SOCIAL SECURITY

Office of the Inspector General

December 7, 2001

The Honorable Jo Anne B. Barnhart
Commissioner

Dear Ms. Barnhart:

In November 2000, the President signed the *Reports Consolidation Act of 2000*, which requires Inspectors General to provide a summary and assessment of the most serious management and performance challenges facing the agencies and the agencies' progress in addressing them. This document responds to the requirement to include this statement in the Fiscal Year (FY) 2001 *Social Security Performance and Accountability Report*.

In January 2001, we identified the following 10 significant management issues facing the Social Security Administration (SSA) for FY 2001.

Critical Information Infrastructure

Earnings Suspense File

Fraud Risk

Identity Theft

Service to the Public

Disability Redesign

Enumeration

Government Performance and Results Act

Representative Payees

Systems Security and Controls

In FY 2001, SSA took action to address these issues, many of which are of a long-term nature and do not lend themselves to quick fixes. Our assessment of the status of these 10 management challenges is enclosed.

Sincerely,

James G. Huse, Jr.
Inspector General of Social Security

Enclosure

Inspector General Statement on the Social Security Administration's Major Management Challenges

DECEMBER 2001

Critical Information Infrastructure

As technology advances and our reliance on technology increases, the need for a strong information infrastructure becomes more important. Protection of critical information and its infrastructure is an issue that is significant not just to the Agency, but to the entire Government. For example, Presidential Decision Directive (PDD) 63, issued in 1998, requires Federal agencies to identify and protect their critical infrastructure and assets. One of the Social Security Administration's (SSA) most valuable assets is the information it collects and uses to complete its mission. SSA is depending on technology to meet the challenges of ever-increasing workloads with fewer resources. A physically and technologically secure Agency information infrastructure is a fundamental requirement.

SSA Has Taken Steps to Address this Challenge

SSA addresses critical information infrastructure and systems security in a variety of ways. It has established workgroups to conduct ongoing system reviews, including a Critical Infrastructure Protection workgroup that works toward compliance with PDD 63. The workgroup has created several components throughout SSA to handle systems security.

Government Information Security Reform Act: The Government Information Security Reform Act requires each agency to develop and implement an agency-wide information security plan for its assets and operations, and requires the agency's Office of Inspector General (OIG) to determine the efficiency and effectiveness of the overall security program and practices. SSA has initiatives underway in support of key Governmentwide initiatives focused on information assurance and data protection. For this mandate, SSA completed an assessment of its security program using a self-assessment tool provided by the National Institute of Standards and Technology.

PDDs 63 and 67: PDDs 63 and 67 address the new physical and cyber threats to our national infrastructure. PDD 63 calls for a national level effort to assure the security of increasingly vulnerable and interconnected infrastructures of the United States, and provides for a protection plan for national assets from both physical and cyber attack. SSA has identified its most critical assets and their relationship to other critical functions of Government and private industry. It has begun vulnerability analyses of these most critical assets.

PDD 67 directs all executive agencies to have a viable continuity of operations plan to enable the agency to continue essential functions during an emergency. SSA revised PDD-67 plan to reflect current Agency priorities, and further actions are planned to permit automated updating and access of information.

Additionally, SSA is planning to increase its information infrastructure to better meet the American public's expectations and needs. SSA is building an Internet infrastructure to allow its users and business partners to enter information about life events directly into its programmatic systems, rather than calling or visiting a teleservice center or field office (FO) and having SSA employees enter the data. SSA expects to make the conversion to this new architecture within the next 2 years.

SSA Needs to Continue to Address this Challenge

SSA has taken steps to strengthen its critical information infrastructure, however, further action is needed to protect the systems and information SSA is charged with managing and protecting.

Exposures exist primarily because SSA has not completed implementation of its enterprise-wide security program. Until a complete security framework is implemented and maintained, SSA's ability to mitigate effectively the risk of unauthorized access to, and/or modification or disclosure of, sensitive SSA information will be impaired. Unauthorized access to sensitive data can result in the loss of data, loss of trust fund assets, and/or compromised privacy of information associated with SSA's enumeration, earnings, and benefit payment processes and programs. The need for a strong security framework to address threats to the security and integrity of SSA operations will continue to grow as SSA implements Internet and Web-based applications.

We have recommended SSA continue its efforts to fully implement the information security framework by:

- Assigning specific resources to complete the full information security framework, with priority given to implementation, enforcement, and monitoring of technical security standards;
- Fully implementing technical security configuration standards;
- Establishing a process to determine that configuration standards remain consistently enforced;
- Establishing and enforcing effective procedures for monitoring security violations, periodic review of access assignments, and firewall log reviews; and
- Consistently enforcing policies and procedures for physical access to information resources based on the concept of access required to perform assigned job responsibilities.

The continuing expansion of SSA's information infrastructure is an essential part of SSA's plans to meet its future workloads. However, expansion of the critical information infrastructure must be implemented in a balanced manner. SSA must continue to ensure that its critical information infrastructure is secure as it expands to better meet the demands of the American public and an ever-increasing workload.

Disability Redesign

SSA's initiatives to redesign its disability determination process have not resulted in significant improvements. SSA administers two programs providing benefits based on disability: Disability Insurance (DI) and Supplemental Security Income (SSI). Most disability claims are initially processed through Social Security FOs and State Disability Determination Services (DDS). SSA's FO staff are responsible for obtaining applications for disability benefits and verifying non-medical eligibility requirements, which may include age, employment, or marital status information. The FO sends the case to a DDS for a disability evaluation. DDSs are State agencies fully funded by SSA responsible for developing medical evidence and rendering the initial determination on whether the claimant is legally disabled or blind. In Fiscal Year (FY) 2001, some 2,166,623 initial disability claims were processed, and the average processing time was 106 days.[1]

If a claimant is not satisfied with a DDS decision, the individual may file an appeal. The Office of Hearings and Appeals (OHA) is responsible for holding hearings and issuing decisions at two distinct stages in SSA's appeals process—in hearing offices and at the Appeals Council. Administrative Law Judges (ALJ) hold hearings and issue decisions in hearing offices nationwide. In FY 2001, hearing offices disposed of 465,228 cases, and the average time a claimant waited for a decision on an appeal was 308 days.[2] The Appeals Council is the final level of administrative review for claims filed under SSA's disability programs. The Appeals Council reviews ALJ decisions and dismissals upon the claimant's request for review. In FY 2001, the Appeals Council disposed of 115,589 cases.

SSA Has Taken Steps to Address this Challenge

SSA has tested several improvements to the disability claims process as a result of concerns about the timeliness and quality of its service. SSA's Disability Redesign plan combines initiatives that have been tested and piloted over the last few years and includes all levels of eligibility determinations beginning with State DDSs and continuing through the hearings and appeals processes.

The Disability Redesign plan was originally issued in September 1994, but SSA has revised its plans several times to accommodate changes in the improvement initiatives. SSA's updated plan entitled, *Social Security and Supplemental Security Income Disability Programs: Managing for Today Planning for Tomorrow*, was issued on March 12, 1999. The updated plan had four broad goals: Improve the Disability Adjudication Process; Enhance Beneficiaries' Opportunities to Work; Safeguard the Integrity of Disability Programs; and Improve the Knowledge Base for the Next Century.

[1] In FY 2000, the average processing time was 102 days.

[2] In FY 2000, a claimant waited 297 days for a decision on an appeal.

To date, SSA’s initiatives have not resulted in significant improvements to the disability determination process.

- As of May 2, 2001, decisions about the expansion of a prototype initiative at additional DDSs were delayed. Preliminary data from the prototypes raised questions about the program costs of national implementation.
- On October 22, 2001, the Disability Claim Manager (DCM) initiative was cancelled. The DCM test results showed that case-processing costs increased and more resources would be needed to support a blended Federal/State process.
- A plan for a new quality assurance (QA) system has not been developed. In reviewing SSA's QA system, a contractor informed SSA that modifying the system would not move SSA toward its quality improvement goals. Instead, SSA should adopt an advanced quality management system. In July 2001, the Acting Commissioner appointed a senior-level steering committee to develop recommendations for a new quality process. The results of the committee's work have not been released.
- The Hearings Process Improvement (HPI) initiative has not resulted in the planned improvements in OHA productivity and processing times.

SSA Needs to Continue to Address this Challenge

SSA needs to continue to improve the disability process. While it created a framework to address weaknesses in the disability process, it continues to fall short of most of its established disability-related performance goals. SSA did not meet 10 of 14 disability-related performance goals contained in SSA’s FY 2001 performance report. Particularly troublesome is the hearings and appeals process. SSA did not meet any of its goals related to the hearings and appeals process, and often failed to get within 5 percent of its goals in this area. The disability process continues to be a serious concern given the level of resources SSA has devoted to its disability process improvement initiatives and the lack of substantial improvement to date.

During FY 2001, we obtained and evaluated employee assessments of the results of OHA’s implementation of Phase 1 of the HPI plan. Our evaluation identified areas that SSA needed to improve during full implementation of the HPI plan. These areas included staffing, training, and ALJ instructions. Improvements were also needed in the staff's perception of quality of service, processing efficiency, and job satisfaction. Additionally, we found that the current medical evidence collection process accounts for a considerable portion of overall disability claims processing times. We calculated the time it took 8 DDSs to receive 663,293 medical evidence of record folders (MER) from claimant treating sources during FY 1998. For 35 percent of the MERs, the DDSs waited more than 30 days to receive them. Delays in receiving MERs from treating sources resulted in SSA paying over $1 million for MERs that were not received by these DDSs until after the disability decision was made. We made recommendations for SSA to improve DDS medical collection processes.

Earnings Suspense File

SSA's Earnings Suspense File (ESF) represents a major management challenge because its size and rate of growth may impact the calculations of beneficiaries' benefits, adds administrative costs, and represents a sizeable portion of nationwide Social Security number (SSN) misuse.

The ESF primarily consists of reported earnings that are put into suspense because the name/SSN combination does not match validation criteria within SSA's systems. Although SSA has reported it correctly posts over 99 percent of all wages received, those wages that cannot be posted to earners' accounts continue to accumulate in the ESF. Between Tax Years 1937 and 1999, the ESF grew to about $333 billion in wages representing approximately 227 million wage items. Each year, SSA receives about 21 million wage items that have an invalid name and SSN combination, and, through extensive computer matches and manual efforts, this number is reduced to about 6.5 million items, annually. However, further efforts to resolve invalid wage items can take years.

The integrity of SSA's process for posting workers' earnings is critical to ensuring eligible individuals receive the full retirement, survivor, and/or disability benefits due them. If earnings information is reported incorrectly, or not reported at all, SSA cannot ensure that all eligible individuals are receiving the correct payment amounts.

Finally, the ESF is indicative of a nationwide problem of potential fraud and misuse that not only affects SSA programs but crosses over to other Federal entities such as the Internal Revenue Service (IRS) and the Immigration and Naturalization Service (INS). The IRS uses Wage W-2s to enforce tax laws and can penalize employers and employees for providing incorrect information. The INS has oversight responsibility for unauthorized noncitizens. The Immigration Reform and Control Act of 1986 made it illegal for employers to knowingly hire or continue to employ unauthorized noncitizens. Employers must request newly hired employees to present documents that establish their identity and eligibility to work.

SSA Has Taken Steps to Address this Challenge

SSA developed Key Initiatives within its annual performance plan containing an overall strategy and several individual projects designed to reduce the ESF's size and rate of growth. For example, SSA plans to expand the use of the voluntary Employee Verification Service (EVS) to assist employers in verifying new hire names/SSNs. Under the Key Initiatives, SSA is also evaluating the results of two pilot projects that used the data bases of other Federal agencies to assist employers in verifying employees' names/SSNs. However, the success of many of these projects and pilots depends on the collaboration with and support from other agencies, such as the IRS, the INS, and the Office of Child Support Enforcement (OCSE).

SSA also hired a national accounting firm to review the ESF and provide recommendations and alternatives for management of this file. The contractor provided the final report to SSA in July 2001. The Agency is currently considering the recommendations made in the report.

SSA has developed other processes to validate the earnings data in the Master Earnings File (MEF). In recent years, SSA started mailing Social Security statements to individuals who had earnings and were age 25 or older. In FY 2001, SSA mailed 137 million of these statements. However, over 7 million were returned to SSA as undeliverable. If an individual contacts SSA about missing earnings, these amounts are either reinstated from the ESF to the MEF, if they are currently in suspense, or added as new earnings to the MEF.

SSA Needs to Continue to Address this Challenge

We commend SSA for its ESF Key Initiatives, but the changes called for in the Initiative are long-term, and several factors, both internal and external to SSA, hinder the efforts with the most potential to reduce the ESF's size and growth. Some of the internal factors include a higher priority placed on other automated system developments and the fact that SSA has not linked available information in its data base to identify chronic "problem" employers who continually submit annual wage reports with multiple errors. External factors include other Federal agencies with separate yet related mandates, such as the IRS' failure to sanction employers for submitting invalid wage data and the INS' complicated employer procedures for verification of eligible employees.

Recent OIG reviews have found SSA needs to improve communications with employers and enforce existing regulations if it expects to improve the accuracy of reported wages. For example, in a recent review, we found a chronic problem employer was not familiar with SSA's verification programs that could have prevented as much as 76 percent of the employer's wages from entering the ESF. In another audit, we found that SSA did not maintain sufficient controls over the wage reporting process to ensure employers were submitting quality earnings data. The audit noted that 285 employers submitted wage reports that failed SSA's wage reporting accuracy threshold 3 years in a row without SSA taking any action, even though more than $8.5 million in IRS penalties could have been assessed.

Enumeration

Enumeration, the process of assigning SSNs to U.S. workers and Social Security beneficiaries, is a major management challenge since it is one of the key elements SSA employs to effectively administer the Nation's Social Security system. The enumeration process also includes issuing replacement cards to people with existing SSNs and verifying SSNs for employers and other Federal agencies. In FY 2001, SSA issued over 18 million original and replacement SSN cards.

The magnitude of SSA's enumeration area and the importance placed on SSNs provides a tempting motive for unscrupulous individuals to fraudulently acquire an SSN and use it for illegal purposes. To effectively combat these criminals and reduce the occurrences of fraudulent SSN attainment, SSA must employ effective front-end controls in its enumeration process.

SSA Has Taken Steps to Address this Challenge

Some of the Agency's current and planned initiatives include the following:

- SSA, INS and the Department of State are working on agreements that will enable INS and the Department of State to collect enumeration data from aliens entering the United States.
- SSA implemented an enhancement to the Comprehensive Integrity Review Program (CIRP). CIRP is a business function used to deter and/or identify fraud by selecting fraud prone transactions for review on a regular basis. The enhancement to CIRP entailed automating a process to identify instances in which five or more SSN cards are sent to the same address within a 5-week period.
- SSA is working with States through the National Association of Public Health Statistics and Information Systems to allow FOs on-line access to State vital records data. Once implemented, FOs will be able to verify all U.S. birth certificates presented in support of SSN applications.
- SSA established a workgroup to identify enhancements that could be made in the Modernized Enumeration System to address certain fraud-prone situations.

SSA Needs to Continue to Address this Challenge

The September 11th terrorist attacks have only highlighted the importance of having a secure and efficient enumeration process. Before the attacks, we made several recommendations to address a variety of enumeration weaknesses. We believe these recommendations are still relevant today and will help to make the enumeration process more secure. Specifically, we recommended SSA:

- Obtain independent verification from the issuing agency (for example, INS and State Department) for all evidentiary documents submitted by noncitizens before issuing an original SSN;

- Establish a reasonable threshold for the number of replacement SSN cards an individual may obtain during a year and over a lifetime;
- Educate SSA staff about counterfeit documents; and
- Continue public policy discussions through interaction with the Departments of Justice and Treasury as well as the Federal Trade Commission.

Additionally, as we reported to Congress, we believe Congress and SSA should consider the following steps:

- Increase the number of investigative and enforcement resources provided for SSN misuse cases;
- Expand the Agency's data matching activities with other Federal, State, and local Government entities; and
- Explore the use of other innovative technologies such as biometrics in the enumeration process.

Since the events of September 11th, SSA created the Enumeration Response Team to develop proposals to strengthen the enumeration process. The OIG is a partner on the Response Team. As a result of the team's work, the Acting Commissioner approved the following seven recommendations:

- Provide refresher training on enumeration policy and procedures, with emphasis on enumerating noncitizens, for all involved staff;
- Convene a joint task force between SSA, INS, the Department of State and the Office of Refugee Resettlement to work out procedures for verifying noncitizen documentation;
- Eliminate driver's licenses as a reason for a nonwork SSNs to be implemented through the Program Operations Manual System (POMS);
- Provide an alternative to giving out Numident printouts for SSN verification. The Numident contains much of the information needed to establish credit or to get other "breeder" documents to perpetrate identity theft;
- Conduct a mandatory interview for applicants over the age of 12 applying for an original card and require evidence of identity for all children, regardless of age;
- Expedite implementation of a pilot to photocopy or scan all documentary evidence submitted with the Form SS-5 applications; and
- Change the Modernized Enumeration System to provide an electronic audit trail, regardless of the mode used to process the Forms SS-5.

Implementation of these recommendations and continued vigilance in this area is absolutely necessary to ensure the integrity of the enumeration process. We understand the Agency has a difficult task in balancing service and security. However, we believe the Agency has a duty to the American public to safeguard the integrity of the enumeration process.

Fraud Risk

Fraud risk is a major management challenge since it drains needed resources away from SSA's programs and beneficiaries, and attacks the very credibility of SSA's programs. As SSA's payments to beneficiaries approach half a trillion dollars annually, its exposure to fraud increases proportionately. Many unscrupulous individuals target SSA's programs to secure funds for their own personal gain. Fraud is an inherent risk in all of SSA's core business processes: enumeration, earnings, claims, and post-entitlement. All of these processes include vulnerabilities that provide individuals the opportunity to defraud third parties, SSA, and/or SSA's beneficiaries and recipients. Our focus on fraud risk is based on program eligibility factors that individuals misrepresent to attain or maintain eligibility.

Examples of the eligibility factors under the Old-Age, Survivors and Disability Insurance (OASDI) program include family relationships and, for surviving spouses under age 60, children in-care. SSA's difficulties in monitoring eligibility factors for SSI recipients is a key reason the SSI program has remained on the General Accounting Office's (GAO) list of "high-risk" Federal programs since 1997. Because the SSI program is means-based, it includes eligibility factors that tend to be more difficult for SSA to verify and monitor. These include income, resources, living arrangements, U.S. residency, and deemed income. While SSA is addressing the factors affecting the complexity of the SSI program, the Agency still relies on self-reporting of income, living arrangements and medical improvement in determining whether an individual is eligible for SSI payments. Other key risk factors common to both programs are the detection of beneficiary deaths and the monitoring of medical improvements for disabled beneficiaries.

SSA Has Taken Steps to Address this Challenge

SSA has taken an active role in addressing the integrity of the OASDI and SSI programs through its "zero tolerance for fraud" initiative. Key projects under this initiative include Prisoners, Fugitive Felons, and Electronic Death Registration. Additionally, through its Access to State Records On-line program, SSA has obtained on-line query access to selected records in 69 agencies in 42 States. SSA has also implemented a program for FO staff to identify recipient income before awarding SSI payments. This program provides FO staff with direct access to OCSE data bases related to wages, new hires, and unemployment insurance.

In addition to these new initiatives to address program fraud, SSA and the OIG continue to expand existing programs. SSA's Office of Operations and Office of Disability, in conjunction with the OIG, have formed 13 Cooperative Disability Investigation (CDI) teams. To combat disability fraud, these teams rely on the combined skills and specialized knowledge of OIG investigators, State and local law enforcement officials, and SSA and DDS personnel. During FY 2001, CDI teams prevented over $52 million in improper payments.

SSA's efforts to identify and terminate payments to incarcerated beneficiaries and recipients continue to be fruitful. SSA has agreements with 5,782 correctional facilities that cover over 99 percent of the inmate population. SSA estimates the suspension of payments to prisoners is saving the OASDI and SSI programs $500 million, annually. Incentive payments under the *1996 Welfare Reform Act* have contributed to that success. From March 1997 through July 2000, SSA paid $31.57 million in incentive payments. SSA's Actuary estimates that cumulative 7-year savings through the year 2001 will be $3.5 billion. Furthermore, a study based on Calendar Year 1996 data conducted by SSA's Office of Quality Assurance and Performance Assessment (OQA) estimated that 45 percent of prisoner alerts were productive with identification of retroactive overpayments totaling $202 million. In addition, OQA found that about $20 million per month in incorrect benefit payments were prevented.

SSA Needs to Continue to Address this Challenge

For SSA to fulfill its role as a steward of public dollars, it is imperative that the universe or magnitude of fraud be identified. For example, the insurance, retail, and banking industries have baselines to estimate potential dollars lost to fraud. A specific and significant fraud risk is the detection of unreported beneficiary and recipient deaths. SSA relies on its Death Alert, Control, and Update System (DACUS) to identify unreported deaths from Federal and State data bases through computer matches. One audit disclosed that about 881 auxiliary beneficiaries were paid about $31 million after their deaths because DACUS could not properly match their records. Another audit found inadequate controls over DACUS and identified 26 individuals who appeared to have fraudulently negotiated benefits of $429,779 paid for deceased beneficiaries.

Our audits have disclosed the need for SSA to improve its capability to avoid improper payments to fugitive felons. One audit disclosed that, without effective matching of State fugitive files, SSA would pay fugitives at least $30 million in SSI payments per year. As of October 2001, SSA had obtained and matched against the SSI benefit rolls fugitive data files from a number of States, the National Crime Information Center, and the U.S. Marshals Service.

Our investigative efforts to administer the Fugitive Felon Program since August 1, 1996 have identified 45,071 fugitives who were overpaid more than $81.6 million. Of the 45,071 fugitives, 5,019 were arrested, and we estimated the related savings to be about $133 million for the SSI program. While SSA has made progress in obtaining fugitive data, much more work remains in this area.

Another audit recommended that SSA pursue legislation to prohibit the payment of OASDI benefits to fugitives. We estimated that fugitives would receive at least $39 million in OASDI benefits annually unless legislation is enacted to prohibit these payments. While SSA agreed to pursue this legislation, it was not included in SSA's FY 2003 legislative package sent to Congress.

Government Performance and Results Act

The Government Performance and Results Act of 1993 (GPRA) established a system of strategic planning and performance measurement across the Federal Government. GPRA calls for Federal agencies to develop 5-year strategic plans, annual performance plans and annual performance reports. While SSA has made strides toward improving its performance measures, SSA can further strengthen its use of performance information by fully documenting the methods and data used to measure performance, and by improving the data sources that appear to be unreliable.

President Bush has placed great emphasis on the management and performance of Federal agencies. Through the Office of Management and Budget (OMB), the President has outlined Governmentwide management reforms and specific priority management issues for SSA to address. The Governmentwide reforms are budget and performance integration, strategic management of human capital, competitive sourcing, improved financial performance, and expanding electronic Government. The specific priority management issues that OMB outlined for SSA to address are the implementation of the Ticket-to-Work program, disability process redesign, and an updating of the disability medical listings. OMB also called for specific performance measures to be included within SSA's FY 2003 budget, including measures on disability claims processing costs, retirement claims processing costs, disability claims processing times, and amounts of improper payments paid to beneficiaries each year.

Recognizing the importance of GPRA and the results-oriented management it mandates, we developed a work plan to review SSA's implementation of GPRA. Our work has focused on two issues that are critical to the success of SSA's efforts to manage for results; determining the reliability of SSA's performance data and ensuring SSA's implementation of GPRA is in accordance with its requirements.

SSA Has Taken Steps to Address this Challenge

In response to GPRA, SSA also developed strategic plans, annual performance plans, and annual performance reports. Its most recent performance report for FY 2001 is included within SSA's Performance and Accountability Report. The FY 2001 performance plan and report are organized by SSA's five strategic goals, for which SSA describes the activities performed in support of each goal. There are 17 strategic objectives and 2 categories of output measures for major budgeted workloads supporting the 5 strategic goals. Under the objectives and categories, there are 71 specific performance indicators. SSA provides a general rationale, baseline performance information, data sources, and background information for each indicator.

To date, SSA has released multiple annual performance plans and reports. It has continually updated its annual performance plans, taking in to consideration changing priorities and workloads, as well as recommendations from the OIG and GAO.

SSA Needs to Continue to Address this Challenge

Our performance reviews over the last few years have found most of SSA's data to be reliable. We have, however, found that SSA often lacks documentation of the methods and data used to measure its performance. Despite these deficiencies for most measures, we were able to reproduce or obtain enough of the needed documentation to support our conclusions.

In some cases, the lack of documentation was significant and did not allow us to conclude on the quality of SSA's performance data. In FY 2001, we could not conclude on the reliability of the data, due to a lack of required documentation, for 6 of the 15 performance measures we reviewed.

Other reviews concluded that some data sources did not provide a reliable assessment of performance of the program being measured. We found the data for 5 of the 15 performance measures we reviewed in FY 2001 to be unreliable.

GPRA provides a framework by which SSA management can strategically plan and manage to meet its mission. SSA has made a commitment to use GPRA to develop plans and strategies that help it strategically manage and meet its mission. Our work has found that SSA can further strengthen its use of GPRA in its management through additional improvements to its performance plans and reports, by fully documenting the methods and data used to measure performance, and by working to improve the data sources where we found such sources to be unreliable estimates of performance.

Identity Theft

One of the fastest growing areas of concern for SSA and the OIG is the misuse of SSNs to commit crimes, particularly in the area of identity theft. In most cases, identity theft begins with the misuse of an SSN, and, while the ability to punish identity theft is important, the ability to prevent it is even more critical.

The public's growing concern with SSN misuse and identity theft is reflected in the large number of allegations our Fraud Hotline receives annually. In FY 2001, over 56 percent of the 115,101 allegations received involved SSN misuse and/or identity theft. The growth of these numbers is only limited by our capacity to answer the calls. We believe identity theft is a significant problem, and it is growing. We anticipate the complaints will increase unless SSA and Congress take firm actions to regulate the uses of SSNs.

Identity theft was already a significant problem facing law enforcement, the financial industry, and the American public before September 11th. In the weeks since that terrible day, it has become increasingly apparent that improperly obtained SSNs were a factor in the terrorists' ability to assimilate themselves into our society while they planned their attacks. While this has heightened the urgency of the need for Congress, SSA, and the OIG to take additional steps to protect the integrity of the SSN, it has not altered the nature of the steps that must be taken.

SSA Has Taken Steps to Address this Challenge

SSA employs a number of methods to combat identity theft. Specifically, SSA protects the privacy of the American public by using personal identifying information for Social Security purposes only—SSA does not give, sell, or transfer personal information to third parties. To assist in the prevention of invalid SSN use in the workplace, SSA provides a mechanism through which States and employers can verify SSNs provided by employees. SSA has also provided training to its FO employees on how they can best advise the public on how to prevent identity theft as well as helping victims resolve their problems. To detect, identify, and deter potential employee and client fraud within the Social Security programs, SSA uses its CIRP. CIRP is a business function used to deter and/or identify fraud by selecting fraud prone transactions for review on a regular basis. High-risk transactions are selected for review based upon selection criteria designed to identify transactions that have the highest fraud potential. Additionally, SSA has entered into partnerships with other agencies, such as the Federal Trade Commission, to fight identity crimes.

SSA Needs to Continue to Address this Challenge

To successfully address identity theft, we believe SSA must focus on three stages of protection: upon issuance of the SSN card, during the life of the SSN holder, and upon that individual's death.

For example, birth records, immigration records, and other identification documents presented to SSA must be independently verified as authentic before SSA issues an SSN. While this may subject the enumeration process to delays, such delays may be necessary to ensure the integrity of the SSN.

Protecting the integrity of an SSN during the life of the SSN holder is a difficult charge. The SSN has become an integral part of every day life, particularly in financial transactions, which makes it more difficult to give the number the degree of privacy it requires. Legislation, and more importantly, coordination between SSA and the financial services industry, can help limit the SSN's public availability to the greatest extent practicable.

Finally, SSA must do more to protect the SSN after the SSN holder's death. SSA receives death information from a wide variety of sources and compiles a Death Master File, which is updated monthly and transmitted to various agencies. It is also required to be offered for sale to the public and can be accessed over the Internet through a number of sources. Accuracy in this area is critical to SSA in the administration of its programs, to the financial services industry, and to the American people. Our audit work has revealed systematic errors in the Death Master File, and we have recommended steps that SSA can take to improve the reliability of this critical data.

The OIG plays an important role in helping other law enforcement agencies in their investigations. Because the SSN is such a widely-used means of identification, we are frequently contacted by Federal, State, or local law enforcement agencies seeking to verify that a name and SSN match.

Under existing law, the authority of the Commissioner of Social Security to provide this information is tenuous at best, and the authority of the Inspector General (IG) to do so is non-existent. We have entered into an agreement with the Commissioner by which the IG can provide this information under limited circumstances, but the authority should be statutory, unconditional, and irrevocable. In our current environment, this critical information should be available to law enforcement, and we should have the authority and the duty to provide it.

Privacy safeguards protecting IRS information in the possession of SSA are more restrictive than those protecting other SSA information, and rightly so. However, since the events of September 11th, there needs to be a mechanism in place so that information can be disclosed to law enforcement in emergency situations. Specifically, there should be a provision in law under which either the Commissioner of SSA (who has possession of the necessary information) or the SSA IG (who receives requests from the Federal Bureau of Investigation [FBI] and others) can make the determination that disclosure is necessary, then authorize and make the necessary disclosures to the law enforcement community in an expeditious manner.

Representative Payees

Some individuals cannot manage or direct the management of their finances because of their age or mental and/or physical impairments. While Representative Payees (Rep Payee) provide a valuable service for beneficiaries, SSA must employ appropriate safeguards to ensure they meet their responsibilities to the beneficiaries they serve.

Congress granted SSA the authority to appoint Rep Payees to receive and manage these beneficiaries' payments. A Rep Payee may be an individual or an organization. SSA selects Rep Payees for OASDI beneficiaries or SSI recipients when representative payments would serve the individual's interests. Rep Payees are responsible for using benefits in the beneficiary or recipient's best interests. There are about 4.2 million Rep Payees who manage approximately $45 billion in annual benefit payments for 6.5 million beneficiaries.

SSA Has Taken Steps to Address this Challenge

SSA has developed a monitoring program for certain Rep Payees. This program consists of:

*Triennial On-site Reviews—*On a 3-year cycle, SSA conducts on-site reviews of all fee-for-service Rep Payees, all volume organizational payees (serving over 100 beneficiaries), and all individual payees serving 20 or more beneficiaries.

*Annual Certification—*SSA annually verifies that the required license or bond is current for all fee-for-service Rep Payees.

*Random Reviews—*SSA conducts reviews of a random sample of 30 percent of all volume organizational and fee-for-service Rep Payees.

*6-Month Site Visits—*SSA visits fee-for-service Rep Payees 6 months after their initial appointment as a Rep Payee to ensure they fully understand their duties and responsibilities.

*Quick Response Checks—*SSA conducts reviews of organizational Rep Payees as needed in response to certain "trigger" events, such as third-party reports of misuse, complaints from vendors of failure to receive payment, or failure to complete the annual Rep Payee Report.

Finally, SSA has established a Rep Payee Task Force to perform a comprehensive review of the features and vulnerabilities of the Rep Payee program. The Task Force is comprised of three subgroups concentrating on monitoring Rep Payees; systems support for the Rep Payee program; and bonding and licensing of Rep Payees.

SSA Needs to Continue to Address this Challenge

In FY 2001, we performed six financial-related audits of Rep Payees. Our audits showed that Rep Payees did not always meet their responsibilities to the beneficiaries they served. We identified deficiencies with the financial management of, and accounting for, benefit receipts and disbursements; vulnerabilities in the safeguarding of beneficiary payments; poor monitoring and reporting to SSA of changes in beneficiary circumstances; and inappropriate handling of conserved funds.

We continue to identify problems with SSA's oversight of Rep Payees. For example, in March 2001, we alerted SSA to a condition whereby individuals were serving as Rep Payees who also had a Rep Payee to manage their own Social Security benefits. SSA subsequently identified approximately 3,800 instances where this had occurred.

Much is left for SSA to do to address the vulnerabilities and weaknesses in the Rep Payee program. This work includes the following:

*Selection of Rep Payees—*SSA has not determined how it will stop the selection of those Rep Payees who are most likely to commit misuse. Currently, SSA does not perform background checks of Rep Payees to determine whether they have financial problems, bad credit, or have been convicted of a felony. However, SSA has issued a contract to research options for criminal and financial background checks.

*Rep Payee System—*SSA is working to correct a number of system weaknesses we previously identified. Our findings in this area include:

- SSA's systems do not effectively track Rep Payees who do not respond to and complete Rep Payee Reports.
- SSA cannot always locate and retrieve completed Rep Payee Reports when needed.
- SSA's systems do not include information on all Rep Payees, and beneficiaries who have Rep Payees, as required by law.

*Bonding and Licensing of Rep Payees—*SSA's policy specifies neither the amount of bond necessary to adequately protect beneficiaries nor the type or nature of licenses that are required. To date, SSA has not made any revisions to its policy to address these vulnerabilities.

Stored Value Cards[3]*—We are exploring the use of Stored Value Cards (SVC) to help ensure the proper management of beneficiaries' funds. SSA may be able to employ the use of SVCs to better monitor its Rep Payees and reduce the administrative costs related to mailing, processing and storing annual Rep Payee Reports.*

[3] An SVC is a prepaid spending card that can be used everywhere a credit card is accepted. SVCs do not have a line of credit and can be used to make automated teller machine withdrawals.

Service to the Public

SSA is committed to providing responsive, world-class service. Providing quality service remains a critical management issue facing SSA, and SSA recognizes there are significant service delivery problems that need attention. SSA's workloads will continue to increase as "baby boomers" reach retirement age, challenging SSA to keep pace. As the Social Security Advisory Board reported, the result has been, and will continue to be, uneven service. Persons filing for retirement or survivor benefits are likely to be satisfied with the service provided. However, individuals with complicated cases, such as DI or SSI, may encounter problems. As workloads increase, the dimensions of SSA's problems can be expected to grow. If left unattended, the public will be faced with crowded reception areas, long waiting times, inadequate telephone service, and reduced quality of work.

SSA Has Taken Steps to Address this Challenge

SSA has developed a long-term Service Vision to describe its 10-year plan. The *Vision* is based on the premise that the convergence of the forecasted trends will provide SSA with the opportunity to (1) reshape its business processes, (2) reform its management of human capital and technology, and (3) deliver the service the American public demands. SSA plans to allow individuals to have access to one-stop shopping with single-points-of-entry to high quality Government services. Business partners that use SSA's earnings reporting process will switch from paper and magnetic tape reporting to Internet reporting, reducing their costs as well as SSA's. SSA plans on sharing information with Federal and State Government partners to serve the American public better. Additionally, SSA will rely on e-government solutions to increase its productivity and allow it to bridge the resource gap that will be created by the expected explosive growth in its workloads.

SSA Needs to Continue to Address this Challenge

While SSA met or came close to all of its goals related to its service, it will need to maintain existing service levels while exploring new and innovative ways to address service delivery problems. To accomplish this, SSA must recruit and retain a cadre of highly skilled employees. However, even at current staffing levels, SSA finds it difficult to maintain an acceptable level of service especially in its most complicated workloads. To make matters worse, SSA is facing an unusual wave of management and staff retirements. At the same time, the Agency may find it difficult to replace employee losses as the Nation's labor force of people between the ages of 25 to 44 is expected to shrink. If predicted shortages in human capital are realized, SSA may not be able to strengthen and revitalize future employee ranks as its workloads continue to grow in volume and complexity. Increasing workloads coupled with human capital shortages will further stress SSA's ability to provide quality service to the public.

In January 2001, GAO designated strategic human capital management as a high-risk, Government-wide issue needing immediate attention. This issue involves four pervasive Federal agency human capital challenges:

Acquisition and development of staffs whose size, skills, and deployment meet agency needs—ensuring current and future human capital needs are identified and gaps are filled through such efforts as effective recruiting, training, and contracting.

Leadership continuity and succession planning—ensuring there are qualified people available to assume top leadership positions before they become available.

Strategic human capital planning and organizational alignment—ensuring human capital strategies support strategic and program goals so an agency's mission, vision, and objectives are realized.

Creation of results-oriented organizational cultures—ensuring staff is empowered and motivated in conjunction with workplace accountability.

OIG and GAO have identified specific SSA human capital challenges and vulnerabilities that impact the Agency's ability to meet projected service delivery needs. These include:

Increasing demands for services—Beginning around 2008, the 76 million "baby boomers" will begin to move into their disability-prone years and begin to retire. SSA anticipates that by 2010, applications for DI will increase by as much as 54 percent over 1999 levels and applications for retirement benefits by 20 percent over 1999 levels. A large proportion of retirees is expected to be non-English speaking. Also, many disability cases are expected to be mental-related impairments. Demands for the way services will be delivered are also expected to change, with citizens wanting different modes of accessibility, for example, using the Internet and "one-stop shopping" to access services and programs through one interaction with the Government.

Retirement of a substantial portion of SSA's workforce—SSA workforce retirements will peak between 2007 and 2009 with about 3,000 employees retiring per year. For example, over 80 percent of SSA's upper-level managers and executives will be eligible to retire by 2010.

Mixed success in past technological investments—To address anticipated increased workload demands, SSA plans to rely heavily on information technology. However, according to the OIG and GAO, some of the Agency's past experiences have shown mixed success.

Ensuring funds are available to support human capital management efforts—SSA must ensure that its future budget request are adequate to address its human capital needs for the future.

Systems Security and Controls

The importance of computer system security increases as opportunities for users to disrupt critical systems, modify key processes, and read or copy sensitive data increases. Strong systems security and controls are needed to prevent access to confidential information and critical systems and the fraudulent use of SSA data. SSA continues to address systems vulnerabilities that could lead to unauthorized access or sabotage. Many of these vulnerabilities have been identified during the annual audit of SSA's financial statements, which have included reviews of SSA's systems security and controls.

SSA Has Taken Steps to Address this Challenge

SSA has taken steps to strengthen its system security and controls. Its security program has a number of key components created to help protect its systems:

- SSA uses an access control package to enforce its policies of separation of duties. The package also includes an authentication process that users must complete prior to accessing SSA systems;
- SSA continues to enhance its CIRP, which is a business function used to deter and/or identify fraud by selecting fraud-prone transactions for review on a regular basis. SSA has an audit trail system that can identify individuals who have accessed or processed specific records. This system can identify suspected problems and support investigation of these problems;
- All employees with access to SSA systems are required to sign an annual acknowledgement of the Agency's sanctions for systems access violations;
- SSA uses firewall technology to protect its network. The technology includes alerts and anomaly detection that identifies suspect activity; and
- SSA monitors its network 24 hours a day, 365 days a year.

Additionally, SSA has many on-going initiatives and new projects to further security awareness including:

- The Systems Security Handbook is available to all employees on SSA's Intranet;
- SSA's Intranet also has a variety of information for users of SSA systems including virus alerts and descriptions, listings of security officers and contacts, and links to other security web sites;
- Security training for all new employees and new supervisors;
- Risk/management training for all SSA systems managers and security personnel;
- Hosting security and anti-fraud conferences, as well as participation in numerous security conferences/symposiums hosted by other organizations;
- Producing desk-to-desk security alerts; and
- Certification training for SSA security professionals.

SSA established the Division of Systems Security and Program Integrity within its Office of Operations to enhance its security and integrity network and provide a focal point to address security issues. The Office of Operations also established Centers for Security and Integrity within each region and the Office of Central Operations to provide the proper level of focus on security and integrity issues nationwide.

SSA Needs to Continue to Address this Challenge

Strong systems security and controls are essential to protecting SSA's critical information infrastructure. SSA's current information security challenge is to understand system vulnerabilities and how to mitigate them. By improving systems security and controls, SSA will be able to use current and future technology more effectively to fulfill the ublic's needs.

To better protect its systems and the information contained within them, SSA should centralize all of its systems security management structure under the Chief Information Officer (CIO) to comply with the Government Information Security Reform Act (GISRA) and other laws to ensure all key security components responsible for agencywide security, policy, and administration report directly to the CIO. Currently, these functions are spread across several components within SSA.

GISRA requires each Agency to develop and implement an agencywide information security plan for its assets and operations, and requires the OIG to determine the efficiency and effectiveness of the overall security program and practices. SSA has developed and implemented an agency-wide information security plan for its assets and operations. Our assessment of SSA's compliance with GISRA concluded that SSA generally meets the requirements of GISRA; however, there are opportunities for the Agency to strengthen its information security framework to ensure full compliance with GISRA and the information security-related laws and regulations that provide the foundation for GISRA.

Our work to date has noted other control weaknesses, including:

- SSA needs to perform background checks on SSA employees and contractors to protect its most sensitive data;
- SSA needs to limit employee access to those on a need to know basis;
- SSA needs to implement more stringent physical security measures at all SSA facilities so its most valuable asset, its human capital, is properly protected;
- SSA needs to develop performance measures to protect its critical physical assets, and continue to perform risk and possibly vulnerability assessments; and
- SSA needs to strengthen its information security framework to ensure full compliance with GISRA. Specifically, SSA needs to (1) have specific security performance measures, (2) evaluate all of its critical assets, (3) globally track information technology (IT) security training by its security staff, and (4) itemize IT security costs by projects.