OFFICE OF
THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

THE IMPACT ON NETWORK SECURITY OF THE SOCIAL SECURITY ADMINISTRATION'S OPERATING SYSTEMS' CONVERSIONS

September 2004 **A-14-04-24019**

AUDIT REPORT

Mission

We improve SSA programs and operations and protect them against fraud, waste, and abuse by conducting independent and objective audits, evaluations, and investigations. We provide timely, useful, and reliable information and advice to Administration officials, the 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

By conducting independent and objective audits, investigations, and evaluations, we are agents of positive change striving for continuous improvement in the Social Security Administration's programs, operations, and management and in our own office.

SOCIAL SECURITY

MEMORANDUM

Date: September 17, 2004 Refer To:

To: The Commissioner

From: Acting Inspector General

Subject: The Impact on Network Security of the Social Security Administration's Operating Systems' Conversions (A-14-04-24019)

OBJECTIVE

Our objective was to determine if the Social Security Administration's (SSA) conversion from the Windows NT operating system increased, maintained, or decreased network security.

BACKGROUND

The network operating systems in SSA's distributed data processing environment have intrinsic security features that protect the sensitive information that the Agency processes, stores, and transmits. In converting from its Windows NT network operating system, SSA had the opportunity to maintain, diminish, or enhance network security. The effect the conversion will have on network security depends on SSA's ability to take advantage of the security features the operating systems contain.

Operating system security features work by limiting user access to system resources including data and application programs. They also identify and report on such accesses. These identification, exclusion, and reporting functions keep unauthorized individuals or groups from obtaining confidential information that they do not legitimately need. The use of these security features is affected by system security configuration settings. The availability of specific features and the configuration settings vary depending on the operating system. The security features of newer operating systems tend to be more specific in defining who has access to sensitive resources, and reporting these accesses.

We began this audit when SSA began to migrate its network environment to the newer Windows 2000 operating system. We conducted our review to determine the effect that changing from one operating system's security features to another would have on overall network security.

SCOPE AND METHODOLOGY

We reviewed SSA's operating system migration to determine its effect on a number of factors of network security. These factors included: 1) the security capabilities of the operating systems involved; 2) the criteria used to select and set security features; 3) the effect security-related settings would have on system operation for the users; 4) any problems encountered by changing the operating systems; and 5) compliance with Government standards and industry best practices.

We based our determinations on interviews with staff involved with the operating system migration and on the examination of policy, practice, and available management information, as well as guidelines, standards, and best practices.

During the course of our audit, SSA expanded its operating system migration plan to include a changeover to a third, newer operating system environment using Windows 2003 and Windows XP. This expansion was initiated before the original migration from Windows NT to Windows 2000 was completed. The scope of this audit encompasses this migration as well.

We audited components within SSA's Office of Systems and Office of Operations at SSA Headquarters in Baltimore, Maryland between June 2003 and April 2004. Our audit was conducted in accordance with generally accepted government auditing standards.

RESULTS OF AUDIT

SSA migrated its network environment from one based on Windows NT to one based on Windows 2000. Because of strategic considerations including the problems encountered, SSA decided to migrate ahead of schedule to the next operating systems, Windows 2003/XP. With each conversion, the Agency has taken advantage of newer, improved, and more developed operating systems to increase network security. SSA network developers acknowledge, and we noted, several problems that prevented the migrations from proceeding as originally planned.

- When SSA implemented Windows 2000, its security settings would not allow a number of application programs to run.

- Some of the application compatibility problems experienced in the first migration are beginning to surface in the second.

- In cases of problem applications, SSA does not use an established and enforceable set of standardized processes and programming language to ensure operating system security compliance and compatibility.

- Integration and Environmental (IE) testing procedures, which prevent the implementation of problem applications, were not always used in the operating system migrations.

WINDOWS NT TO WINDOWS 2000 MIGRATION

Federal law[1] and guidance[2] require SSA to provide for the cost-effective security and privacy of sensitive information in its systems. This is to "assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications." To provide such security, the migration as originally planned used a Windows 2000 security template to enforce security at a high level. Although not mandated to do so, the Agency chose to develop its template by adapting the most secure of five available templates, the "Gold Standard Template"[3] to the SSA network environment.

This collection of security configuration settings was very restrictive and would not allow some applications to access system resources they needed to run. Applications affected included those developed for earlier environments and carried over as "legacy" applications. These and other applications posed problems when their developers didn't ensure their compatibility with the new network environment. Some of these applications[4] are used on a routine basis for regular Agency operations.

Developers first tried to solve the problems encountered by lowering, turning off, and/or circumventing the configuration settings of the security template so that individual applications could run. This compromised the system security. After SSA made a number of these adjustments to the security template, it decided that the template was not capable of providing the intended level of security and replaced it with one containing lower security, specifically default, configuration settings. They also started to modify applications individually so that they could eventually run under higher security settings. SSA believed that if all necessary applications were modified in this way, the system would return to a high security level. This process, however, became overly time consuming and demanding of programmer resources, and was not guaranteed to work.

After we initiated our audit, SSA abandoned this approach, settled the network environment at whatever level of security it could implement and still run the problem applications, and started to concentrate efforts on a new environment.

---

[1] The Computer Security Act of 1987, Pub. L. No. 100-235 §4.
[2] Office of Management and Budget (OMB) Circular No. A-130, Appendix III, A.3.
[3] The "Gold Standard Template" is the composite best thinking of security groups that have developed security templates in the past (National Institute of Standards and Technology, National Security Agency, SANS Institute, etc.).
[4] These applications include, for example, national legacy applications that are used for: Amortization, Computation of Military Income, One Time Payment, Net Rental Income, and Retrospective Monthly Accounting.

SSA's network systems environment currently operates as a compromise as follows:

- Servers run the older Windows NT operating system to authenticate users to the system,
- Servers run Windows 2000 to manage accesses to data and applications, and
- User workstations run on Windows 2000 without high security.

This compromise may provide better security than networks running solely on older operating systems, like Windows NT, but does not take advantage of the security potential that Windows 2000 or newer operating systems provide.

In the current network environment, overall network security configuration settings have to be changed to allow legacy application programs to run on newer operating systems with more stringent requirements. These changes are necessary because the programs themselves are not being changed to accommodate higher network security.

WINDOWS 2000 TO WINDOWS 2003/XP MIGRATION

In 2003, SSA began the transition to a newer network operating system environment: Windows 2003 for servers and Windows XP for workstations (Windows 2003/XP). This implementation is currently under development with different projects progressing at different rates and is subject to the same requirements for security as previously discussed.[5] Both the server and workstation operating systems should be able to work with similar security templates and take advantage of enhanced features for providing security, including Active Directory.[6] Such capability would lessen the risk of inappropriate access while maintaining a high level of security like that specified in Microsoft's High Security template.

It is impossible to verify at this point whether Windows 2003 and Windows XP will be implemented to use high security templates that permit all necessary applications to run. The environment using these operating systems is still under development. Project plans for some components have not been drafted yet and some are still subject to frequent changes. The planned security templates are still being modified on a regular basis to accommodate users and applications. Even this early in the transition, developers have found the same problems as in the first migration. Some applications may still require security adaptations that lower, turn off, and/or circumvent configuration settings.

---

[5] OMB Circular No. A-130, Appendix III, A.3, and the Computer Security Act of 1987, Pub. L. No. 100-235.

[6] The Active Directory feature allows the operating system to manage access to system resources and users with more granularity, or a greater degree of specificity. Access to particular system resources can be granted or denied to smaller, more exclusive groupings of users, or even individual users where before they were managed on the basis of larger, less specific groupings.

STANDARD APPROACH TO APPLICATION DEVELOPMENT

SSA does not require legacy or new applications to be changed or developed to appropriately use newer security capabilities. Currently, the Office of Telecommunications and Systems Operations (OTSO) maintains and enforces a standardized process that ensures its applications are compatible with the security potential of newer operating systems. Generally, applications developed by non-headquarters components do not follow the same development process as OTSO's. There is no Agency-wide entity to ensure that standards are met. Without enforcing Agency-wide standards, some SSA applications are developed that are incapable of taking advantage of the high security configuration settings available in newer operating systems.

There is nothing to prevent new application programs that require either "work-arounds," or holes in the security templates, from being developed and installed on SSA's network structure. As a result, template adaptations may prevent the use of "high security" configuration settings available in the Agency's newer operating systems.

INTEGRATION AND ENVIRONMENTAL TESTING

IE testing is used to ensure that new software can effectively be incorporated into the current operating environment. IE testing serves to identify system incompatibilities before they are put into production. Some Agency components create network software applications that avoid IE testing and still run in the network environment. Without testing, SSA has no assurance that network applications adhere to software development guidelines established to ensure compatibility with accepted security standards.

Developers did not apply OTSO's IE testing procedures for all application programs that run under the network security structure. In some cases, non-headquarters applications did not require this testing.

In the future, SSA should use IE testing to help avoid incompatibilities when implementing new systems and should expand its use to all applications in its network environment. IE testing, if complete and extensive, could also have detected the incompatibilities between Windows 2000 and legacy applications that were discovered only on implementation. Detecting incompatibilities in a controlled, confined testing environment, rather than in production, minimizes the risk of exploitation or corruption of SSA's information resources.

CONCLUSIONS and RECOMMENDATIONS

SSA continues to migrate its network environment from one based on the Microsoft Windows NT operating system to one based on the newer Microsoft operating systems, Windows 2003 and Windows XP.

Each of the conversions involved, from Windows NT to Windows 2000 and from Windows 2000 to Windows 2003/XP, has increased network environment security over the level of security that preceded it. The problems the Agency encountered during these conversions, did however, prevent network security from reaching the full potential available in its newer operating systems.

We recommend SSA:

1. Require new application programs installed on SSA's network structure be developed to operate under the high security configuration settings originally intended for SSA's network environment.

2. Require, where possible, applications carried over from older operating system environments be replaced or modified when incompatible with newer, more stringent security configurations.

3. Require network applications to undergo adequate IE testing to meet security requirements under operating systems using high security configuration settings.

AGENCY COMMENTS AND OIG RESPONSE

In response to our draft report, SSA agreed with all three recommendations and plans to implement the recommended changes. SSA will continue to work to ensure that new and existing applications are tested and secured prior to implementation, and are compliant with best practices described under Microsoft's Designed for Windows XP Logo Program. SSA also plans to modify or replace applications as necessary to adopt them to newer operating systems with higher security configurations.

Patrick P. O'Carroll, Jr.

Appendices

Acronyms

IE	Integration and Environmental
OMB	Office of Management and Budget
OTSO	Office of Telecommunications and Systems Operations
SSA	Social Security Administration

Agency Comments

SOCIAL SECURITY

MEMORANDUM 33175-24-1100

Date: September 3, 2004 Refer To: S1J-3

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

From: Larry W. Dye /s/
Chief of Staff

Subject: Office of the Inspector General (OIG) Draft Report, "The Impact on Network Security of the Social Security Administration's Operating Systems' Conversions" (A-14-04-24019)—INFORMATION

We appreciate OIG's efforts in conducting this review. Our comments on the draft report are attached.

If you have any questions, you may contact Candace Skurnik, Director of the Audit Management and Liaison Staff, at extension 54636.

Attachment

COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL'S (OIG) DRAFT REPORT, "THE IMPACT ON NETWORK SECURITY OF THE SOCIAL SECURITY ADMINISTRATION'S OPERATING SYSTEMS' CONVERSIONS" (A-14-04-24019)

Thank you for the opportunity to review and provide comments on this report. The Social Security Administration (SSA) continues to maintain a secure information systems environment as we convert to use newer operating systems with more stringent security configurations. Our commitment to achieving maximum security in this area is evidenced by our decision, made in the absence of relevant Government standards, to develop our security template by adapting the most secure available template (the "Gold Standard Template") to the SSA network environment.

Recommendation 1

Require that new application programs installed on SSA's network structure be developed to operate under the high security configuration settings originally intended for SSA's network environment.

Comment

We agree. New applications are required to meet high security standards set by the Agency. Specifically, we require that newly developed applications be developed using the best practices described under Microsoft's Designed for Windows XP Logo Program, and that appropriate testing be performed to ensure new applications are compliant.

Recommendation 2

Require that, where possible, applications carried over from older operating system environments be replaced or modified when incompatible with newer, more stringent security configurations.

Comment

We agree. We will make modifications to or replace applications as necessary to maintain a high security environment when using such applications with newer operating systems with higher security configurations. When making decisions about modifying or replacing existing applications, we will balance the risks, costs, and benefits, as well as consider the remaining system life of such applications.

Recommendation 3

Require network applications to undergo adequate Integration and Environmental (IE) testing to meet security requirements under operating systems using high security configuration settings.

Comment

We agree. SSA system application developers are required to follow an application development process which includes IE testing. We continue to work aggressively to ensure all applications are appropriately tested and secured prior to implementation, irrespective of the network environment on which they are intended to be used.

OIG Contacts and Staff Acknowledgments

OIG Contacts

Kitt Winter, Director, Data Analysis and Technical Audit Division
(410) 965-9702

Patrick Kennedy, Audit Manager, Mainframe Controls and Advanced Techniques
(410) 965-9724

Acknowledgments

In addition to those named above:

Gregory P. Hungerman, Senior Auditor

Annette DeRito, Writer/Editor

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-14-04-24019.

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 Executive Operations (OEO). 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 Executive Operations

OEO supports OIG by providing information resource management and systems security. OEO also coordinates OIG's budget, procurement, telecommunications, facilities, and human resources. In addition, OEO 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.