA believes this organizational change reflects the emphasis it has given to systems security, including contingency planning. However, to appropriately reflect the control environment that existed at the time of our audit, we will retain the current language.

We commend SSA's recent efforts to improve its contingency planning program, and we encourage SSA to continue its commitment. Further, we understand the reasoning for implementing some corrective actions before initiating others. As such, we concur that SSA should wait until its corrective actions are complete before conducting any further risk assessment.

⁴ After our review, SSA changed the name of the Division of Systems Security to the Office of Systems Security.

TABLE OF CONTENTS

| | Page |
|--|------|
| EXECUTIVE SUMMARY..... | i |
| INTRODUCTION..... | 1 |
| RESULTS OF REVIEW..... | 5 |
| SSA'S CONTINGENCY PLANNING PROGRAM LACKED FUNDAMENTAL INFRASTRUCTURE ELEMENTS | 5 |
| CONTROLS WITHIN SSA'S CONTINGENCY PLANNING PROGRAM WERE INADEQUATE | 9 |
| SSA HAD NOT RESOLVED OPEN RECOMMENDATIONS FROM PREVIOUS AUDIT REPORTS..... | 16 |
| CONCLUSIONS AND RECOMMENDATIONS | 17 |
| | |
| APPENDICES | |
| APPENDIX A – Acronyms | |
| APPENDIX B – SSA's Comments | |
| APPENDIX B – Major Contributors to this Report | |
| APPENDIX C – SSA Organizational Chart | |

INTRODUCTION

OBJECTIVE

The objective of this audit was to assess the effectiveness of the Social Security Administration's (SSA) contingency planning program to mitigate the impact of unexpected events that could interrupt service delivery throughout SSA.

BACKGROUND

An agency's ability to safeguard its information resources is a critical element of its management controls. Contingency planning is a key management control for protecting information resources against loss or damage because it ensures the continuity of operations in the event of any interruptions in operation.

SSA's information resources are principally supported by the National Computer Center (NCC). The NCC is a large data processing facility that is managed by SSA's Deputy Commissioner for Systems. The NCC receives, processes, and/or stores about 20 million program transactions a day at its Baltimore, Maryland, location. These transactions contain sensitive beneficiary data that are submitted by SSA's nationwide telecommunications network, which supports over 1,300 field offices. SSA depends on the NCC and its communications network to accomplish its mission of service to beneficiaries.

The Computer Security Act of 1987 (Computer Security Act), Public Law 100-235, 101 Stat. 1724, designates responsibility for developing standards and guidelines for Federal computer security programs to the National Institute of Standards and Technology (NIST). NIST guidance for contingency planning documentation and risk management of Federal systems is promulgated in NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*. As defined by NIST, contingency planning should address all the resources needed to perform a function, regardless of whether the functions directly relate to a computer. Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources* (OMB A-130), implements the requirements of the Computer Security Act and other statutes, including the Privacy Act and the Paperwork Reduction Act of 1995. OMB A-130 requires that Federal agencies implement contingency planning documentation and risk management consistent with NIST guidance for protecting Federal information resources against unavailability.

To comply with NIST and OMB guidance, SSA has implemented some components of a contingency planning program. These components include a contingency planning policy, the Emergency Response Procedure (ERP), the Backup and Recovery Plan (BRP),⁵ and the Business Plan.

SSA's Division of Systems Security (DSS), under the Deputy Commissioner for Finance, Assessment, and Management, is responsible for developing a contingency planning policy. SSA's contingency planning policy is published in the *SSA Systems Security Handbook* (Handbook).

The ERP establishes the actions to be taken by key SSA offices and personnel after a catastrophic event that threatens the data processing operations at the NCC. In addition, the ERP provides milestone events that dictate the maximum allowable times for conducting emergency response activities.

SSA developed the BRP to lessen SSA's loss in service and productivity in case of a catastrophic event at SSA's NCC. The Office of Telecommunications and Systems Operations (OTSO), under the Deputy Commissioner for Systems, is responsible for executing the BRP. To lessen the effect a catastrophic event would have on the NCC's operations, the BRP:

- provides for the NCC processing activity to be moved to a remote contract facility equipped to process critical SSA workloads;
- defines the support role for each Deputy Commissioner's component in the event of a catastrophic event at the NCC; and
- provides instructions for testing and back-up facility operations, outlines data processing and communications environments, lists systems to be restored, states the processing limitations, and contains the implementation procedures for staff to follow during recovery of critical systems.

Aggressive customer service performance measures set by SSA in its Business Plan establish the expectation of prompt service to millions of beneficiaries. SSA's Business Plan complements and integrates SSA's long-range strategic planning with short-term tactical plans and other planning documents. The Business Plan establishes customer service as a pre-eminent driver of SSA strategy, describes critical enablers, and includes an assessment of core business processes. The Business Plan describes SSA's planning framework, critical elements of SSA's strategy, agency performance

⁵ Officially entitled, *Backup Plan for National Computer Center Operations*, SSA staff commonly refer to it as the *Backup and Recovery Plan*, *Backup and Recovery Plan for the National Computer Center (NCC) Operations*, and *Disaster and Recovery Plan*.

measures, key performance initiatives, and impact of the Business Plan on SSA's service to the public. Achievement of SSA's customer service goal is critically dependent on the availability of SSA's systems.

SCOPE AND METHODOLOGY

We originally initiated this audit to determine whether SSA had addressed contingency planning weaknesses that were identified in a prior Office of the Inspector General (OIG) report, *Review of the Back-Up and Recovery Procedures at the National Computer Center (A-13-96-11052)*, June 1997, on SSA's back-up and recovery procedures implemented in the event of a disaster. That report stated that SSA needed to:

- begin planning for a long-term outage,
- perform a cost-benefit analysis to determine the feasibility of processing death notices as a critical workload, and
- establish a clear policy for handling walk-in clients while the system is being brought up at the hot-site.

Since the release of that report, OIG contracted with Price Waterhouse, LLP (PW),⁶ to audit SSA's Fiscal Year (FY) 1997 and 1998 Annual Financial Statements. As a part of these audits, PW evaluated SSA's internal control structure and reported significant deficiencies. In its FY 1997 and 1998 Reports on Internal Controls, PW identified deficiencies in SSA's disaster recovery element of service continuity as a reportable internal control weakness. A reportable internal control weakness is a matter that, in the auditor's judgment, should be communicated because it represents a significant deficiency in the design or operation of internal controls, which could adversely affect the entity's ability to meet its internal control objectives.

PW's designation of disaster recovery as a reportable internal control weakness raised concern about the exposure of SSA's operations to disastrous interruptions in service, but does not address interruptions of a lesser nature. Therefore, we expanded the scope of this audit to focus on the overall effectiveness of SSA's contingency planning program.

In determining the extent to which SSA had an effective contingency planning program in place to address program deficiencies, we determined whether: (1) SSA's contingency planning program was in compliance with Federal requirements and (2) SSA's planning documents were consistent with its contingency plan. To determine

⁶ Now known as PricewaterhouseCoopers.

SSA's compliance with Federal requirements for contingency planning, we compared the regulatory criteria contained in the Computer Security Act, OMB A-130, and NIST Special Publication 800-12 to:

- the SSA BRP, and
- a non-statistical sample of component contingency plans, including *The Social Security Administration's Y2K Business Continuity & Contingency Plan*, the contingency plan for loss of mainframe processors at the NCC, and the contingency elements of Sensitive System Security Plans and Field Office Security Action Plans.

We also compared:

- the above regulatory criteria to the requirements of the Handbook;
- contingency planning aspects of SSA planning documents (such as the BRP, draft ERP, and Business Plan) and the SSA Information Systems Plan for consistency; and
- Brown and Company, LLP's,⁷ 1994 NCC risk assessment to Federal guidelines for risk management/assessments.

To determine the extent and effectiveness of management's involvement in contingency planning, we sat in on SSA contingency planning meetings and interviewed SSA staff involved in contingency planning activities. We will address the evaluation of SSA's testing of the BRP and contractor support of SSA contingency planning activities in subsequent OIG audit reports.

We conducted the audit field work from April through June 1998 at SSA Headquarters and the NCC in Baltimore, Maryland. We conducted this audit in accordance with generally accepted government auditing standards.

⁷ SSA contracted with Brown and Company, LLP, (a certified public accounting firm) to perform an objective risk assessment (Prime Contract Number 600-93-0062, Task Order 4, September 1993 through May 1994). The purpose of the assessment was to determine the NCC's security status to satisfy SSA's requirement to conduct a risk assessment every 3 years under Federal criteria and SSA's financial systems review program. Specifically, Brown and Company was tasked to identify and assess specific threats and NCC vulnerabilities, identify the value of potential losses, identify and evaluate potential safeguards, conduct a cost/benefit analysis, and recommend safeguards for implementation at the NCC.

RESULTS OF REVIEW

Although SSA has some controls in place to mitigate the impact of interruptions in the data processing function at the NCC, these controls only focus on widespread catastrophic events and do not address interruptions of a lesser nature. Specifically, we found that the infrastructure for SSA's contingency planning program lacked fundamental elements, and controls within SSA's contingency planning program were inadequate. In addition, SSA had not resolved several open issues from our 1997 report. These findings are discussed in detail in the following pages.

Our audit included a review of the methodology for *The Social Security Administration's Y2K Business Continuity & Contingency Plan*. The Plan is limited to planning for Year 2000 contingencies; however, it does demonstrate a useful foundation upon which to build a contingency planning infrastructure for SSA. If SSA applied this methodology and expanded on the information already available from the project to identify information assets, assess risk, and implement risk mitigation for all SSA systems, we believe SSA would have a good start on effective contingency planning.

SSA'S CONTINGENCY PLANNING PROGRAM LACKED FUNDAMENTAL INFRASTRUCTURE ELEMENTS

SSA's contingency planning program lacked fundamental infrastructure elements that are prescribed by Federal guidelines. This occurred because (1) SSA's contingency planning program did not clearly establish roles and responsibilities for each component and (2) SSA's BRP did not comply with NIST criteria or with SSA's own definition. This inhibited SSA's ability to mitigate the impact of unexpected events that could interrupt service delivery.

Fundamental to a strong contingency plan is an infrastructure that adheres to Federal contingency planning requirements. An infrastructure is the basic framework that supports the contingency plan. OMB Circular A-130, implementing the requirements of the Computer Security Act, requires agencies protect Federal information resources and document, in security plans, their controls for the continuity of operations (that is, contingency planning controls). These controls should cover all general support systems (such as local area networks) and all major applications (such as the Old-Age, Survivors and Disability Insurance Initial Claims System). Processing alternatives (such as reverting to manual processing or purchasing redundant resources) are to be considered and the selected alternatives documented in the security plans.

A contingency planning infrastructure establishes program accountability, assigns process responsibilities, and implements procedures and technology to support the program. This infrastructure is reinforced by the program's framework, which is established by the methods implemented by senior management for:

- risk management to analyze security costs and benefits of contingency planning options and identify critical resources needed to support the organization in the event of a contingency;
- physical and environmental controls to prevent contingencies from major threats such as fire, loss of power, or natural disasters;
- incident handling and emergency response to various technical threats and prevent future incidents; and
- support and operations for recovery of systems from common contingencies, such as disk failure or corrupted data files.

SSA Had Not Established a Strong Contingency Planning Infrastructure

SSA's contingency planning program did not have a strong infrastructure in place to support an effective program to minimize interruptions in the availability of SSA systems. Specifically, SSA had not established and communicated a consistent understanding of contingency planning to all SSA staff, accountability for SSA contingency planning, and explicit roles and responsibilities for the planning process. Therefore, SSA was not in compliance with Federal requirements, which require the development of a contingency planning program. As a result, SSA may not be prepared in the event of a disruption in critical mission and business functions for any duration, such as a hurricane or a tornado.

SSA staffs did not have a consistent understanding of what constitutes the SSA contingency planning program. Our discussions with SSA's Office of Systems (OS) and DSS staffs and our review of SSA's contingency planning policy revealed that there was no clear understanding of the concept of contingency planning. The Handbook defines contingency planning as ". . . the process for assuring, in advance, that any reasonable and foreseeable disruptions will have a minimal effect" [emphasis added]. The Handbook also provides that an organization must minimize, and prepare to recover from, any disruption that occurs. However, the Handbook states that SSA's BRP and ERP combined meet SSA's definition when, in fact they do not. They are elements of the contingency planning program. All staff interviewed believed the BRP was SSA's contingency plan. Based on this, we concluded that SSA makes no distinction between contingency planning (processing alternatives to overcome interruptions of any nature) and disaster recovery planning (strategy for recovery from catastrophic events). Training in contingency planning was not conducted, which contributed to the lack of understanding by the staff involved. Without defining and communicating a consistent

understanding of SSA's contingency planning policy to all SSA staff, we believe SSA has no reasonable assurance that an effective contingency planning has been implemented.

SSA staffs were not consistent in their understanding of who, if anyone, had overall program accountability or component responsibility for processes within the program. Contingency planning involves all SSA components (such as Systems, Operations, and Financial Assessment and Management components). A formal focal point for program accountability and a definition of individual responsibilities for all components are necessary to ensure consistent program implementation SSA-wide and to coordinate the effective development of all contingency plans.

Our discussion with SSA's OS and DSS staffs revealed that there was no clear understanding as to which components were responsible for program functions. For example, DSS established the contingency planning policy but deferred to OTSO for executing the policy. OTSO staff only claimed responsibility for executing the BRP for disaster recovery. To add to the confusion, the Handbook assigned responsibility for maintaining and executing the BRP to the Facilities Operations Managers, but OTSO actually performs duties with regard to disaster recovery of the NCC. This lack of clearly defined roles and responsibilities minimizes the effectiveness of SSA's contingency planning program.

Management must take the lead in resolving accountability issues to ensure that an effective contingency planning program is implemented. Strong leadership is needed to ensure the program complies with Federal requirements and reduce SSA's exposure to the potential damage caused by service interruptions.

SSA's Contingency Plan Was Not Consistent With NIST Guidance

SSA staff did not distinguish the contingency planning policy from its disaster recovery plan—the BRP. SSA staffs we interviewed were not aware of NIST guidance for contingency planning. Because the BRP is the primary component of SSA's contingency planning program, we compared SSA's BRP to NIST contingency planning criteria and determined that the BRP did not meet NIST guidelines, as detailed below.

Identification of Mission-Critical Functions. One of the six steps in the contingency planning process NIST recommended is identifying critical business process workloads on which contingency efforts are to be focused. In the BRP, SSA lists "Critical Workloads" and "Workloads to be Processed." SSA staff could not explain the difference between these two workloads nor could they crosswalk one list to the other. Some of the workloads listed under "to be processed" did not correlate to any item on the "critical workload" list. Without a clear identification of mission-critical workloads, some of SSA's critical functions may be omitted from the contingency program, which could lead to significant interruptions in service to beneficiaries.

Identification of Resources That Support Critical Functions. NIST states that, “Contingency planning should address all the resources needed to perform a function, regardless whether they directly relate to a computer.” However, SSA’s BRP did not identify all resources, such as hardware and software identification, critical resource time frames,⁸ human resources, or supplies. In addition, there was no clear prioritization of these resources. NIST advises that an analysis of needed resources and their dependencies allows an organization to assign priorities to resources since not all elements of all resources are crucial to critical functions. Without identification and prioritization of specific resources and workloads for contingency activities, SSA’s successful recovery of activities in their appropriate order may not be fully achieved in a timely manner. This could result in loss of benefits to millions of people who depend on SSA to sustain their quality of life.

Anticipation of Potential Contingencies or Disasters. NIST recommends that Federal agencies identify a likely range of problems in their planning programs. Examples of these problems include whether: (1) people can get to the NCC or remote recovery site, (2) surviving personnel will have sufficient knowledge to recover the systems, (3) only a portion of the computer hardware is operational, or (4) the event affected data integrity—such as from a sabotaged application or virus. Without considering the full spectrum of possible events, SSA’s mission-critical functions may be subject to unanticipated service interruptions.

Select Contingency Planning Strategy. In evaluating cost-effective alternatives, management must consider those controls that are in place to prevent and minimize contingencies. Coordination of emergency response, critical systems recovery, and business resumption activities are elements of a contingency planning strategy. For example, depending on the results of risk assessments and cost-benefit analyses performed, an organization may strategize that it is more cost-effective to focus on contingency prevention controls than investing in expensive recovery facilities. SSA’s strategy was to invest in a recovery facility. However, SSA’s document for recovery operations at the facility, the BRP, was not kept current as recommended by NIST. In fact, SSA’s BRP requires that updates be performed as SSA increases its automated functions, at the completion of testing, each year in January, and when the critical business process workloads have changed. However, we found that:

- the only update to the BRP was at the completion of testing⁹ in 1997,
- the BRP reference to OMB A-130 was not up-to-date, and
- the BRP had not been updated to reflect September 1997 changes in recovery functions related to daily shipments to the off-site tape storage facility.

⁸ The time it takes to have critical resources in place and functioning at a hot- or cold-site.

⁹ SSA tested the BRP February 28 through March 2, 1997, and updated the BRP in August 1997.

Without an up-to-date BRP, SSA cannot ensure its compliance with Federal regulations or be prepared to recover systems for which recovery resources have changed.

Implementing Contingency Strategies. NIST recommends that the contingency planning program clearly state in simple language the sequence of tasks to be performed in the event of a contingency so that someone with minimal knowledge can immediately begin executing the plan. The BRP did not describe recovery steps in simple language or provide detailed procedures for implementing each step. Instead, the BRP provided a generic overview of what the end result of each step was expected to be. Without detailed recovery procedures, the availability of experienced and knowledgeable staff to recover processing of critical systems becomes a necessity. However, in the event of an actual disaster, this staff may not be available. In addition, SSA did not maintain copies of all existing contingency plans and detailed recovery procedures at an off-site,¹⁰ protected facility, such as the hot-site, as recommended by NIST. Without adequate documentation available at an off-site facility, SSA cannot be assured of effective recovery of all SSA core business processes in the event of a disaster.

CONTROLS WITHIN SSA'S CONTINGENCY PLANNING PROGRAM WERE INADEQUATE

Contingency activities were not adequately documented for all SSA components, systems, and field offices. In addition, SSA had not adopted Federal criteria for risk management of Federal systems. Improvement is needed to effectively correlate other SSA planning documents, such as the ERP and the Business Plan, to SSA's contingency strategy. Finally, SSA has initiated increased management support of contingency planning activities to implement an effective program since we completed our field work, but more action need to be taken.

SSA's controls to mitigate the impact of interruptions in SSA's data processing functions were neither complete nor consistent with Federal criteria. We reviewed the extent to which component and SSA contingency planning is addressed in the following SSA documentation:

- Office of System's *The Social Security Administration's Y2K Business Continuity & Contingency Plan* and the contingency plan for loss of mainframe processors at the NCC;
- Office of Finance, Assessment, and Management's Sensitive System Security Plans contingency elements;
- Office of Operation's Security Action Plans for Field Offices;

¹⁰ Facility that is sufficient distance from the NCC so as not to fall victim to a mutual disaster impacting a larger area than just the NCC (such as a regional weather disturbance).

- The policy in the Handbook provides some information regarding the program definition and responsibilities; and
- The ERP addresses initial disaster determination and notification procedures after a catastrophic event at the NCC.

NIST considers contingency planning to consist of three parts: initial emergency response to an event, recovery of critical functions to maintain continuity, and resumption of normal activities. SSA addresses the emergency response element of contingency planning with the ERP. The BRP addresses disaster recovery procedures for immediate hot-site operations only in the event of major outage of the NCC. As of the end of field work, SSA did not have a document to address resumption of normal activities.

Without adequately addressing each of the three parts of a contingency plan, we believe SSA has no reasonable assurance that interruptions in service to beneficiaries will be mitigated.

SSA Did Not Have Component or System-Level Contingency Plans Consistent With Federal Criteria

SSA had not developed contingency plans for significant SSA components or systems that complied with NIST guidance because they were unaware of the NIST guidance for documentation of the plans. Of the documents we reviewed, the SSA Year 2000 contingency plan was the closest SSA had to a well-documented contingency plan. The Year 2000 plan generally demonstrates a logical, industry-accepted method of risk management and contingency planning. The Year 2000 contingency plan refers to local contingency plans intended to provide more detail for the SSA core business processes and systems. However, SSA personnel stated these local plans had not yet been developed.

The contingency elements of system security plans and Field Office Security Action Plans did not comply with NIST guidance for contingency plan documentation. SSA management could not readily provide us additional component-level contingency plan documents. According to NIST, organizations may have one overall plan, or one overall plan that addresses each component or individual plans that address each system, application, regional office, or other remote node, such as field or state offices integral to the business processes. Regardless of the approach used by an agency, the plan or plans should be documented in the agency's policies and procedures. Without adequately documented component contingency plans, SSA cannot be reasonably assured of continued service to the public through effective recovery of all SSA core business processes in the event of a regional or localized disaster.

SSA's Systems Security Contingency Planning Policy Was Inadequate

SSA's BRP contains a disaster recovery plan to address major outages at the NCC. Most staff interviewed believe SSA's BRP is the same as SSA's contingency plan. Likewise, SSA's systems security policy considers the BRP to be SSA's contingency plan. However, the BRP is actually part of the contingency plan.

The contingency planning policy in the Handbook does not reflect NIST guidance for contingency planning. NIST recommends that a policy be developed to create and document the organization's approach to contingency planning, and that the policy explicitly assign responsibilities. However, SSA's systems security policy was based on obsolete requirements for contingency planning and risk management. Without strong policy guidance, SSA cannot establish a strong contingency planning infrastructure. In the absence of clear guidance, any resulting contingency plan will not effectively ensure that processing interruptions will be minimized. The following describes inadequacies of SSA's policy.

Handbook References Needed Updating. The Handbook contains numerous references to "detailed guidance" intended to assist SSA staff in performing system risk analyses. However, the Handbook contained a reference to the obsolete OMB Bulletin 90-08, *Guidance for the Preparation of Security Plans for Federal Computer Systems That Contain Sensitive Information*, and the current NIST guidance was not even listed. In addition, the reference to OMB A-130 was for the 1985 version and did not reflect the 1996 revised requirements.

The Handbook also addresses security plans, as required by the Computer Security Act. Again, regulatory references to OMB were obsolete, and NIST requirements were omitted. DSS staff were aware of some of the obsolete references to OMB A-130, but they were not aware of NIST guidance. They were also unaware that OMB Bulletin 90-08, *Guidance for the Preparation of Security Plans for Federal Computer Systems That Contain Sensitive Information* and NIST's Federal Information Processing Standard 65 had been replaced. Without referencing the most current guidance developed for the latest technology, SSA's contingency plan is not likely to have the most current and effective procedures to minimize disruptions.

The Handbook Did Not Address OMB A-130 Documentation Requirements. The Handbook did not address the 1996 revised OMB A-130 requirements for security plans for all general support systems and major applications because the DSS staff was unaware of changes in Federal requirements and did not update the policy. OMB A-130 requires that contingency plans be documented in agency security plans. Because SSA did not document security plans for all general support systems and major applications, there was no corresponding documentation of the related contingency plans. Therefore, SSA did not meet the OMB requirement for general support systems security plans to include a "continuity of support" element to define service provisions and restoration priorities. Further, SSA did not meet the requirement

for major application security plans to include a “contingency planning” element to define SSA’s ability to perform functions supported by certain applications in the event of an interruption. If OMB documentation requirements are not implemented in SSA’s system security program and communicated to SSA employees, there can be no assurance that SSA has identified and properly documented contingency plans for all general support systems and major applications to keep them in operation.

SSA Policy Did Not Adequately Define Roles and Responsibilities. The SSA contingency planning policy contained in the Handbook was vague because the DSS staff was unaware of NIST requirements and did not update the policy. Contingency planning was defined in the Handbook, but roles and responsibilities described for the process were generic. The only specific role identified was that of the SSA System Security Officer (SSASSO), who issues policy and guidelines for SSA contingency planning. Our discussion with staff in DSS confirmed that there was fragmentation of contingency planning responsibilities among DSS, OTSO, and Regional Operations components. Without a clear definition of roles in the process and assignment of responsibilities, there is no accountability for ensuring that the contingency planning functions are completed and the plan is tested and fully operational.

SSA’s Systems Risk Management Program Needed Improvement

OMB Circular A-130, implementing the requirements of the Computer Security Act, specifies that risk management is an element of the contingency planning program to maintain systems availability. However, SSA was unaware of current NIST guidance for contingency planning and had not instituted in its written policy the NIST guidance (or a method consistent with NIST’s) for risk management that requires:

- determining the assessment’s scope and methodology (such as the technical and operational controls of a new application, the use of telecommunications, a data center, or an entire organization);
- collecting and analyzing data regarding asset valuation, threat identification, vulnerability assessment, safeguard analysis, consequence assessment, and likelihood of occurrence; and
- interpreting the risk analysis results to select cost-effective controls and accept residual risk of not implementing protective controls.

Furthermore, SSA had not performed a risk assessment since the Brown and Company May 1994 assessment of the NCC. OMB requires that risk assessments be performed in conjunction with reviews of controls when significant changes are made to a system or application, or at least every 3 years. SSA had not adequately identified and assigned value to critical resources needed to support its program service functions. As indicated in NIST guidance, risk management is the foundation of a computer security program and recommends that risk management be a tool for analyzing the security costs and benefits of various contingency planning options. Risk management

identifies the assets to be protected as well as the threats and likelihood of occurrence, and it values the assets for determination of cost-beneficial protection measures. By using obsolete risk management information, SSA is not ensured that the appropriate or most complete and cost-effective contingency strategy is in place.

SSA's ERP for a NCC Disaster Needs Improvement

The ERP is one of the primary service continuity controls in place at SSA. However, SSA had not finalized this critical document, which PW identified as a deficiency in its FY 1997 Report on Internal Controls. Key assumptions upon which the ERP was based were not reasonable. Furthermore, the emergency contact information in the ERP was inaccurate and incomplete. In addition, the ERP did not provide adequate detailed procedures to be followed by emergency teams when the ERP is activated. Finally, the ERP's staffing requirements were not coordinated with the BRP. Without planned staff requirements and clear procedures, SSA may not be able to implement its contingency plan.

Some of the Assumptions Cited in the ERP Were Not Reasonable. The ERP states most key personnel to implement the ERP are located in the NCC. The ERP assumes that (1) all key NCC personnel will be available in the event of a disaster and (2) the disaster will be confined to the NCC. These assumptions seem to be contradictory. If the disaster has a catastrophic affect on the NCC, it can reasonably be assumed that at least some, if not all, key personnel as well as their primary and secondary backups will be adversely affected, unless the disaster occurs during off-duty hours. SSA management believes the likelihood of such a worst-case scenario is remote. In addition, the ERP does not consider natural disasters that may cover a wide area that could prevent personnel from getting to the NCC or the recovery site. Without considering the full spectrum of possibilities, SSA may not be prepared to recover its critical systems in the event of a disaster.

The ERP Was Not Accurate or Complete. Emergency team contact information was not accurate for 8 of the 27 staff assigned to Administrative Support, Facilities Emergency, Transportation/ Supplies/Warehousing, Personnel, Contracting, Emergency Preparedness, and Finance Teams in the draft ERP provided for our review. For example, the phone number of the primary contact for the payment delivery alert systems activity, and the contact information for four (three of which are primary contacts) of six staff in contracting are not correct. Also, the ERP provided for our review was not yet final. For example, some pages had statements such as "This information to be developed," or "insert . . . team call roster." SSA was working to finalize the document. We could not determine why these critical documents were inaccurate or complete. However, without accurate and complete contact information in the ERP, we believe SSA may experience delays in notifying primary contacts. Similarly, these delays may impact SSA's ability to implement its ERP procedures in a timely manner.

The ERP Did Not Contain Detailed Procedures. The ERP did not contain detailed procedures for administrative and logistic support because the DSS staff was unaware of NIST requirements and did not update their policy. SSA expanded on this element to include activation of some support activities, but the ERP did not describe the steps to be taken to continue support during recovery. NIST recommends that the initial actions taken to protect lives and limit damage be documented in the emergency response element of the contingency planning program. In addition, NIST recommends agencies address steps to continue support activities during recovery and steps to take to return to normal operations.

The ERP assumes that the emergency will be from 3 to 30 days whereas the BRP assumes NCC outages from 42 days to 6 months. Furthermore, the ERP instructs that, in the event insufficient volunteers are available to go to the remote back-up processing facility, the staff selected will “. . . likely be those with the latest service computation date,” meaning those with the least service. We believe more experienced SSA staff should be directed to go to the facility to minimize recovery time for SSA's critical systems. Without knowledgeable staff at the hot-site, errors and delays most likely would occur due to inexperience with the systems or the recovery process.

Generalized activities are described in the ERP, such as “keep adequate supplies of printed materials on hand,” or “contact OAG [Office of Acquisition and Grants] representative for any purchase or leases needed.” Without clear steps for continuing support activities during recovery or for resumption of normal business processing, continuity of SSA systems could be significantly impaired.

SSA's BRP Needed to Provide for Business Plan Strategies

In its Business Plan, SSA documents measurable customer service performance goals and long-term expectations. Contingency planning must consider this business strategy to ensure that all potential interruptions in services critical to the achievement of these goals are addressed. Unavailability of SSA systems may cause public distrust in SSA's reliability to perform its mission.

SSA's Business Plan emphasized increased use of automation of manual processes for efficiencies, electronic service delivery options for customers, and use of networked workstations and distributed software by employees. In addition, SSA has established performance measures to comply with the Government Performance and Results Act of 1993, Public Law 103-62, 107 Stat. 285, that rely heavily upon the availability of SSA systems. The increased dependency of SSA's performance on automated services directly impacts its contingency planning program.

In the Business Plan, SSA acknowledged that its employees' ability to keep up with their work would be seriously diminished if automation were unavailable. However, the BRP had not been updated to address contingencies for these critical workloads or to ensure adequate resources and processing capacity is available at the back-up

recovery facility. Finally, none of the planning documents we reviewed (such as the BRP, ERP, or Business Plan) addressed detailed resumption activities for SSA's return to normal business operations after a disaster. Without adequately planned recovery resources and a plan to return to normal business operations, service to the public may be more adversely affected than is necessary. Also, SSA cannot ensure achievement of the customer service performance goals established in the Business Plan in the event of a contingency (of any magnitude) that could interrupt processing of critical SSA services.

Increased Management Support for Contingency Planning Activities Was Needed

The SSA staff members invited to attend weekly and monthly planning and status meetings did not always attend, and all essential SSA components were not invited to these meetings. The monthly NCC back-up and recovery meetings provide a forum for senior-level managers to obtain an update on the status of activities. However, we observed that, at April's meeting, only 8 of 28 managers (29 percent) attended, and the May and June meetings were canceled and not rescheduled. Meeting minutes distributed to all invitees documented that poor attendance was a problem for the 2 critical months before the BRP's annual test. Finally, all essential SSA components were not included in the meetings. For example, the SSASSO was not invited to either the monthly or weekly meetings. Participation by the SSASSO's staff may have prevented deficiencies in compliance of SSA's contingency planning program with Federal regulations because the SSASSO issues guidelines for SSA's contingency planning.

Management support of attendance by all organizational components is needed to implement an effective contingency planning program and provide awareness for all SSA organizations of the importance of contingency planning in daily activities. Without the participation of all organizational components in the planning meetings, SSA cannot be assured that unique requirements have been included in the test. In the event of a disaster, these unique requirements may be critical to the successful restoration of service to the public. Since the completion of our field work, SSA management has notified us that it has formed an Agency Contingency Planning Workgroup with representatives from each Deputy Commissioner's office. SSA established the Workgroup to conduct a Business Impact Analysis and to make recommendations for the new Agency Contingency Plan.

SSA HAD NOT RESOLVED OPEN RECOMMENDATIONS FROM PREVIOUS AUDIT REPORTS

SSA has achieved progress since we issued the 1997 audit report; however, there are still open actions that SSA needs to resolve. Our 1997 report recommended and SSA agreed that it would:

- begin planning for a long-term outage of more than 42 days—SSA has limited references in the BRP to extend operations for up to 6 months,
- perform a cost-benefit analysis to determine the feasibility of processing death notices as a critical workload—SSA has not completed the analysis, and
- document a contingency plan for handling walk-in clients during a disaster event—SSA has not completed this contingency plan.

These issues still need to be addressed to provide effective service to the public in the event of a disaster.

CONCLUSIONS AND RECOMMENDATIONS

Based on our findings, we do not believe SSA's overall contingency planning program fully complies with Federal contingency planning guidelines. As such, we question the effectiveness of SSA's contingency planning program to mitigate the impact of unexpected events that could interrupt service delivery throughout SSA.

SSA has some service continuity controls in place, and its contingency plan for Year 2000 compliance provides a foundation on which it can build its overall contingency planning program. However, SSA still needs to ensure the protection of all general support systems and major applications from service interruptions of any magnitude. SSA needs to establish a strong contingency planning infrastructure to support an effective contingency planning program, with increased management support for contingency planning activities.

Although many of our recommendations are focused at the systems component of contingency planning, SSA must recognize that contingency planning involves every component of the Agency. SSA's approach for contingency planning should address operational as well as systems issues. As such, all SSA components must coordinate their plans to ensure that all critical elements of business continuity are addressed.

Once SSA has developed an overall contingency planning program, it must test the plan to ensure the plan adequately addresses service continuity needs. Without complete and fully tested contingency plans, we believe SSA will likely be unable to provide an acceptable level of service to the public in the event of minor or major disruptions. To improve its contingency planning program, we recommend that SSA:

1. Establish and communicate to SSA staff, a formal infrastructure for the SSA contingency planning program.
2. Adopt NIST guidance for contingency planning; address accountability for the contingency planning process; define the organizational roles and responsibilities for the process functions; and provide for training of SSA staff in contingency planning duties.
3. Adopt and communicate a definition of contingency planning so responsible staff understands the concept.
4. After a defined infrastructure is in place, develop an Agency contingency plan and individual component contingency plans, compliant with NIST guidance for

contingency planning. This effort needs to address and document plans for all SSA general support systems and major applications located throughout the SSA complex, including Central Office components and regional office elements, such as area offices, field offices, and disability determination services.

5. Ensure the BRP is kept current.
6. Document an Agency contingency planning policy consistent with NIST guidance. The policy should address the established SSA contingency planning infrastructure, define explicit roles and responsibilities of specific SSA components, and be clearly communicated to all SSA staff.
7. Ensure that requirements and references within the Handbook are kept current, and add the current definition of OMB A-130 categories of general support systems and major applications to the Handbook to ensure proper security plan documentation.
8. Institute in written policy the NIST standard for risk management of Federal information systems and perform a risk assessment of the NCC that is in compliance with the requirements of OMB A-130, the Handbook, and NIST guidance.
9. Ensure that all general support systems and major applications have current and compliant risk assessments documented.
10. Ensure that the ERP is kept current. Specifically, update the ERP to reflect sound planning assumptions, to ensure current key personnel contact information is included, and to include complete information regarding team contact rosters.
11. Update the ERP to include detailed procedures to be followed by the various teams involved in the event of activation of the ERP.
12. Update the ERP to reflect staffing requirements that correlate to staffing requirements in the BRP, and consider the requirement of more experienced personnel at the hot-site in the event of ERP.
13. Ensure that contingency planning document(s) support the strategy for increased reliance upon automated systems reflected in the Business Plan.
14. Emphasize the importance of contingency planning at all levels to ensure service performance goals established in the Business Plan would be achieved in the event of contingency.
15. Proactively promote awareness within SSA's organizational components of the importance of contingency planning for SSA systems.

16. Encourage and support attendance at the weekly and monthly planning and status meetings.
17. Include SSA Systems Security staff in contingency planning.
18. Continue corrective actions identified in audit recommendations contained in the 1997 report. Specifically, SSA needs to begin planning for a long-term outage and detail the transition steps from disaster recovery back to normal operations.
19. Perform a cost-benefit analysis to determine the feasibility of processing death notices as a critical workload.
20. Document a policy for handling walk-in clients while the system is being brought up at the hot-site.

AGENCY COMMENTS AND OIG RESPONSE

With the exception of the following comments, SSA concurred with our findings and recommendations. (See Appendix B for the full text of SSA's comments.)

- SSA did not agree with the portion of our eighth recommendation suggesting that SSA perform a risk assessment of the NCC. SSA contends that it has a program in place, which would normally call for a contractor to perform a risk assessment of the NCC on a regular 5-year cycle. However, the Agency has suspended its risk assessment efforts in an attempt to address concerns previously identified by OIG and its contract auditors. SSA believes it would be cost-beneficial to correct the vulnerabilities already identified before engaging a contractor for further risk assessment.
- With respect to our 19th recommendation, since June 1998, when we concluded our fieldwork, SSA has completed corrective action and has included death notices as a critical workload.

In addition, SSA provided general comments explaining the increased focus the Agency has placed on contingency planning. As such, the Agency recommended that references made to the Division of Systems Security be changed to the Office of Systems Security. SSA believes this organizational change reflects its emphasis on systems security, including contingency planning. Footnote 4 references the Agency's elevation of security responsibility to an Office level. However, to appropriately reflect the control environment that existed at the time of our audit, we will retain the current language.

We commend SSA's recent efforts to improve its contingency planning program, and we encourage SSA to continue its commitment. Further, we recognize that it is cost-beneficial to implement some corrective actions before initiating others. As such, we concur that SSA should wait until its corrective actions are complete before conducting any further risk assessment.

APPENDICES

ACRONYMS

| | |
|--------|--|
| BRP | Backup and Recovery Plan |
| DSS | Division of Systems Security |
| ERP | Emergency Response Procedure |
| FY | Fiscal Year |
| NCC | National Computer Center |
| NIST | National Institute of Standards and Technology |
| OIG | Office of the Inspector General |
| OMB | Office of Management and Budget |
| OTSO | Office of Telecommunications and Systems Operations |
| PW | Price Waterhouse, LLP |
| SSA | Social Security Administration |
| SSASSO | Social Security Administration System Security Officer |

SSA'S COMMENTS



SOCIAL SECURITY

MEMORANDUM

Date: September 27, 1999

Refer To: S1NA1

To: James G. Huse, Jr.
Acting Inspector General

From: John R. Dyer **JRD**
Principal Deputy Commissioner

Subject: Office of the Inspector General Draft Report,
"Contingency Planning for the Social Security
Administration"--INFORMATION

Attached are our comments to the draft report. Staff questions may be referred to Sandra H. Miller on extension 50372.

Attachment

COMMENTS ON OFFICE OF THE INSPECTOR GENERAL (OIG) DRAFT
REPORT, "CONTINGENCY PLANNING FOR THE SOCIAL SECURITY
ADMINISTRATION" (A-13-98-12022)

Thank you for the opportunity to review and comment on the subject report. We appreciate your recommendations for improvement in this important area. While we generally agree with the substance of the recommendations, the report does not reflect activities and improvements in the Agency's contingency planning since this audit was conducted during April through June 1998.

In addition to providing responses to the specific report recommendations, we have the following general comments regarding the three major areas of concern addressed in the report:

Social Security Administration's (SSA) contingency planning program lacked fundamental infrastructure elements

SSA recently convened an Agencywide workgroup to develop an infrastructure for contingency planning in response to Presidential Decision Directive (PDD) 67. This workgroup will address five of the 20 recommendations contained in this audit report and is expected to present its recommendations by October 1999.

Controls within SSA's contingency planning program were inadequate

SSA has been working to address the control weaknesses identified in this audit report and other reports, such as the audit report for SSA's financial statements for fiscal years (FY) 1997 and 1998. PricewaterhouseCoopers (PwC), the contractor conducting the financial statement audits, indicated that we are making "noteworthy" progress.

SSA had not resolved open actions from previous audit reports

SSA implemented five of the six recommendations contained in OIG report, "Review of the Back-Up and Recovery Procedures at the National Computer Center (NCC)" (A-13-96-11052), June 1997. We decided not to accept the sixth recommendation concerning environmental requirements for handling tape cartridges since we believe that adequate

controls exist in the current method of handling cartridges. To date, a tape failure has never occurred. With respect to the Price Waterhouse audit report, "Social Security Accountability Report for FY 1997," November 1997, SSA has corrected three of the five recommendations. In the audit report for FY 1998, PwC stated that SSA is making noteworthy progress on the remaining two recommendations that require long-term solutions. We will continue our improvements until all corrective actions are completed.

The following are our comments on the specific report recommendations:

1. Recommendation

Establish and communicate to SSA staff, a formal infrastructure for the SSA contingency planning program.

Comment

We agree. In compliance with PDD-67, Enduring Constitutional Government and Continuity of Operations Plan (COOP), SSA has convened an Agencywide workgroup to develop an infrastructure for contingency planning. This includes defining organizational roles and responsibilities, essential operations and staffing, training, maintenance, etc. The actions recommended by the workgroup will be incorporated into the Agency contingency plan, if approved by SSA management.

2. Recommendation

Adopt National Institute of Standards and Technology (NIST) guidance for contingency planning; address accountability for the contingency planning process; define the organizational roles and responsibilities for the process functions; and provide for training of SSA staff in contingency planning duties.

Comment

We agree. As noted in the comment to the first recommendation, this area is being considered by an Agencywide workgroup. Upon receipt of the workgroup's recommendations, SSA will address the areas mentioned.

3. Recommendation

Adopt and communicate a definition of contingency planning so responsible staff understands the concept.

Comment

We agree. As noted in the comment to the first recommendation, this area is being considered by an Agencywide workgroup. After the workgroup's recommendations are considered, we will communicate the definition of contingency planning to responsible staff.

4. Recommendation

After a defined infrastructure is in place, develop an Agency contingency plan and individual component contingency plans, compliant with NIST guidance for contingency planning. This effort needs to address and document plans for all SSA general support systems and major applications located throughout the SSA complex, including central office components and regional office elements, such as area offices, field offices and disability determination services.

Comment

We agree. As noted in the comment to the first recommendation, this area is being considered by an Agencywide workgroup. After the workgroup's recommendations concerning infrastructure are considered, we will ensure that the appropriate contingency plans are developed.

5. Recommendation

Ensure the Backup and Recovery Plan (BRP) is kept current.

Comment

We agree. The Disaster Recovery Plan (DRP) (formerly BRP) is currently updated at least once annually. When the Agencywide workgroup has completed its work and the Agency adopts a COOP, we will determine what, if any, changes are needed to the DRP.

6. Recommendation

Document an Agency contingency planning policy consistent with NIST guidance. The policy should address the established SSA contingency planning infrastructure, define explicit roles and responsibilities of specific SSA components and be clearly communicated to all SSA staff.

Comment

We agree. As noted in the comment to the first recommendation, this area is being considered by an Agencywide workgroup. SSA will address the above areas after considering the workgroup's recommendations.

7. Recommendation

Ensure that requirements and references within the Handbook are kept current, and add the current definition of Office of Management and Budget (OMB) A-130 categories of general support systems and major applications to the Handbook to ensure proper security plan documentation.

Comment

We agree. The Systems Security Handbook is consistent with OMB A-130, Appendix III, and is updated annually. The last update was completed in December 1998. The definitions of OMB A-130 categories will be added in the next update.

8. Recommendation

Institute in written policy the NIST standard for risk management of Federal information systems and perform a risk assessment of the National Computer Center (NCC) that is in compliance with the requirements of OMB A-130, the Handbook and NIST guidance.

Comment

We agree that SSA policy should give full consideration to NIST guidance on risk management and believe that it currently does so. We do not agree with performing a risk assessment of the NCC at this time. SSA has a program in place, which would normally call for a risk assessment of the NCC on a regular 5-year cycle. Historically, a contractor who was a recognized expert in the field

performed the task in accordance with OMB Circular A-130, Appendix III. The last formal risk analysis of the NCC was completed in 1994. Current OMB guidance no longer requires a formal risk analysis. Reviews such as those conducted by OIG and its contractor in conjunction with the annual audit of the financial statements also constitute assessment of risk for NCC operations. A comparison of the work performed by SSA's contractor in 1994 and that performed by OIG and its contractor during the past two years reveals that the latest assessment covered all the areas covered in 1994, plus some.

SSA has deferred engaging a contractor to conduct a risk assessment this year since OIG and its contractor made a thorough examination of the NCC operations over the past 2 years and identified several areas for improvement. SSA believes it would be cost-beneficial to correct the vulnerabilities already identified prior to engaging a contractor for further risk assessment.

9. Recommendation

Ensure that all general support systems and major applications have current and compliant risk assessments documented.

Comment

We agree. All SSA's general support systems and major applications are designated as mission critical and included in the Agency's contingency planning strategy. SSA will ensure that formal risk assessment documentation, as well as documentation on other comparable reviews and audits, are retained.

10. Recommendation

Ensure that the Emergency Response Procedures (ERP) are kept current. Specifically, update the ERP to reflect sound planning assumptions, to ensure current key personnel contact information is included and to include complete information regarding team contact rosters.

Comment

We agree. The ERP is currently updated and distributed quarterly. When the Agencywide workgroup has completed its work and the Agency adopts a COOP, we will determine what, if any, changes are needed to the ERP.

11. Recommendation

Update the ERP to include detailed procedures to be followed by the various teams involved in the event of activation of the ERP.

Comment

We agree. The ERP, which is updated and distributed quarterly, currently includes detailed procedures.

12. Recommendation

Update the ERP to reflect staffing requirements that correlate to staffing requirements in the BRP, and consider the requirement of more experienced personnel at the hot-site in the event of ERP.

Comment

We agree. The ERP now references three teams: emergency response; damage assessment; and operations. The ERP lists those key personnel on the operations team who are prepared to implement emergency procedures. The experience of those persons is commensurate with their responsibilities under emergency procedures.

13. Recommendation

Ensure that contingency planning documents(s) support the strategy for increased reliance upon automated systems reflected in the Business Plan.

Comment

We agree. SSA completed a business impact analysis in February 1999 which validated its critical business processes and processing priorities and most of the

conclusions contained in the analysis were approved by SSA at the Executive Internal Control Committee meeting on February 8, 1999. We are in the process of incorporating the conclusions into SSA's contingency plan.

14. Recommendation

Emphasize the importance of contingency planning at all levels to ensure service performance goals established in the Business Plan would be achieved in the event of contingency.

Comment

We agree. SSA has emphasized the importance of contingency planning at all levels in its efforts to implement corrective actions for the OIG report, "Review of the Back-Up and Recovery Procedures at the NCC," June 1997, and PwC audit reports for the audit of SSA's financial statements for FY 1997 and 1998, November 1997 and 1998.

SSA developed a corrective action plan to address each specific recommendation, assigned staff responsibility for each action and tracked the corrective actions. SSA senior management has monitored the status of those corrective actions through their respective components and ensured that every effort has been made to implement the recommendations. SSA's Executive Internal Control Committee, chaired by the Principal Deputy Commissioner, has also monitored the status of the corrective actions thus emphasizing the importance of contingency planning.

The importance of contingency planning has also been reinforced throughout the Agency through SSA's planning for contingencies as required by PDD-67 and in planning for contingencies for Year 2000.

15. Recommendation

Proactively promote awareness within SSA's organizational components of the importance of contingency planning for SSA systems.

Comment

We agree. SSA will continue to promote awareness of the importance of contingency planning for SSA systems.

16. Recommendation

Encourage and support attendance at the weekly and monthly planning and status meetings.

Comment

We agree. SSA will encourage and support attendance at the planning and status meetings.

17. Recommendation

Include SSA Systems Security staff in contingency planning.

Comment

We agree. The SSA Systems Security staff is currently involved in contingency planning through the publication of contingency planning policy and procedures in the SSA Systems Security Handbook. The staff also participates in weekly and monthly planning and status meetings and the periodic backup and recovery tests.

18. Recommendation

Continue corrective actions identified in audit recommendations contained in the 1997 report. Specifically, SSA needs to begin planning for a long-term outage and detail the transition steps from disaster recovery back to normal operations.

Comment

We agree. SSA will continue to address past recommendations until they are implemented.

SSA implemented five of the six recommendations contained in the OIG report, "Review of the Back-Up and Recovery Procedures at the NCC," June 1997. We decided not to accept the recommendation concerning environmental requirements for tape cartridges. The current practice of acclimating a cartridge to surrounding conditions for a period not greater than 24 hours before processing has never resulted in a tape failure.

With respect to the PwC audit report, "Social Security Accountability Report for FY 1997," November 1997, SSA has corrected three of the five recommendations and is making noteworthy progress on the remaining two recommendations. SSA has developed and documented a strategy to address the worse case scenario, conducted a business impact analysis identifying the critical business processes and processing priorities, and updated its emergency response procedures for the NCC. SSA has made significant progress towards planning for critical scenarios, including long-term outages; identifying capacity requirements; and implementing contractual agreements for satisfying the requirements. SSA has also made significant progress in the testing of critical workloads. SSA has tested all 13 critical processes in the last 3 years and will increase our testing capacities for future tests.

19. Recommendation

Perform a cost-benefit analysis to determine the feasibility of processing death notices as a critical workload.

Comment

We disagree. Death notices were added as a critical workload in late 1998 and are being processed accordingly. This will be documented in the next update of the disaster plan. Since we have already included death notices as a critical workload, a cost-benefit analysis is not necessary.

20. Recommendation

Document a policy for handling walk-in clients while the system is being brought up at the hot-site.

Comment

We agree. The Disaster Recovery Plan for NCC operations was revised to document the policy for handling walk-in clients while the system is being brought up at the hot-site. This provision is contained in Appendix H, Section IV.B, "Operating Policy Until BF is Functioning."

General Comment

The references throughout the report to the Division of Systems Security should be changed to read the Office of Systems Security. This organizational change reflects the emphasis given to systems security, including contingency planning, in the Agency.

MAJOR CONTRIBUTORS TO THIS REPORT

Office of the Inspector General

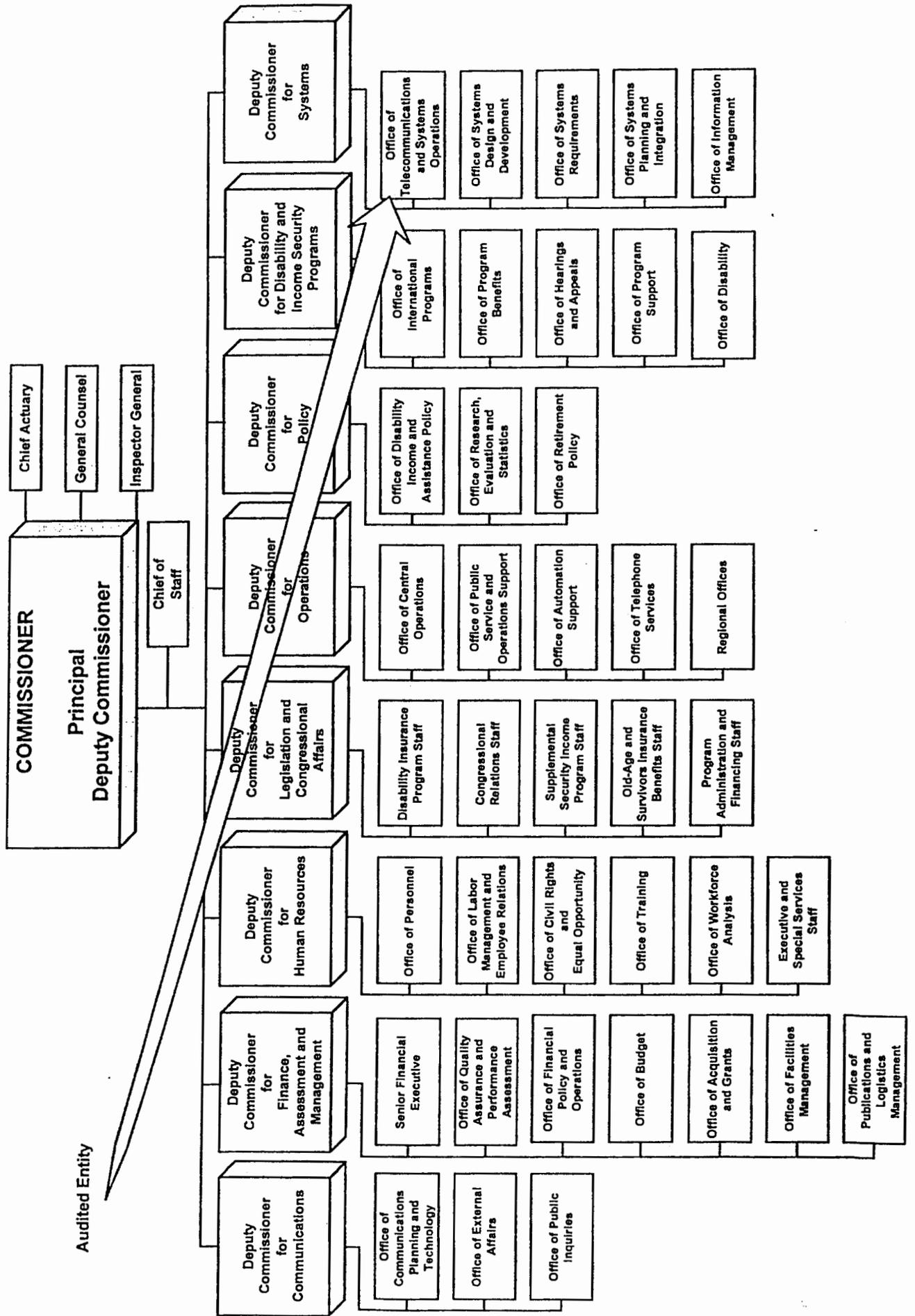
Gale Stone, Director, Systems Audit Division

Nancy DeFrancesco, Senior Auditor

Kimberly Archer-Beauchamp, Writer-Editor

For additional copies of this report, please contact the Office of the Inspector General's Public Affairs Specialist at (410) 966-5998. Refer to Common Identification Number A-13-98-12022.

Social Security Administration



Audited Entity

DISTRIBUTION SCHEDULE

| | <u>No. of Copies</u> |
|--|--------------------------|
| Commissioner of Social Security | 1 |
| Management Analysis and Audit Program Support Staff, OFAM | 10 |
| Deputy Commissioner for Systems | 1 |
| Acting Inspector General | 1 |
| Assistant Inspector General for Investigations | 1 |
| Assistant Inspector General for External Affairs | 3 |
| Acting Assistant Inspector General for Management Services | 1 |
| Acting Assistant Inspector General for Audit | 1 |
| Acting Deputy Assistant Inspector General for Audit | 1 |
| Director, Systems | 1 |
| Director, Financial Management Audits | 1 |
| Director, Program Audits (East) | 1 |
| Director, Program Audits (West) | 1 |
| Director, Program Audits (North) | 1 |
| Director, Management Audits and Technical Services | 1 |
| Issue Area Team Leaders | 16 |
| | |
| Total | <u>42</u> |