OFFICE OF
THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

PROCESSING CAPACITY OF THE SOCIAL SECURITY ADMINISTRATION'S DURHAM SUPPORT CENTER

September 2009 **A-14-09-19100**

EVALUATION REPORT

Mission

By conducting independent and objective audits, evaluations and investigations, we inspire public confidence in the integrity and security of SSA's programs and operations and protect them against fraud, waste and abuse. We provide timely, useful and reliable information and advice to Administration officials, Congress and the public.

Authority

The Inspector General Act created independent audit and investigative units, called the Office of Inspector General (OIG). The mission of the OIG, as spelled out in the Act, is to:

- Conduct and supervise independent and objective audits and investigations relating to agency programs and operations.
- Promote economy, effectiveness, and efficiency within the agency.
- Prevent and detect fraud, waste, and abuse in agency programs and operations.
- Review and make recommendations regarding existing and proposed legislation and regulations relating to agency programs and operations.
- Keep the agency head and the Congress fully and currently informed of problems in agency programs and operations.

To ensure objectivity, the IG Act empowers the IG with:

- Independence to determine what reviews to perform.
- Access to all information necessary for the reviews.
- Authority to publish findings and recommendations based on the reviews.

Vision

We strive for continual improvement in SSA's programs, operations and management by proactively seeking new ways to prevent and deter fraud, waste and abuse. We commit to integrity and excellence by supporting an environment that provides a valuable public service while encouraging employee development and retention and fostering diversity and innovation.

SOCIAL SECURITY

MEMORANDUM

Date: September 30, 2009 Refer To:

To: The Commissioner

From: Inspector General

Subject: Processing Capacity of the Social Security Administration's Durham Support Center (A-14-09-19100)

OBJECTIVE

Our objective was to review the plan, design, status, and data processing capacity of the Social Security Administration's (SSA) Durham Support Center (DSC). This is one in a series of reviews that will address the Agency's future processing needs. This evaluation focused on SSA's strategic planning in the acquisition of the DSC.

BACKGROUND

The DSC is a critical element in SSA's Information Technology Operations Assurance (ITOA) initiative. The purpose of the ITOA initiative is to mitigate inherent risks in the Agency's disaster recovery (DR) strategy by eliminating single points of failure[1] associated with a single national computing facility—the National Computer Center (NCC). The ITOA project was intended to mitigate these risks by establishing a second fully functional, co-processing data center. The project was initiated in response to Agency vulnerabilities identified in a 2002 Lockheed Martin assessment of SSA's DR plan.[2] The assessment concluded that no commercial vendor existed that could meet the Agency's data processing needs in the event of a disaster that rendered the NCC unavailable. It recommended that the Agency explore the feasibility of establishing an SSA DR site or second data center as opposed to using a commercial DR vendor.

In 2005, SSA's Office of Facilities Management worked with the General Services Administration (GSA) to acquire a second data center. SSA identified the following specific requirements for the center:

- 68,200 square feet of space, 36,700 of which is for automated data processing;

[1] A single point of failure is any part of a system that, if it fails, will stop the entire system from working. They are undesirable in any system whose goal is high availability.

[2] Lockheed Martin, *Disaster Recovery Vendor Viability Report,* December 27, 2002.

- acceptable distance from SSA Headquarters and inland; in a low-risk area for natural disasters; not subject to severe climatic conditions; close to electrical utility services that provide at least two separately fed utility substations for power; and close to points of presence for both SSA telecommunications contract providers;
- multiple fundamental fire protection requirements;
- raised floor that is in accordance with industry standards and best practices; and
- meet Department of Justice, Office of Management and Budget, and Interagency Security Committee (ISC) requirements for security.

SSA took possession of the DSC in January 2009. Although initially referred to as the Second Data Center, the DSC is actually a co-processing center as routine operations will be divided between it and the NCC. Data from each data center will be backed up to the other data center on a continual basis. In a recent Office of the Inspector General (OIG) report,[3] we evaluated SSA's current DR posture and how it is impacted by the new DSC. The report indicated that, while the DSC was not designed as a backup and recovery center, in the case of a disaster at the NCC, the DSC will have the capability to handle the Agency's information technology (IT) workloads associated with SSA's Mission Essential Functions (MEF)[4] and Primary Mission Essential Functions (PMEF).[5] Likewise, it is planned that the NCC will have the ability to handle the Agency's IT workloads associated with the MEFs and PMEFs in the event of a disaster at the DSC. During a disaster, the functioning data center will eventually assume non-critical workloads by expanding the existing infrastructure.

To perform our evaluation, we reviewed Federal directives, standards, and industry best practices. We also interviewed key SSA executives and personnel with oversight responsibility for the acquisition process and conducted physical walkthroughs of the DSC facility. We performed field work at the DSC and SSA Headquarters in Baltimore, Maryland, from January through May 2009. See Appendix B for more information on our scope and methodology.

RESULTS OF REVIEW

Based on our observations and analysis of the project-level plans, designs, and current status of the DSC, SSA, with the assistance of GSA and other construction experts, appears to have successfully designed a co-processing center that incorporates a

---

[3] SSA OIG, *Quick Response Evaluation: Social Security Administration's Disaster Recovery Process (*A-4-09-29139) Limited Distribution Report, June 2009.

[4] MEFs are the limited set of department and agency-level Government functions that must be continued after a disruption of normal activities.

[5] PMEFs are a subset of MEFs that directly support the eight functions the President and national leadership will focus on to lead and sustain the Nation during a catastrophic emergency.

number of Tier III[6] level features and complies with industry security standards.[7] Although the DSC was acquired to mitigate the DR risk of having only one data center, we believe SSA should have optimized the use of the DSC for mitigating this risk by more effectively planning for the processing needs of the Agency. We also identified project delays and cost increases for which the Agency had not adequately planned. Finally, we noted other minor observations related to information security that should be addressed.

Strategic Planning

Our review of the DSC project-level planning documents and discussions with SSA personnel indicated that although prior vendor and OIG reports questioned the ability of third parties to provide DR services, the DSC was not considered an alternative DR location earlier than 2010. In the event of an NCC outage before the DSC is fully operational in 2012, the back-up and recovery strategy would continue to rely on a vendor hot site;[8] but the demand on the hot site would be reduced since some of the processing would be done at the DSC.

Even though SSA took occupancy of the DSC in January 2009, the Agency's operations remain fundamentally reliant on a single, national computing facility—the NCC. The age and infrastructure of the NCC suggest that even if a disaster does not occur, the deficiencies of the facility place it at risk of an outage—thus highlighting the need for SSA to have a comprehensive plan of action to ensure its information systems remain operational and the Agency can continue to provide services to the public.

A prior OIG report[9] recommended a more integrated approach to SSA's IT strategic planning. As early as March 2001,[10] we raised concerns about SSA's strategic planning for IT. Effective strategic planning helps an agency set priorities and decide how best to

---

[6] Tier III facilities have redundant capacity that allows for any planned site infrastructure maintenance and activities without disrupting the computer hardware operation. All IT equipment is dual powered and has multiple independent distribution paths.

[7] The ISC, *ISC Security Design Criteria For New Federal Office Buildings and Major Modernization Projects*, September 29, 2004.

[8] A hot site is an alternate facility that is equipped with the computer, the telecommunications, information technology, environmental infrastructure, and personnel required to recover critical business functions or information systems in the event a disaster impacts the normal processing facility.

[9] SSA OIG, *Information Technology Capital Planning and Investment Control Process at the Social Security Administration* (A-14-99-12004), March 30, 2001.

[10] Develop and use a risk model in the strategic planning process for all proposed IT projects. Selection criteria should include weighing risk for cost, benefits, schedule, technical, etc.

coordinate activities to achieve its goals.[11] For example, a strategic plan identifies interdependencies among project activities and helps ensure these interdependencies are understood and managed. With strategic planning, projects—and thus system solutions—are effectively integrated agencywide.

Had the Agency taken a more integrated approach to its IT strategic planning, the DSC might have been given greater consideration as a part of the Agency's overall DR strategy. In our recent report on SSA's DR process,[12] we suggested the Agency accelerate its plans for using the DSC given the current state of the NCC and the processing capacity limitations at the vendor hot site. The DSC has sufficient space available for additional equipment and staff could be brought in to handle 100 percent of SSA's computing needs in the event the NCC becomes non-operational. Currently, the DSC may be able to function as an effective DR back-up site; however, the effectiveness and efficiency of the systems will not be fully tested until 2012.

SSA has begun to address the DR shortcomings by working to have the DSC operational sooner. With full use of the DSC in 2012, the Agency anticipates meeting its DR objectives of restoring critical functions within 24 hours of a disaster, losing less than 1 hour of data. Federal Continuity Directive (FCD) 1[13] mandates that all necessary and required communications and IT capabilities be operational as soon as possible following continuity activation and in all cases within 12 hours of the activation.

The Agency is taking a phased approach to achieve full functionality at the DSC. SSA stated that the mainframes at the DSC were configured in May 2009, and that between April and July 2009, the operating environments for two of its workloads—electronic folder and software engineering—were transferred to the DSC. Since problems have surfaced with the NCC, steps have been taken to ensure that the DSC will have the mainframe capacity to perform all critical NCC workloads by 2010, if needed. Although mainframe capacity will be available, additional equipment and data connections will still be necessary for full utilization, which is expected in Fiscal Year (FY) 2012. The recovery of the DSC's mainframes will be tested at the NCC in 2011, and the recovery of the NCC's mainframes could be tested at the DSC as early as 2012. In 2012, the Agency's goal is to have the DSC and NCC interface designed so that, in the event of a disaster, the critical workloads of one can be assumed by the other within 24 hours. Non-critical workloads will be deferred until the impacted center is restored to full operations or the capacity of the unaffected center is expanded.

---

[11] Government Accountability Office (GAO) GAO-09-662T, *Testimony Before the Subcommittee on Social Security, Committee on Ways and Means, House of Representatives: Social Security Administration, Effective Information Technology Management Essential For Data Center Initiative*, Highlights page, April 28, 2009.

[12] SSA OIG, *Quick Response Evaluation: Social Security Administration's Disaster Recovery Process (*A-14-09-29139) Limited Distribution Report, June 2009.

[13] FCD 1, *Federal Executive Branch National Continuity Program and Requirements*, Section 9.e., page 9, February 2008.

Until the DSC can be used for DR purposes, a system outage resulting from a disaster at the NCC would effectively shut down operations across the organization for approximately 10 days, and only 34 percent of SSA's systems processing capacity would be available after the systems are established at the DR vendor site. Furthermore, full restoration of systems capacity may be delayed for an additional 10 days because, upon returning to the NCC, the Agency would again be faced with limited service availability while SSA restores the systems and updates the files with all of the transactions processed at the vendor site.

We believe the Agency would be in a better DR posture had these issues been addressed in an integrated strategic planning process. Given the limitations of the current DR scenario, plans to replace the NCC, and status of the DSC, the Agency plans to have an overall data processing strategy that considers a new NCC, the DSC, and a new DR plan by 2011. We recommend that the Agency complete the development of a comprehensive DR plan that considers the NCC, the project to replace the NCC, and the viability of the DSC to maximize SSA's ability to continue operations. This DR plan should also take into account the short- and long-term interdependencies of all these projects to devise a strategy that best positions SSA to continue operation. While we recognize the Agency is making a concerted effort to ensure adequate preparation and testing before it relies on the DSC for its DR plan, we recommend that SSA develop integrated strategic plans to expedite the use of the DSC as the NCC's DR site.

During a recent review of Agency-level strategic IT planning, we noted that SSA's current IT strategic plans are short-term, tactical plans that do not provide a detailed description of how the Agency intends to address its long-term IT processing needs.[14] The review identified a need for SSA to focus its efforts on strengthening its IT strategic planning process and related documents.

The strategic plans should be comprehensive, transparent,[15] and integrated[16] with other components and include possible constraints and challenges on all aspects of the project. Specifically, as the Agency considers a new data center, the strategic plan should include both IT and facilities.

[14] SSA OIG, Congressional Response Report: *The Social Security Administration's Information Technology Strategic Planning* (A-44-09-29120), June 29, 2009.

[15] Transparency promotes accountability and provides information across the organizational components.

[16] Per Office Management and Budget (OMB) A-130, Section 8.a.1(e). Agencies should integrate planning for IT with plans for resource allocation and use, including budgeting and acquisition.

We also believe SSA should fully document the goals of such projects. When we reviewed the OMB Exhibit 300 submissions,[17] SSA's OMB Exhibit 53 submissions,[18] and the Information Technology Advisory Board (ITAB) documentation,[19] we found SSA did not document the goals and resources for the structural building of the DSC as part of its IT project plan. According to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, security controls are applicable to those sections of the facility that protect the information system including its IT assets such as server farms and data centers.[20] Since NIST has recognized a data center as an IT asset, SSA should also consider a data center as an IT asset to ensure it receives the appropriate attention.

In a 2007 OIG report,[21] we found SSA could have improved its IT plan by providing its stakeholders with a clear roadmap of how the Agency plans to reach its goals and objectives. Since the DSC is a key component of the backbone of SSA's automated operations, the Agency needs to implement an integrated strategic plan. In the context of its strategic vision, it is important that the Agency identify goals, resources, and interdependencies among the various components. Had the Agency included the facilities objectives in its ITOA project plan, it may have better achieved its goals. For example, facilities should have been included in the Agency's ITAB proposal for systems functionality, strategic objectives, risks, dependencies, budget, and resources.

Project Costs and Schedule Delays

To initiate the project, SSA submitted an original Reimbursable Work Authorization (RWA) in FY 2005 for $675,000 for an existing data center. After changes in construction options and building location, SSA ultimately submitted a total of $44.26 million in RWAs for the DSC. When the ITOA project was conceived, the Agency anticipated finding an existing data processing facility that could be quickly converted for SSA use. When the market survey and solicitation exercise produced only unused office space, in FY 2006, SSA submitted a subsequent RWA for $5.5 million for anticipated renovation costs. Because of potential toll road construction near the proposed renovation site, plans changed to building a new facility. This

---

[17] An OMB Exhibit 300 is the capital asset plans and business cases submitted to OMB by executive agencies for IT investments.

[18] An OMB Exhibit 53 is the Agency IT Investment Portfolio submitted to OMB by executive agencies for IT investments. It is used to create an overall Federal IT Investment Portfolio published as part of the President's Budget.

[19] The ITAB addresses Agency IT issues and investments and prioritizes Agency IT workload. The ITAB has a 2-year planning timeframe with annual and quarterly meetings. It is an ongoing process of evaluating current and new IT projects to ensure the projects fulfill SSA goals.

[20] NIST SP 800-53, *Recommended Security Controls for Federal Information Systems,* Revision 2, Section 3.3, page 18, December 2007.

[21] SSA OIG, *The Social Security Administration's Information Resources Management Strategic Plan* (A-14-07-27133), September 28, 2007.

adjustment required additional funds, and the Agency submitted a FY 2007 RWA to GSA for $8.5 million. In late FY 2007, based on actual construction pricing, SSA received the first estimate from GSA that required two subsequent modifications to the RWAs totaling $44.26 million in outlays.

In addition, the Agency encountered a number of delays during the acquisition and construction of the DSC. We determined that it took 6 years, starting in December 2002, for the Agency to plan, construct, and occupy the co-processing center. The Agency spent the first 26 months analyzing DR solutions, which did not take into account all factors and alternatives. The Agency spent the following 14 months selecting a site and the last 32 months obtaining permits and constructing a new data center.

In May 2006, the DSC lease was awarded with an anticipated completion date of August 2007. In June 2006, GSA and SSA learned that the State was revisiting a 1958 plan to build a toll road to reduce congestion, which would permit the State to purchase the site GSA had leased for SSA. To allow ITOA to move forward, SSA located an alternate site with occupancy no later than November 2007. In March 2007, DSC construction started with access to the DSC expected in May 2008. Additional delays in material delivery schedules caused GSA and the lessor to revise the scheduled occupancy date to January 16, 2009. Despite delays in construction, SSA was able to continue the planned IT activities not directly dependent on occupation of the DSC—the isolation and testing of the workloads scheduled to move to the DSC and the testing and pre-configuring of equipment at the NCC.

Better IT investment management and planning could have ensured that SSA proceeded in a more timely fashion toward agreed-upon budget and milestones. For IT investment management, an agency should follow a portfolio-based approach in which investments are selected, controlled, and monitored from an agency-wide perspective.[22] Investment management is aimed at goals to avoid unnecessary delays and cost overruns.[23] For example, accurate cost estimating provides a sound basis for establishing a baseline to formulate budgets and measure program performance.[24] Had SSA closely managed the establishment of a second data center as a single project including both IT and facilities, it may have avoided unnecessary delays and cost overruns, and could have projected a budget closer to the final cost.

Although the DSC is more than 300 miles from the NCC, being located on the east coast leaves the Agency susceptible to regional events. According to SSA, the Agency performed a comprehensive site selection security review to assist in identifying a potential location for the DSC. However, in accordance with *Federal Executive Branch National Continuity Program and Requirements*, Annex G, the Agency should have

[22] GAO-09-662T, supra at Highlights page.

[23] Id.

[24] Id.

conducted an all-hazards risk assessment before deciding on a location.[25] This assessment must include identification of all hazards that may affect the facility; a vulnerability assessment that determines the effects of all hazards on the facility; a cost-benefit analysis of implementing risk mitigation, prevention, or control measures; and a formal analysis by management of acceptable risk. The site location selection security review does not meet these FCD1 requirements.

A prior OIG report[26] found that SSA could encounter longer delays in recovering its systems should the Agency have to compete for hot site resources in the event of a regional or global disaster. These outages not only have a monetary impact, they also damage the public trust in the Agency. SSA should have performed an all-hazards risk assessment that included the site location to ensure the Agency is protected from regional disaster events.

"Reviewing an organization's risks and risk management programs must take into consideration additional factors such as the probabilities of events occurring, mission priorities, and impact assessments. Further, cost may also be a factor to consider, because informed decisions about acceptable and unacceptable levels of risk will ultimately drive the expenditure of resources (i.e., money, people, and time) to mitigate risk".[27] Because organizations cannot afford to counter every threat to their mission, successful continuity planning demands an intelligent analysis and prioritization of where and when to focus resources and to apply funding and other assets.

By requiring that an all-hazards risk assessment—based on location—be performed for any future buildings, SSA could ensure that its data centers are not susceptible to the same regional event and also encounter fewer construction delays. Furthermore, a cost-benefit analysis will enable the Agency to implement proper measures for preventing or mitigating the identified risks.

NCC Considerations

It should be noted that SSA's DSC construction was well underway before the 2008 Lockheed Martin report,[28] which detailed major concerns with the physical infrastructure of the NCC. Some of the concerns identified in the 2008 report had been identified as early as 1989.[29] As a part of this review, we determined whether the infrastructure concerns identified at the NCC were considered in the planning process. Although

---

[25] FCD 1, supra, Annex G, page G-3.

[26] SSA OIG, Quick Response Evaluation: *Social Security Administration's Disaster Recovery Process* (A-14-09-29139), June 2009.

[27] FCD 1, supra, Annex A, *page A-2.*

[28] Lockheed Martin, *Final Feasibility Study*, February 08, 2008.

[29] SSA OIG, Congressional Response Report: *The Social Security Administration's Information Technology Strategic Planning (*A-44-09-29120), June 2009.

these concerns were not specifically considered as part of the planning process, the DSC was designed and constructed in a manner that minimizes the likelihood that the physical concerns at the NCC will be repeated. For example, the Agency took steps to ensure that

- there are no structural problems;
- there is adequate electrical distribution and backup power supplies; and
- the raised floor for cooling meets Tier III standards.

The building was designed to meet the specific criteria set forth in the requirements provided to GSA. Furthermore, SSA built the co-processing center with consideration of the data center's possible future growth. According to the Telecommunications Industry Association, a data center should be designed with plenty of flexible "white space"—empty space that can accommodate future racks and cabinets.[30] SSA stated the DSC has "white space" that will accommodate additional mainframes, tape silos, and other IT equipment. It also has space and infrastructure to allow for additional cooling equipment, uninterruptible power supply, and generator power.

During a recent audit, the Agency advised us that the new data center had to be located within 40 miles of the existing data center to facilitate the transfer of the tightly integrated workloads. Because of the interdependence of the workloads involved, SSA's initial data transfer from the NCC to the new data center is unique. The Agency plans to use special software to mitigate the risks of the transfer of these tightly integrated workloads and interdependent systems.

Currently, in the event of a disaster at the NCC, SSA would use back-up tapes stored at an off-site storage facility to restore the NCC workloads at the DSC. As of 2010, the Agency plans to recover the NCC data at the DSC and test its ability to restore and recover NCC workloads comparable to the current vendor facility recovery methodology and timeframes. The Agency's goals under the ITOA project are to have the systems operating within 24 hours of a disaster with a loss of only 1 hour. In 2012, SSA expects recovery of NCC critical workloads at the DSC within 24 hours with a 1-hour acceptable loss of data.

Physical Security Plans

According to NIST SP 800-34,[31] every building should have emergency instructions and Occupant Emergency Plans (OEP) manuals. Furthermore, SSA's Administrative

---

[30] Telecommunications Industry Association (TIA), *TIA-942 Data Center Standards Overview*, April 2005.

[31] NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, Section 2.2, *Types of Plans*, pages 7-11, June 2002.

Instruction Manual System (AIMS) requires that field locations[32] develop and approve a Physical Security Action Plan (PSAP) and OEP within 45 days of occupancy for all new offices and relocations.[33] The Agency has identified the DSC as a Headquarters facility since it, along with the NCC, form a dual data processing center scenario—the management and staff are split between the two locations. At the time of the our site visit in February 2009, the Agency had not completed the emergency documentation for the DSC citing that the facility had no production environment and was not considered complete. In June 2009, a physical security review was performed. The DSC continues to pursue the development of the OEP.

In January 2009, the Agency took occupancy, and in May 2009, production systems began operating out of the DSC. While the Agency does not have a policy covering PSAP or OEP development for Headquarters facilities and considering the critical nature of the DSC, the Agency should have completed an OEP and PSAP in a manner at least consistent with the AIMS policy for field administration.

The lack of an OEP and PSAP impairs the Agency's ability to prevent injury, save lives, and protect Federal assets. SSA employees, visitors, facilities, records, and equipment may not be adequately protected. Prompt coordinated steps may not be taken to obtain assistance when needed, as employees may not be aware of proper protective and emergency procedures. Therefore, we recommend that SSA develop a policy to ensure emergency instructions and plans, such as the PSAP and OEP, are completed for Headquarters facilities within at least the same time frame as required by the AIMS field administration policy. SSA should also complete the OEP and the PSAP for the DSC.

Information Security

We identified minor information security concerns that SSA should address and ensure are considered as an integral part of future planning, design, and construction of new buildings and major modernization projects.[34]

Physical security is defined as the protection of building sites and equipment (and all information and software contained therein) from theft, vandalism, natural disaster, manmade catastrophes, and accidental damage. It requires solid building construction, suitable emergency preparedness, reliable power supplies, adequate climate control,

---

[32] SSA AIMS 12.06.02 indicates that the requirement for establishing and maintaining a PSAP and OEP applies to regional offices; program service centers; data operations centers; teleservice centers; field offices; the Office of Disability Adjudication and Review in Falls Church, Virginia, and its hearings offices; and the Office of Quality Performance regional and satellite offices.

[33] SSA, AIMS, General Administration Manual, Chapter 12, Field Administration, Section 12.06.03.

[34] ISC, *ISC Security Design Criteria for New Federal Office Buildings and Major Modernization Projects*, page 2, September 29, 2004.

and appropriate protection from intruders.[35] Agency facilities shall meet the minimum requirements listed in the ISC Security Standards for new Federal office buildings.[36] During our visit to the DSC, we found vulnerabilities based on ISC standards and SSA's policy. We recommend that SSA management assess and appropriately address the security weaknesses identified in this review to ensure Agency compliance with applicable ISC standards[37] and SSA policy.[38]

(We have separately provided management with details on each of the specific security weaknesses noted in our review, including individual recommendations for addressing them.)

CONCLUSION AND RECOMMENDATIONS

Despite the challenges to the project, SSA appears to have successfully designed a co-processing center that incorporates a number of Tier III level features and meets industry security standards. The Agency not only considered future processing needs of the center, such as "white space," it designed and constructed the DSC in a manner that minimizes the likelihood that the physical concerns at the NCC will be repeated. While SSA performed some IT planning, the Agency could have benefited had more integrated strategic planning been performed. Given the significance of the Agency's current efforts to build a new NCC, we believe SSA should learn from its experience with the DSC and take the necessary steps to ensure proper planning to mitigate project delays and cost increases. Specifically, SSA should:

1. Accelerate the use of the DSC as a fully functioning data center—with particular emphasis on using the DSC as the DR site for the NCC.

2. Develop a comprehensive, long-range IT strategic plan that (i) is transparent and integrated within other SSA components, (ii) includes possible constraints and challenges on all aspects of IT projects, and (iii) conforms to the Agency's strategic plan. This applies to the Agency-level and project-level strategic plans.

3. Formally document the Agency's plan to accelerate the use of the DSC as part of SSA's overall DR plan and continually update the DR plan as the DSC and NCC replacement become fully functional. The updated DR plan should consider the viability of the DSC to maximize SSA's ability to continue operations in the current NCC, as well as during the transition to its replacement.

---

[35] SysAdmin, Audit, Network, Security Institute, *Data Center Physical Security Checklist*, page 2, December 1, 2001.

[36] ISC, *ISC Security Design Criteria For New Federal Office Buildings and Major Modernization Projects*, page 3, September 29, 2004.

[37] ISC, *ISC Security Design Criteria For New Federal Office Buildings and Major Modernization Projects*, September 29, 2004.

[38] SSA, AIMS, General Administration Manual, Chapter 12, Field Administration.

4. Develop a policy to ensure that emergency instructions and plans, such as the PSAP and OEP, are completed for Headquarters facilities within at least the same time frame as required by the AIMS Field Administration policy and complete the OEP and PSAP for the DSC.

For future IT investments, SSA should better manage control of the projects. Specifically, SSA should:

5. Monitor actual performance compared to expected results to ensure projects meet agreed-upon budget and milestones.

6. Ensure a risk assessment is undertaken to identify environmental risks associated with the site location of new structures (that is, flood plain, hurricane, tornado).

With the particular security weaknesses identified in this review, we recommend SSA:

7. Assess and appropriately address the security weaknesses identified in this review to ensure Agency compliance with applicable ISC standards and SSA policy.

AGENCY COMMENTS

SSA agreed with our recommendations (see Appendix C).

Patrick P. O'Carroll, Jr.

Appendices

Acronyms

ADRE	Accelerated Disaster Recovery Environment
AIMS	Administrative Instructions Manual System
CCTV	Closed Circuit Television
CIO	Chief Information Officer
DR	Disaster Recovery
DSC	Durham Support Center
FCD	Federal Continuity Directive
FY	Fiscal Year
GSA	General Services Administration
ISC	Interagency Security Committee
IT	Information Technology
ITAB	Information Technology Advisory Board
ITOA	Information Technology Operations Assurance
MEF	Mission Essential Function
NCC	National Computer Center
NIST	National Institute of Standards and Technology
OEP	Occupant Emergency Plan
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PMEF	Primary Mission Essential Function
PSAP	Physical Security Action Plan
RWA	Reimbursable Work Authorization
SP	Special Publication
SSA	Social Security Administration

Scope and Methodology

Our objective was to review the plan, design, status, and data processing capacity of the Social Security Administration's (SSA) Durham Support Center (DSC). This is one in a series of reviews that will address the Agency's future processing needs. This evaluation will focus on the strategic planning involved in the acquisition of the DSC. To meet our objective, we examined Federal directives, standards, and best practices. Specifically, we examined:

- Federal Continuity Directive 1, *Federal Executive Branch National Continuity Program and Requirements*, February 2008.
- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources.*
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems,* December 2007.
- NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, Section 2.2, *Types of Plans*, pages 7-11, June 2002.
- NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, July 2008.
- Interagency Security Committee (ISC), *ISC Security Design Criteria for New Federal Office Buildings and Major Modernization Projects*, September 29, 2004.
- Government Accountability Office (GAO) GAO-09-662T, *Testimony Before the Subcommittee on Social Security, Committee on Ways and Means, House of Representatives: Social Security Administration, Effective Information Technology Management Essential For Data Center Initiative*, April 28, 2009.
- SysAdmin, Audit, Network, Security Institute, *Data Center Physical Security Checklist*, December 1, 2001.
- Telecommunications Industry Association, *TIA-942 Data Center Standards Overview*, April 2005.
- Uptime Institute, *Tier Classifications Define Site Infrastructure Performance,* 2008.

We also reviewed the following:

- SSA's Administrative Instructions Manual System Chapter 12, Field Administration.
- SSA documents such as Commissioner presentations, project schedules, Reimbursable Work Authorizations, the Solicitation for Offers, requirements for the DSC, OMB Exhibit 300 submissions, and OMB Exhibit 53 budget submissions.
- Lockheed Martin's *Disaster Recovery Vendor Viability Report,* December 27, 2002.
- Lockheed Martin's *Final Feasibility Study*, February 08, 2008.

We interviewed representatives from the following SSA components.

- The Office of the Chief Information Officer is responsible for capital planning and investment control, security policy, enterprise architecture, E-Government, and the Information Resources Management Strategic Plan.
- The Office of Budget, Finance and Management provides (i) a comprehensive financial program of budget policy, formulation, and execution; (ii) accounting policy and operations; (iii) the Agency's acquisition and grants program, internal control program, and audit resolution and liaison; (iv) Agency-wide facilities, publications, and logistics management programs; (v) the Agency strategic planning, data matching, and information exchange; and (vi) the information systems security programs.
- The Office of Systems (i) directs the conduct of systems and operational integration and strategic planning processes, (ii) directs the implementation of a comprehensive systems configuration management, database management, and data administration program; (iii) initiates software and hardware acquisition for SSA and oversees software and hardware acquisition procedures, policies, and activities; (iv) directs the development of operational and program specifications for new and modified systems; and (v) oversees development, validation and implementation phases. Specifically, we interviewed staff from the Office of Enterprise Support, Architecture and Engineering; Office of Systems Electronic Services; Office of Telecommunications and Systems Operations; the Information Technology Operations Assurance project officer; and DSC staff.

We performed our field work at SSA Headquarters and the DSC from January through May 2009. We determined the criteria used in this review were sufficiently reliable to meet our objectives. We conducted our review in accordance with the President's Council on Integrity and Efficiency's *Quality Standards for Inspections*.[1]

[1] In January 2009, the President's Council on Integrity and Efficiency was superseded by the Council of the Inspectors General on Integrity and Efficiency, *Inspector General Reform Act of 2008,* Pub. L. No. 110-409 § 7, 5 U.S.C. App. 3 § 11.

Agency Comments

SOCIAL SECURITY

MEMORANDUM

Date: September 28, 2009 Refer To: S1J-3

To: Patrick P. O'Carroll, Jr.
Inspector General

From: Margaret J. Tittel /s/
Acting Chief of Staff

Subject: Office of the Inspector General (OIG) Draft Report, "Processing Capacity of the Social Security Administration's Durham Support Center" (A-14-09-19100)--INFORMATION

Thank you for the opportunity to review and comment on the draft report. We appreciate OIG's efforts in conducting this review. Attached is our response to the report recommendations.

Please let me know if we can be of further assistance. Please direct staff inquiries to Candace Skurnik, Director, Audit Management and Liaison Staff, at (410) 965-4636.

Attachment

COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL (OIG) DRAFT REPORT, "PROCESSING CAPACITY OF THE SOCIAL SECURITY ADMINISTRATION'S DURHAM SUPPORT CENTER" (A-14-09-19100)

Recommendation 1

Accelerate the use of the Durham Support Center (DSC) as a fully functioning data center--with particular emphasis on using the DSC as the disaster recovery (DR) site for the National Computer Center (NCC).

Comment

We agree. The Accelerated Disaster Recovery Environment (ADRE) project is currently underway. We allocated funds, awarded mainframe capacity acquisitions, and we project the installation of all equipment before the end of calendar year 2009. During fiscal year 2010, we expect to conduct a recovery test of the NCC workloads in the DSC. In addition, we will be conducting an exercise using real data from our live production systems.

Recommendation 2

Develop a comprehensive, long-range information technology (IT) strategic plan that (i) is transparent and integrated within other SSA components, (ii) includes possible constraints and challenges on all aspects of IT projects, and (iii) conforms to our strategic plan. This applies to agency-level and project-level strategic plans.

Comment

We agree. We will develop a comprehensive, long-range IT strategic plan that is transparent and integrated. The plan will include possible constraints and challenges on all aspects of IT projects and will conform to our strategic plan.

Recommendation 3

Formally document the agency's plan to accelerate the use of the DSC as a part of SSA's overall DR plan and continually update the DR plan as the DSC and NCC replacement become fully functional. The updated DR plan should consider the viability of the DSC to maximize SSA's ability to continue operations in the current as well as during the transition to the replacement NCC.

Comment

We agree. As stated in our response to recommendation 1, we have initiated the ADRE project with an emphasis on recovering NCC workloads in the DSC. ADRE will deliver a SunGard-like disaster recovery capability in the DSC. In 2009, our SunGard testing restored the targeted NCC environments in approximately 148 hours. Once we have demonstrated a process for recovering NCC workloads in the DSC, we will update our DR documentation accordingly. Further, as the

Information Technology Operations Assurance project progresses we will perform recovery tests in the NCC and update the documentation.

Recommendation 4

Develop a policy to ensure that emergency instructions and plans, such as the Physical Security Action Plan (PSAP) and Occupant Emergency Plan (OEP), are completed for headquarters facilities within at least the same time frame as required by the Administrative Instructions Manual System (AIMS) Field Administration policy and complete the OEP and PSAP for the DSC.

Comment

We agree. We will incorporate a change to the AIMS General Administration Manual that will require completion of a PSAP for each headquarters facility. In addition, we are developing an OEP for the DSC. We will also complete a PSAP for the DSC.

Recommendation 5

For future IT investments, monitor actual performance compared to expected results to ensure projects meet agreed-upon budget and milestones.

Comment

We agree. For future IT investments, we will monitor actual performance compared to expected results to ensure we meet agreed-upon budget and milestones.

Recommendation 6

For future IT investments, ensure a risk assessment is undertaken to identify environmental risks associated with the site location of new structures (that is, flood plain, hurricane, and tornado).

Comment

We agree. For future IT investments, we will conduct a risk assessment to identify environmental risks associated with the site location of new structures. In July 2009, we conducted an all-hazards risk assessment at the DSC.

Recommendation 7

Assess and appropriately address the security weaknesses identified in this review to ensure agency compliance with applicable Interagency Security Committee standards and our policy.

Comment

We agree. We have assessed all security weaknesses identified in this review and taken corrective action.

OIG Contacts and Staff Acknowledgments

OIG Contacts

Brian Karpe, Acting Director, Information Technology Audit Division

Mary Ellen Moyer, Audit Manager

Acknowledgments

In addition to those named above:

Jan Kowalewski, Senior Program Analyst

For additional copies of this report, please visit our web site at www.socialsecurity.gov/oig or contact the Office of the Inspector General's Public Affairs Staff Assistant at (410) 965-4518. Refer to Common Identification Number A-14-09-19100.

DISTRIBUTION SCHEDULE

Commissioner of Social Security

Office of Management and Budget, Income Maintenance Branch

Chairman and Ranking Member, Committee on Ways and Means

Chief of Staff, Committee on Ways and Means

Chairman and Ranking Minority Member, Subcommittee on Social Security

Majority and Minority Staff Director, Subcommittee on Social Security

Chairman and Ranking Minority Member, Committee on the Budget, House of Representatives

Chairman and Ranking Minority Member, Committee on Oversight and Government Reform

Chairman and Ranking Minority Member, Committee on Appropriations, House of Representatives

Chairman and Ranking Minority, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, House of Representatives

Chairman and Ranking Minority Member, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Committee on Finance

Chairman and Ranking Minority Member, Subcommittee on Social Security Pensions and Family Policy

Chairman and Ranking Minority Member, Senate Special Committee on Aging

Social Security Advisory Board

Overview of the Office of the Inspector General

The Office of the Inspector General (OIG) is comprised of an Office of Audit (OA), Office of Investigations (OI), Office of the Counsel to the Inspector General (OCIG), Office of External Relations (OER), and Office of Technology and Resource Management (OTRM). To ensure compliance with policies and procedures, internal controls, and professional standards, the OIG also has a comprehensive Professional Responsibility and Quality Assurance program.

Office of Audit

OA conducts financial and performance audits of the Social Security Administration's (SSA) programs and operations and makes recommendations to ensure program objectives are achieved effectively and efficiently. Financial audits assess whether SSA's financial statements fairly present SSA's financial position, results of operations, and cash flow. Performance audits review the economy, efficiency, and effectiveness of SSA's programs and operations. OA also conducts short-term management reviews and program evaluations on issues of concern to SSA, Congress, and the general public.

Office of Investigations

OI conducts investigations related to fraud, waste, abuse, and mismanagement in SSA programs and operations. This includes wrongdoing by applicants, beneficiaries, contractors, third parties, or SSA employees performing their official duties. This office serves as liaison to the Department of Justice on all matters relating to the investigation of SSA programs and personnel. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

Office of the Counsel to the Inspector General

OCIG provides independent legal advice and counsel to the IG on various matters, including statutes, regulations, legislation, and policy directives. OCIG also advises the IG on investigative procedures and techniques, as well as on legal implications and conclusions to be drawn from audit and investigative material. Also, OCIG administers the Civil Monetary Penalty program.

Office of External Relations

OER manages OIG's external and public affairs programs, and serves as the principal advisor on news releases and in providing information to the various news reporting services. OER develops OIG's media and public information policies, directs OIG's external and public affairs programs, and serves as the primary contact for those seeking information about OIG. OER prepares OIG publications, speeches, and presentations to internal and external organizations, and responds to Congressional correspondence.

Office of Technology and Resource Management

OTRM supports OIG by providing information management and systems security. OTRM also coordinates OIG's budget, procurement, telecommunications, facilities, and human resources. In addition, OTRM is the focal point for OIG's strategic planning function, and the development and monitoring of performance measures. In addition, OTRM receives and assigns for action allegations of criminal and administrative violations of Social Security laws, identifies fugitives receiving benefit payments from SSA, and provides technological assistance to investigations.