OFFICE OF
THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

SOCIAL SECURITY ADMINISTRATION'S CONTROLS OVER REDISCLOSURE OF SENSITIVE INFORMATION IN THE KANSAS CITY REGION

November 2007 A-07-07-17055

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: November 28, 2007 Refer To:

To: Michael W. Grochowski
Regional Commissioner
Kansas City

From: Inspector General

Subject: Social Security Administration's Controls over Redisclosure of Sensitive Information in the Kansas City Region (A-07-07-17055)

OBJECTIVE

Our objective was to evaluate the controls the Kansas City Region has in place to ensure that sensitive information shared with State agencies and their contractors is not being improperly redisclosed to unauthorized parties.[1]

BACKGROUND

The Social Security Administration (SSA) through its computer matching program, also known as the data exchange program, shares applicant and beneficiary information with State agencies for the purpose of verifying eligibility for benefits.[2] The Social Security Act requires that "…a State must have in effect an income and eligibility verification system…" to administer federally-funded benefit programs such as Medicaid, food stamps, and temporary assistance for families.[3]

[1] Sensitive information is defined by SSA as "information, the loss, or misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled to under 5 U.S.C. § 552a (the Privacy Act) …." This includes personally identifiable information (PII), which SSA defines as "information obtained from SSA that can be used … to identify a specific individual." Examples of PII are name, Social Security number, Social Security benefit data, birth date, or State or Government issued driver's license or identification number.

[2] POMS GN03314.001J.2 and GN03314.155A.

[3] The Social Security Act, § 1137(a), 42 U.S.C. § 1320b-7(a).

SSA's written data exchange agreements comply with the Privacy Act,[4] which requires the confidentiality of information maintained by Federal agencies and provides guidance on disclosing personal or sensitive information. The Privacy Act states the data exchange agreement should include:

- procedures for ensuring the administrative, technical, and physical security of the records matched and the results; and

- a ban on duplicating and redisclosing records provided by the source agency within or outside the recipient agency, except as required by law or essential to the matching program.[5]

Each SSA Regional Office has a Data Exchange (DX) coordinator who is the contact for State agencies that have a data exchange agreement with the Region. The DX coordinator plays a vital role in assisting State agencies with issues and problems in the data exchange process.

The Kansas City Regional Office requested this review because of concerns that unauthorized redisclosure of SSA's sensitive information may be occurring.[6] Accordingly, we conducted a review of the Iowa Department of Human Services (IA-DHS) and eight of its contractors performing work in the areas of Medicaid and Foster Care. See Appendix B for the scope and methodology of our review and Appendix C for flow charts of the current data exchange process.

RESULTS OF REVIEW

Our review focused on the controls the Kansas City Regional Office has in place to ensure that sensitive information shared with State agencies and their contractors is not being improperly redisclosed to unauthorized parties.[7] Specifically, we examined the controls the Kansas City Region has in place to prevent, detect and resolve instances of unauthorized redisclosure. We found that the controls in place to resolve reported data exchange problems appear to be adequate. However, the controls to prevent and detect unauthorized redisclosure need to be improved. Specifically, we found the current controls did not prevent IA-DHS and two of its contractors from redisclosing sensitive information without authorization from SSA nor did the controls detect these instances of redisclosure.

---

[4] The Privacy Act of 1974, 5 U.S.C. § 552a.

[5] The Privacy Act of 1974, 5 U.S.C. § 552a(o).

[6] Unauthorized redisclosure of sensitive information refers to the release of sensitive information to a user that has not been granted access to the information through a signed data exchange agreement.

[7] During the course of our review, SSA established a new data exchange agreement which was effective July 1, 2007. The prior data exchange agreement was in effect from January 2005 through June 2007.

INSTANCES OF IMPROPER REDISCLOSURE OF SSA SENSITIVE INFORMATION

Our review of IA-DHS and eight of its contractors identified instances where sensitive SSA information was improperly redisclosed. As such, IA-DHS violated the terms of the data exchange agreement. Specifically, the following instances of improper redisclosure were identified:

- An IA-DHS contractor duplicated SSA information including the Social Security number (SSN) in its private computer system. The contractor used the SSN as a primary identifier for tracking foster care clients. The data exchange agreement prohibits the duplication of sensitive SSA information without SSA's approval.[8]

- All IA-DHS and contractor employees located at the Iowa Medicaid Enterprise facility had computer access to Medicaid reports containing SSA sensitive information. Access to these reports should have been restricted only to employees with a need to know such information.[9]

- IA-DHS allowed a contractor access to sensitive SSA information in its computer system without having a signed contractor redisclosure request form.[10] The contractor redisclosure request form obligates the contractors to follow the terms of the data exchange agreement including securing SSA sensitive information.

- An IA-DHS contractor shared paper copies of computer screen prints with another State agency. The computer screen prints contained sensitive SSA information including SSNs. Prior to sharing this information, a signed redisclosure request form should have been in place.

These instances of improper redisclosure occurred because SSA did not have sufficient controls in place to help prevent the redisclosure or detect that the redisclosure had occurred. As the following discussion illustrates, SSA needs to improve its prevention and detection controls to reduce the risks associated with unauthorized disclosure.

---

[8] Prior data exchange agreement, Article X.A.3; new data exchange agreement, Article XIII.A.5. During the course of our review, the IA-DHS instructed the contractor to delete the SSA sensitive information from its database.

[9] Prior data exchange agreement, Article IX.A.1; new data exchange agreement, Article XI.A.1.

[10] The Kansas City Regional Office created and used the contractor redisclosure request, "Request to SSA to Include Contracted Agent in State Agreement," in the Region's four States. The redisclosure request required signatures by the State agency director, the Regional Commissioner, and the contractor's project director. The redisclosure request (1) obligated contractors to follow provisions in the data exchange agreement, (2) stated the reasons for the contractor's access to sensitive information in the State agency computer system, and (3) authorized the access. Effective with the new data exchange agreement, State agencies are required to obtain the contractors' written agreement to abide by the security requirements, and the access, use, and disclosure restrictions in the data exchange agreement before the disclosure of sensitive information (Article XIII.A.6).

Prevention and Detection Controls

One of SSA's primary controls in the data exchange process is the data exchange agreement. SSA requires the State agency receiving sensitive SSA information to comply with the terms of the agreement. Furthermore, SSA requires the State agency to oversee contractor compliance with the agreement's redisclosure provisions and information safeguards when sensitive information is shared with contractors. Another control SSA has in place is compliance reviews conducted by SSA's Office of Systems Security Operations Management (OSSOM). These reviews evaluate the computer system safeguards that SSA requires of the State agency.[11] However, the reviews do not include the evaluation of safeguards in contractors' private computer systems or detect the type of redisclosure instances we identified during our review.

The data exchange agreement and the OSSOM reviews will not prevent or detect all instances of improper redisclosure. For example, as previously discussed in this report, one of the redisclosure instances we identified involved an IA-DHS contractor that duplicated sensitive SSA information. The data exchange agreement clearly prohibits duplication; however, it does not provide a process to detect it when it occurs.[12] Therefore, SSA remains at risk for such instances of unauthorized redisclosure of its sensitive information since it does not have a process in place that would detect the unauthorized redisclosure.

To mitigate this risk, SSA would have to establish additional controls. SSA and IA-DHS could consider performing reviews targeting instances of unauthorized redisclosure that would not be identified by OSSOM's compliance reviews. In fact, SSA and IA-DHS have the authorization to perform reviews of controls protecting SSA's sensitive information.[13] However, no reviews of contractors' facilities, computer system safeguards, or confidentiality and redisclosure practices have been conducted by the Kansas City Regional Office or IA-DHS. According to IA-DHS, it plans to implement a process to begin reviews of contractors' information safeguards sometime this year.

---

[11] As part of the data exchange agreement, the State agency receives SSA guidelines on computer system security: "Information System Security Guidelines for Federal, State and Local Agencies Receiving Electronic Information from the Social Security Administration." The State agency is required to (1) implement computer security controls before the data exchange with SSA begins and (2) hold contractors accountable for implementing the appropriate computer security.

[12] "Except as necessary for the operation of this matching program, as provided in this agreement, files provided by SSA will not be duplicated or disseminated within or outside the State Agency without the written approval of SSA. SSA will not grant such authority unless the redisclosure is required by law or is essential to the matching program. In such instances, the State Agency must specify in writing what records are being disclosed, to whom, and the reasons that justify such redisclosure." (Sources: prior data exchange agreement, Article X.A.3, effective January 2005 to June 2007; new data exchange agreement Article XIII.A.4, effective July 1, 2007).

[13] A provision in the prior data exchange agreement (Article IX.B) allowed SSA to conduct "on-site inspections or make other provisions to ensure that adequate safeguards are being maintained…" at the State agency level. At the contractor level, SSA considers the State agency responsible for contractors and requires the agency to inspect the security of each contractor's facilities (POMS SM10801.500.5b). Finally, the contractor's agreement with IA-DHS gives authority to IA-DHS or IA-DHS' representative (such as SSA) to monitor and review contractors.

The absence of prevention and detection controls increases the risk of unauthorized redisclosure for SSA. To mitigate the risk, the Regional Commissioner, in cooperation with the Office of the General Counsel, OSSOM, and Office of Automation Support should consider:

- Conducting periodic on-site inspections to verify whether State agencies redisclose sensitive SSA information without authorization; and

- Adding a provision in the data exchange agreement requiring the State agency to perform periodic on-site inspections of contractors' sensitive information safeguards, including confidentiality and redisclosure procedures and practices as well as contractors' computer system safeguards.

CONTROLS TO RESOLVE DATA EXCHANGE PROBLEMS

The Kansas City Regional Office's process for resolving data exchange problems appears to be adequate. The Regional Office's current process is for the State agency to report unauthorized redisclosure or other data exchange problems to the DX coordinator in its Center for Programs Support. The DX coordinator works to resolve the problem with the State agency by using regional resources first. If the problem requires reporting to or further attention from SSA, the DX coordinator refers the problem to one or more SSA components in Baltimore, Maryland for resolution. See Flow Chart 3, Appendix C, for a chart of the reporting and resolution process.

When the data exchange problems involve the loss or possible loss of PII, the reporting requirements for the Regional Office are outlined in the data exchange agreement.[14] The data exchange agreement requires that SSA will: (1) assume responsibility for making the contact within SSA so that a formal report is filed in accordance with SSA procedures and (2) notify the Department of Homeland Security's United States Computer Emergency Readiness Team if loss or potential loss of PII related to the data exchange occurs. Accordingly, the Regional Commissioner should determine if the four incidences of redisclosure identified in this report meet the loss or possible loss of PII criteria and take appropriate actions.

CONCLUSION AND RECOMMENDATIONS

We reviewed IA-DHS and eight contractors to determine if the Kansas City Regional Office had adequate controls to prevent, detect and resolve improper redisclosure of SSA sensitive information. Controls to resolve reported data exchange problems appeared to be adequate. However, SSA's controls to prevent and detect redisclosure were not sufficient and need to be improved to reduce the risk of instances of unauthorized redisclosure like the ones identified in our review.

[14] SSA data exchange agreement, effective July 1, 2007, Article XII.

Improper redisclosure of SSA sensitive information by State agencies and their contractors is an inherent risk in the data exchange process and there is no way to completely prevent it from occurring. However, there are ways to mitigate the risk. Accordingly, we recommend the SSA Regional Commissioner:

1. Ensure that State agency contractors in the Kansas City Region have signed an agreement that obligates them to follow the terms in the data exchange agreement.

2. Work with the appropriate Headquarters' components to determine when and by whom periodic on-site inspections should be conducted to ensure that State agencies in the Kansas City Region have sufficient controls in place to prevent and detect the types of redisclosure instances we identified in our review.

3. Work with the appropriate Headquarters' components to determine whether a provision should be added to the data exchange agreement requiring the State agency to perform periodic on-site inspections of contractors' safeguards for sensitive information, including contractors' private computer system safeguards as well as a review of confidentiality and redisclosure procedures and practices.

4. Determine if the four incidences of redisclosure identified in this report meet the loss or possible loss of PII criteria and take appropriate actions.

AGENCY COMMENTS

SSA agreed with our recommendations. The full text of SSA's comments is included in Appendix D.

Patrick P. O'Carroll, Jr.

Appendices

Acronyms

DX	Data Exchange
IA-DHS	Iowa Department of Human Services
OGC	Office of the General Counsel
OSSOM	Office of Systems Security Operations Management
PII	Personally Identifiable Information
POMS	Program Operations Manual System
SSA	Social Security Administration
SSN	Social Security Number
U.S.C.	United States Code

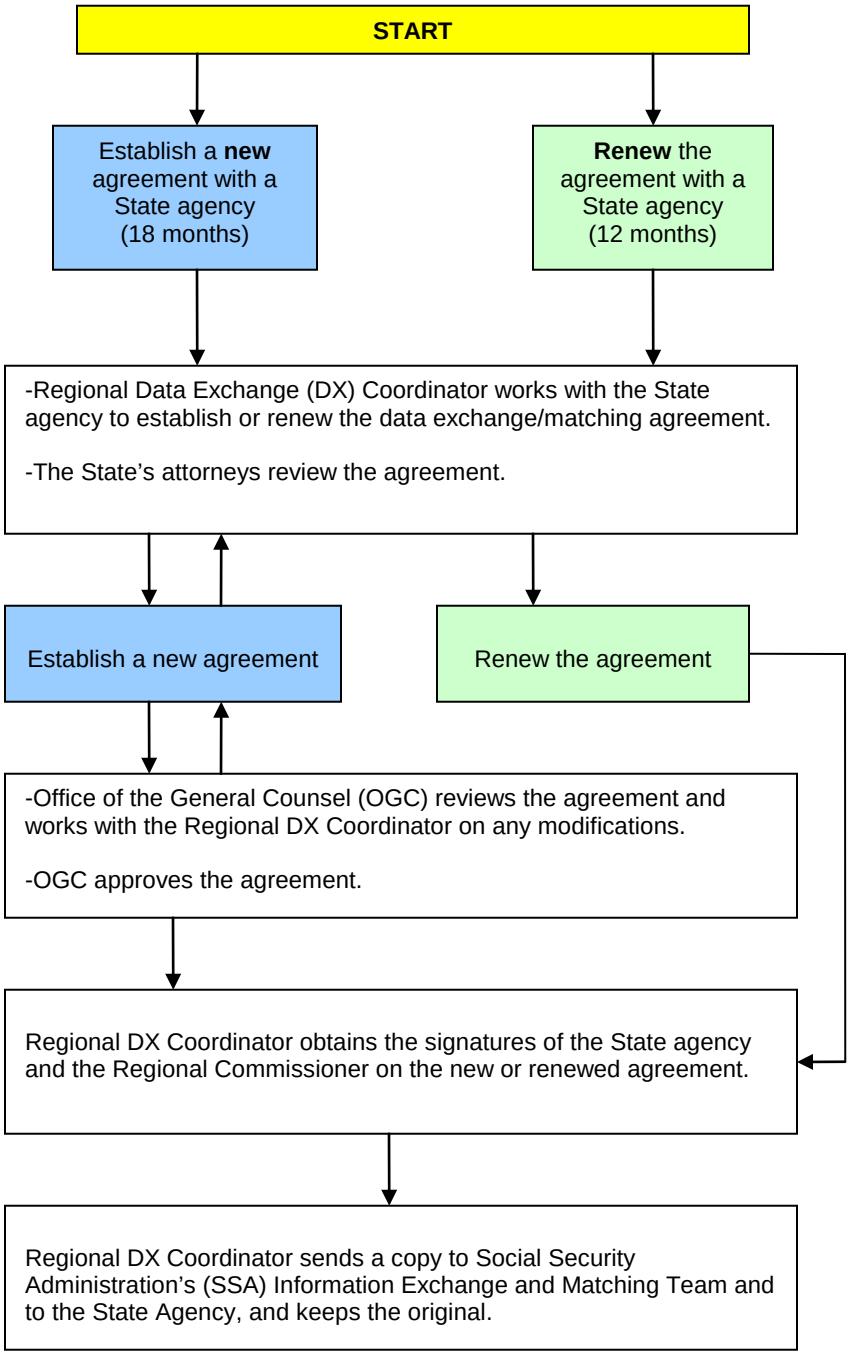
Scope and Methodology

To meet our objective, we:

- Reviewed applicable Federal laws and regulations, as well as pertinent sections of the Social Security Administration's Program Operations Manual System, and Administrative Instruction Manuals.
- Reviewed related Office of the Inspector General reports and Government Accountability Office reports.
- Reviewed Regional Office information related to redisclosure policy and issues.
- Reviewed the prior data exchange agreement between the Social Security Administration (SSA) and Iowa Department of Human Services (IA-DHS), effective January 2005 through June 2007, and the new data exchange agreement, effective July 1, 2007.
- Conducted interviews of IA-DHS and eight of its contractors and performed security walk throughs of offices and facilities.
- Reviewed policy and procedures from IA-DHS related to confidentiality and safeguarding sensitive information; reviewed contractor redisclosure requests and IA-DHS' contractors' agreements.
- Sent questionnaires to SSA components (Office of the General Counsel, Office of Systems Security Operations Management, and Information Exchange and Matching Team) requesting information on their roles in redisclosure policy and issues; analyzed responses and created flow charts of the data exchange process.

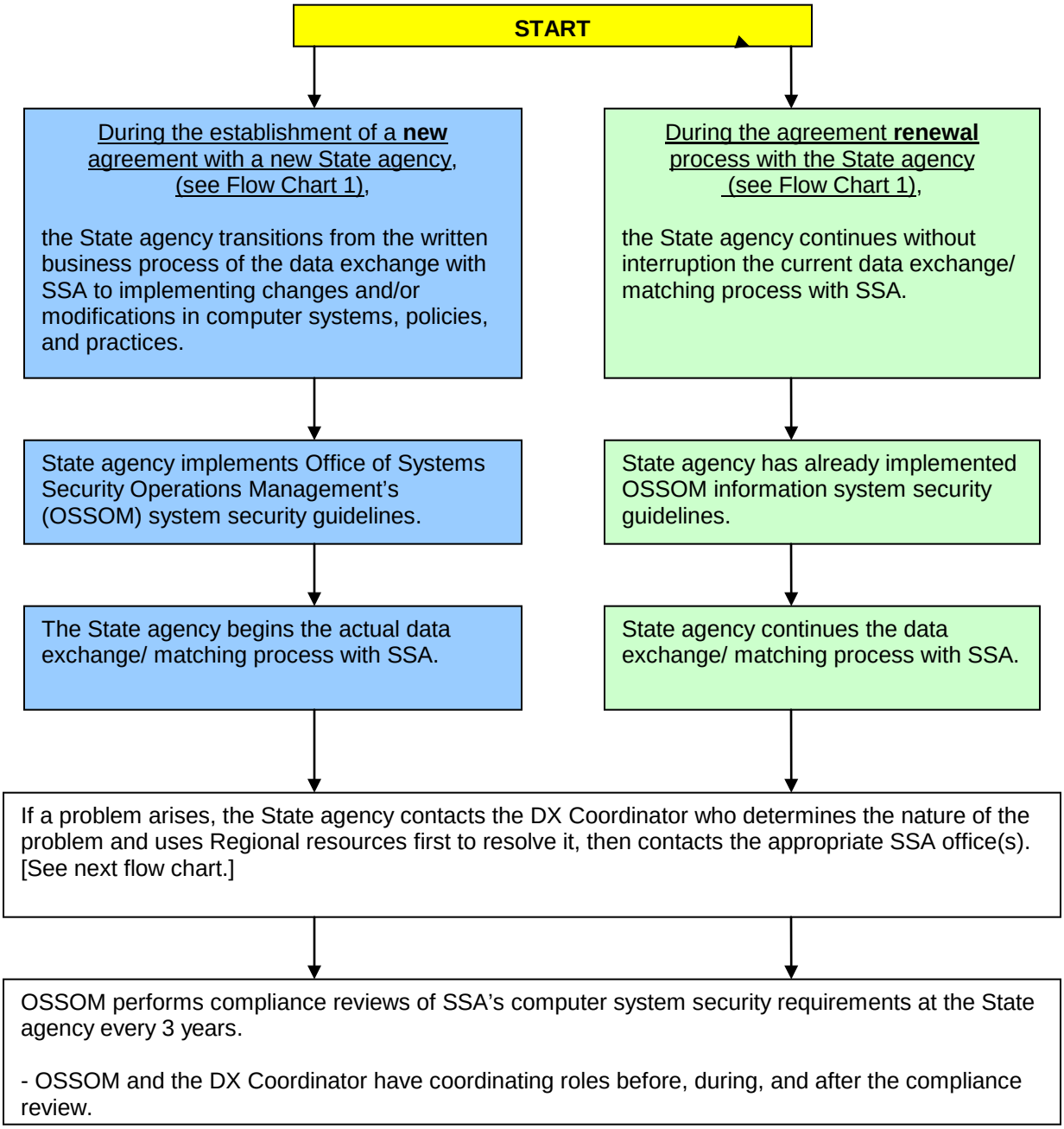
We conducted our evaluation between December 2006 and March 2007 in Des Moines, Iowa, and Kansas City, Missouri. We conducted the review in accordance with the *Quality Standards for Inspections* by the President's Council on Integrity and Efficiency.

Flow Chart 1: The Current SSA Data Exchange/ Matching Agreement Process with a State Agency*



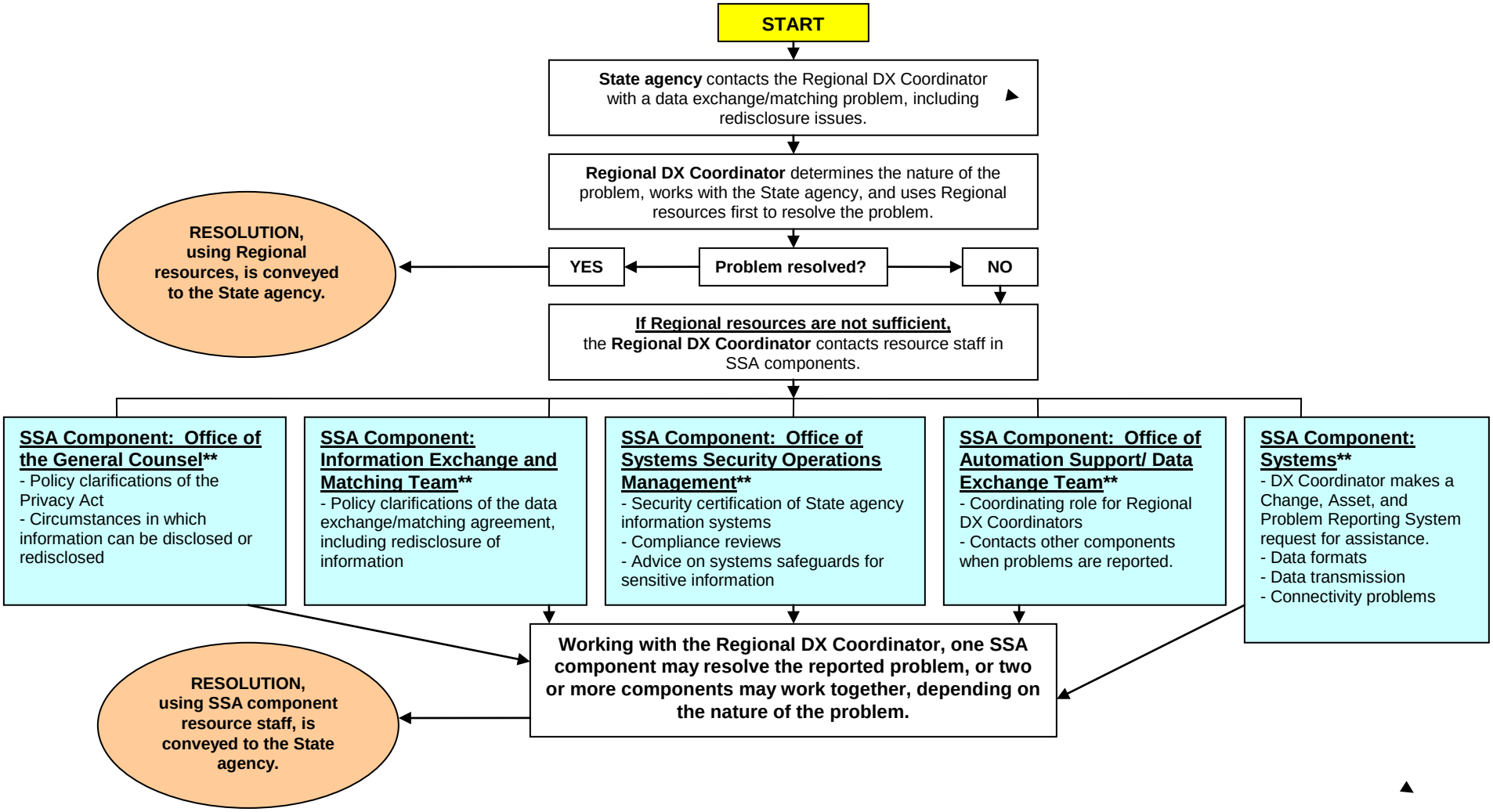
* This flow chart describes the data exchange/matching process which began with the January 2005 model agreements. The data exchange/matching agreement cycle is 30 months: 18 months for a new agreement with a 12-month renewal.

Flow Chart 2: Implementing or Continuing the Data Exchange/ Matching Operation*



* This flow chart describes the data exchange/matching process which began with the January 2005 model agreements. The data exchange/matching agreement cycle is 30 months: 18 months for a new agreement with a 12-month renewal.

Flow Chart 3: Resolution of Problems in the Current SSA Data Exchange/Matching Process*



* This flowchart describes the general problem resolution procedure in the data exchange/matching process which began with the January 2005 model agreements.

** Office of the General Counsel/Office of Program Law; Office of Public Disclosure;
Office of Disability and Income Security Programs/Office of Income Security Programs/Office of Earnings and Information Exchange/Information Exchange and Matching Team;
Office of Financial Policy and Operations/Office of Systems Security Operations Management;
Office of Operations/Office of Automation Support/Division of Electronic Service Delivery/Data Exchange Team;
Office of Systems/Office of Earnings, Enumeration and Administrative Systems/Division of Information, Verification and Exchange Services/Data Exchange Branch.

Agency Comments

To: Inspector General

From: Regional Commissioner
Kansas City Region

Subject: SSA's Controls over Redisclosure of Sensitive Information (A-07-07-17055) - Response

Thank you for the opportunity to comment on the attached draft audit report. During the course of this audit, our staffs had several opportunities to meet and discuss the complexities of the data exchange process. I appreciate the amount of work that went into this audit and the preparation of this report.

Our comments on OIG's recommendations are as follows:

1. Ensure that State agency contractors in the Kansas City Region have signed an agreement that obligates them to follow the terms in the data exchange agreement.

    - We agree with this recommendation. The requirements in SSA's data exchange agreements changed with the July, 2007 agreement cycle. These changes were incorporated to heighten awareness of agreement compliance issues at both the State and Federal level. For example, the agreements now contain specific language regarding the State's use of contractors. In addition, they require State Agencies to provide contractors/agents with a copy of the data exchange agreement and related attachments **before** they provide the initial disclosure of data to the contractor/agent.

2. Work with the appropriate Headquarters' components to determine when and by whom periodic on-site inspections should be conducted to ensure that State agencies in the Kansas City Region have sufficient controls in place to prevent and detect the types of redisclosure instances we identified in our review.

    - We agree with this recommendation. The Office of Systems Security Operations Management (OSSOM) currently has jurisdiction for all Data Matching systems security and agreement compliance reviews and conducts periodic onsite reviews (at least every three years) to ensure compliance with the agreement. Recently, the Kansas City Region has been assigned the Operation's Lead for a workgroup to explore how the regions can assist with oversight of agreement compliance at the regional level. Onsite inspections

are one of many options the workgroup is taking under consideration to improve agreement compliance. If this proposal is adopted, it would have the potential of providing more frequent onsite reviews.

3. Work with the appropriate Headquarters' components to determine whether a provision should be added to the data exchange agreement requiring the State agency to perform periodic on-site inspections of contractors' safeguards for sensitive information, including contractors' private computer system safeguards as well as a review of confidentiality and redisclosure procedures and practices.

   - We will refer this recommendation to our Headquarters component responsible for writing the agreements. Although we agree with the content of this recommendation, the language for the Computer Matching Agreements are determined at the Agency level and approved by the Office of Management and Budget. We believe that State oversight of contractors is critical to agreement compliance. The Kansas City led workgroup will address how this could possibly be accomplished and, where appropriate, make recommendations to the Deputy Commissioner for Operations for possible changes.

4. Determine if the four incidences of redisclosure identified in this report meet the loss or possible loss of PII criteria and take appropriate actions.

   - Through our prior experiences with State Agencies, we have found that one of the obstacles to proper disclosure is the lack of a written definition of what constitutes "SSA Information" as it relates to our computer matching process. Another task of the aforementioned workgroup has been to establish a written definition of "SSA Information" that can be easily understood and applied by all involved. This definition, which has been approved by the Office of Public Disclosure (OPD), provides us with an analysis tool for determining whether SSA or State information is involved in redisclosures. Note: This definition was **not** available when OIG conducted this audit.

     My staff will contact the State to expand upon the details concerning the redisclosures referenced in the OIG report. We will apply the OPD-approved written definition of SSA Information to our analysis of each of the redisclosure scenarios.

     Should we determine that SSA Information was involved, we will refer the incidents to our Regional Security and Integrity staff to determine if loss of Personally Identifiable Information (PII) applies and take appropriate actions.

If you have questions, please contact me at 816-936-5700. If your staff needs additional assistance or information, they may contact Kathy Woolsey, Director, Center for Programs Support by email at kathy.t.woolsey@ssa.gov or by phone at 816-936-5630.

/s/
Michael W. Grochowski

OIG Contacts and Staff Acknowledgments

OIG Contacts

Mark Bailey, Director, Kansas City Audit Division (816) 936-5591

Ron Bussell, Audit Manager (816) 936-5577

Acknowledgments

In addition to those named above:

Carol L. Cockrell, Senior Analyst

For additional copies of this report, please visit our web site at www.ssa.gov/oig or contact the Office of the Inspector General's Public Affairs Specialist at (410) 965-3218. Refer to Common Identification Number A-07-07-17055.

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, Subcommittee on Human Resources

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

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

Chairman and Ranking Minority Member, Committee on Governmental Affairs

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 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 our Office of Investigations (OI), Office of Audit (OA), Office of the Chief Counsel to the Inspector General (OCCIG), and Office of Resource Management (ORM). To ensure compliance with policies and procedures, internal controls, and professional standards, we also have a comprehensive Professional Responsibility and Quality Assurance program.

Office of Audit

OA conducts and/or supervises 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 and program evaluations and projects on issues of concern to SSA, Congress, and the general public.

Office of Investigations

OI conducts and coordinates investigative activity 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 OIG liaison to the Department of Justice on all matters relating to the investigations of SSA programs and personnel. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

Office of the Chief Counsel to the Inspector General

OCCIG provides independent legal advice and counsel to the IG on various matters, including statutes, regulations, legislation, and policy directives. OCCIG 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. Finally, OCCIG administers the Civil Monetary Penalty program.

Office of Resource Management

ORM supports OIG by providing information resource management and systems security. ORM also coordinates OIG's budget, procurement, telecommunications, facilities, and human resources. In addition, ORM is the focal point for OIG's strategic planning function and the development and implementation of performance measures required by the Government Performance and Results Act of 1993.