Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

Audit Report

Legacy Systems Modernization and Movement to Cloud Services

142312 September 2024

Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date: September 26, 2024 **Refer to:** 142312

To: Martin O’Malley
Commissioner

From: Michelle L. Anderson /s/
Assistant Inspector General for Audit
as Acting Inspector General

Subject: Legacy Systems Modernization and Movement to Cloud Services

Attached is Ernst & Young LLP’s (Ernst & Young) final audit report. Ernst & Young met with Social Security Administration staff and management throughout the audit period and reviewed evidence the Agency provided. Ernst & Young conducted its performance audit in accordance with generally accepted government auditing standards. Those standards require that Ernst & Young plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for its findings and conclusions based on the audit objectives. We monitored Ernst & Young’s performance audit by:

- reviewing Ernst & Young’s approach and planning;
- evaluating Ernst & Young personnel’s qualifications and independence;
- monitoring Ernst & Young’s progress;
- examining Ernst & Young’s documentation and deliverables to ensure they complied with our requirements;
- coordinating the issuance of Ernst & Young’s results; and
- performing other procedures as deemed necessary.

Ernst & Young is responsible for the attached auditor’s report and the conclusions expressed therein. We were responsible for technical and administrative oversight regarding Ernst & Young’s performance under the contract terms. We did not conduct our review under generally accepted government auditing standards. Our review was not intended to enable us to express, and, accordingly, we do not express, an opinion about legacy systems modernization and movement to cloud services. However, our monitoring review, as qualified above, disclosed no instances where Ernst & Young did not comply with applicable auditing standards.

If you wish to discuss the final report, please call me or have your staff contact Jeffrey Brown, Deputy Assistant Inspector General for Audit.

Attachment

Legacy Systems Modernization and Movement to Cloud Services
142312

September 2024 **Office of Audit Report Summary**

Objective

To determine the extent to which (1) the Social Security Administration (SSA) had improved its cyber-security posture by defining and implementing plans to modernize or replace and retire its legacy information technology (IT) systems and (2) SSA's efforts and plans to move to cloud services are consistent with Federal guidance.

Background

In October 2017, SSA initiated a 5-year IT modernization plan to replace its core systems, reduce IT and other operating costs, and re-engineer business processes. SSA is developing its next modernization plan, the *Digital Modernization Strategy*.

In addition, SSA established the Benefits Modernization Program Management Office to retire core legacy systems and implement modern claims intake and adjudication software.

Under a contract the Office of Audit monitored, Ernst & Young LLP (Ernst & Young), an independent certified public accounting firm, conducted this audit.

Results

Ernst & Young concluded SSA's modernization program was not effectively designed or, in some instances, SSA had not implemented or complied with its own policies, procedures, and practices to fully address Federal requirements. Ernst & Young found SSA:

- did not have an approved strategy or guidance for defining and implementing plans to modernize, replace, or retire its legacy IT systems;
- had not developed a sufficient process that enables the creation of a comprehensive strategy to identify and track legacy systems;
- in some instances, had not maintained modernization planning and execution as well as cost documentation for sampled system transition projects; and
- had not determined whether cost and return on investment goals were being realized in some instances.

Recommendations

Ernst & Young made eight recommendations that, if implemented, could reduce the risks to the confidentiality, integrity, and availability of the Agency systems and data as well as improve its IT investment management.

Agency Comments

SSA agreed with Ernst & Young's recommendations.

Social Security Administration

Legacy Systems Modernization and Movement to Cloud Services

September 25, 2024

EY

Building a better working world

Report of Independent Auditors on Legacy Systems Modernization and Movement to Cloud Services as of 30 June 2024, based on a Performance Audit Conducted in Accordance with Government Auditing Standards

To: Martin O'Malley
Deputy Commissioner

Re: Legacy Systems Modernization and Movement to Cloud Services – Final Report

Objective

We have conducted a performance audit of SSA's Legacy Systems Modernization and Movement to Cloud Services as of June 30, 2024, with the objective of determining the extent to which (1) the Social Security Administration (SSA) has improved its cyber-security posture by defining and implementing plans to modernize or replace and retire its legacy information technology (IT) systems; and (2) SSA's current efforts and plans to move to cloud services are consistent with Federal guidance.

Background

In conjunction the Social Security Administration (SSA) Financial Statement and Federal Information Security Modernization Act of 2014[1] (FISMA) performance audits, we conducted this performance audit in accordance with generally accepted *Government Auditing Standards*. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. The nature, timing, and extent of the procedures selected depend on our judgment. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

SSA's management is responsible for defining the policies, procedures, and processes supporting the implementation of SSA's modernization programs. We evaluated the implementation of SSA's modernization program in accordance with specified areas outlined in our Statement of Work[2] (SOW)'s Planned Scope and Methodology section. These specified areas were mapped to the National Institute of Standards and Technology Special Publication (NIST) Cybersecurity Framework (CSF) Version 1.1 dated April 16, 2018[3].

This performance audit did not constitute an audit of financial statements in accordance with auditing standards generally accepted in the United States of America or *Government Auditing Standards.*

[1] *Federal Information Security Modernization Act of 2014,* Pub. L. No. 113-283, § 2, 128 Stat. 3073, 3075-3078 (2014).
[2] Contract Number: GS-00F-290CA, Task Order Number 28321323FDX030009.
[3] National Institute of Standards and Technology (2018) The NIST Cybersecurity Framework (CSF) 1.1. (National Institute of Standards and Technology, Gaithersburg, MD), https://doi.org/10.6028/NIST.CSWP.04162018 (https://www.nist.gov/cyberframework).

Findings, Conclusions and Recommendations

Based on the procedures performed, SSA's modernization program was not effectively designed or, in some instances, SSA had not implemented policies, procedures, and practices to fully address requirements outlined in OMB Circular A-130 *Managing Information as a Strategic Resource*, OMB Circular A-11 *Preparation, Submission, and Execution of the Budget,* OMB Capital Programming Guide: Supplement to Circular A-11, OMB Federal Cloud Computing Strategy, and OMB M-18-12 *Implementation of the Modernizing Government Technology Act* and related NIST guidance.[4] Specifically,

- for procedural findings, we noted SSA (1) does not have an approved comprehensive strategy or guidance for defining and implementing plans to modernize or replace/retire their legacy IT Systems, and (2) had not developed a sufficient process for identifying and tracking legacy systems that enables the creation of a comprehensive strategy.
- for practice-related findings, we noted, in some instances, SSA had not (1) maintained modernization planning/execution and cost documentation for sampled system transition projects, and (2) determined whether cost and return on investment goals were being realized.

We have included additional details related to these four (4) findings and eight (8) recommendations in Section 2 of this report.

Management's responses to our findings and recommendations were incorporated into Section 2 of our report and included in Appendix C of this report. Management did not have any disagreements with our recommendations.

This report is intended solely for the information and use of SSA, SSA Office of the Inspector General (OIG), and the appropriate committees of Congress. This report is not intended to be and should not be used by anyone other than the specified parties above.

Ernst + Young LLP

September 25, 2024

[4] For related NIST guidance, refer to each finding.

Table of Contents

Section 1
Background

1 Section 1: Background

1.1 Introduction

We conducted a performance audit of SSA's Legacy Systems Modernization and Movement to Cloud Services as of June 30, 2024. The objective of the audit was to determine the extent to which (1) the Social Security Administration (SSA) has improved its cyber-security posture by defining and implementing plans to modernize or replace and retire its legacy information technology (IT) systems; and (2) SSA's current efforts and plans to move to cloud services are consistent with Federal guidance. To accomplish this objective, we evaluated SSA modernization program in accordance with specified areas mapped NIST Cybersecurity Framework (CSF) Version 1.1, dated April 2018[5]:

- Identify:
  - Governance: Determine if modernization strategies adequately define modernization and cloud execution plans, funding sources/associated costs, and benefits from the associated progress.
  - Risk Management Strategy: Determine if management has implemented risk management controls over legacy systems.

Our methodology is described in Appendix A of this report. Appendix B specifies the criteria the modernization program was evaluated against.

1.2 Background

The Federal Information Security Modernization Act (FISMA) of 2014 (Public Law 113-283)[6] requires that senior agency officials provide information security for the information and information systems that support the operations and assets under its control, including assessing the risk and magnitude of the harm that could result from unauthorized access, use, disclosure, disruption, modification or destruction of such information or information systems.

Legacy Systems Modernization Overview

In 2021, the Government Accountability Office (GAO) testified that ". . . [g]iven the age of the hardware and software in legacy systems, the systems' criticality to agency missions, and the security risks posed by operating aging systems, it is imperative that agencies carefully plan for their successful modernization."[7] The risks of operating legacy systems include:

- Lack of vendor support for hardware or software;
- Operating systems with known vulnerabilities;
- Decreasing availability of individuals with proper skill sets; and

[5] NIST Framework for Improving Critical Infrastructure Cybersecurity v1.1 (https://www.nist.gov/cyberframework).
[6] *Federal Information Security Modernization Act of 2014,* Pub. L. No. 113-283, § 2, 128 Stat. 3073, 3075-3078 (December 18, 2014).
[7] Government Accountability Office (GAO), *Information Technology, Agencies Need to Develop and Implement Modernization Plans for Critical Legacy Systems*, p. 10 (April 27, 2021).

- Rising procurement and operating costs.[8]

According to GAO, government and industry best practices include documenting legacy system modernization plans that include: (1) milestones to complete the modernization; (2) a description of the work necessary to modernize the legacy system; and (3) details regarding the disposition of the legacy system.[9]

Cloud computing has increasingly become part of agencies' modernization efforts. The Office of Management and Budget (OMB) established a Federal Cloud Computing Strategy to accelerate agency adoption of cloud-based solutions. The strategy includes three key pillars—security, procurement, and workforce—to help ensure IT modernization provides the public improved return on investment, enhanced security, and higher quality services.[10]

In October 2017, SSA initiated a five (5) year IT modernization plan to replace its core systems, reduce IT and other operating costs, and re-engineer business processes[11]. The plan included efforts to eliminate legacy systems and expand the use of cloud platforms. GAO reviewed SSA's plan relative to a specific legacy system and found the plan did not include milestones for the entire effort and did not include considerations for the disposition of legacy system components after the modernization initiatives are completed. GAO indicated modernization efforts without complete modernization plans will increase the likelihood of cost overruns, schedule delays, and project failure[12].

As the Agency carried out its modernization activities, it received additional input from public and private technology experts, frontline employees, and the public at large. The COVID-19 pandemic underscored the need for SSA to pivot to additional online, remote service, and self-service options. As a result, the Agency updated its IT modernization plan in June 2020[13]. The updated plan continued, enhanced, added, and paused various modernization investments.

SSA is developing its next modernization plan, entitled the Digital Modernization Strategy. In addition, the Agency established the Benefits Modernization Program Management Office to ensure SSA is working more efficiently to modernize benefits systems—retiring core legacy systems and implementing modern claims intake and adjudication software.

National Institute of Standards and Technology (NIST) Cybersecurity Framework (The Framework)

In April 2018, NIST updated the Framework to version 1.1. The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The Framework consists of three parts:

[8] GAO, *Information Technology, Agencies Need to Develop and Implement Modernization Plans for Critical Legacy Systems,* (April 27, 2021)

[9] GAO, *Information Technology: IRS Needs to Complete Modernization Plans and Fully Address Cloud Computing Requirements*, pp. 7 and 8 (January 2023).

[10] Office of Management and Budget (OMB), *Federal Cloud Computing Strategy, From Cloud First to Cloud Smart*, p. 3 (2019)

[11] SSA, *IT Modernization Plan: A Business and IT Journey*, p. iii, ssa.gov (October 2017).

[12] GAO, *Information Technology, Agencies Need to Develop and Implement Modernization Plans for Critical Legacy Systems,* pp. 11 and 13 (April 27, 2021).

[13] SSA, *Service Modernization: IT Modernization Plan, 2020 Update*, (June 2020).

1. Framework Core – a set of cybersecurity activities, outcomes, and informative references that are common across sectors and critical infrastructure. Elements of the Core provide detailed guidance for developing individual organizational Profiles.
2. Implementation Tiers – the Tiers provide a mechanism for organizations to view and understand the characteristics of its approach to managing cybersecurity risk, which will help in prioritizing and achieving cybersecurity objectives.
3. Framework Profiles – through use of Profiles, the Framework will help an organization to align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerances, and resources.

Additionally, the Framework is divided into five functions: Identify, Protect, Detect, Respond, and Recover. These five functions are designed to be implemented in a continuous cycle of improvement, allowing SSA to adapt to evolving cybersecurity threats and challenges.

Section 2
Conclusion and Recommendations

2 Section 2: Conclusions

2.1 Conclusion

Based on the procedures performed, SSA's modernization program was not effectively designed or, in some instances, SSA had not implemented or complied with its own policies, procedures, and practices to fully address requirements outlined in OMB Circular A-130 *Managing Information as a Strategic Resource*[14], OMB Circular A-11 *Preparation, Submission, and Execution of the Budget*[15], OMB Capital Programming Guide: Supplement to Circular A-11[16], OMB Federal Cloud Computing Strategy[17], and OMB M-18-12 *Implementation of the Modernizing Government Technology Act*[18] and related NIST guidance.[19]

Specifically, for procedural findings, we noted SSA:

(1) does not have an approved comprehensive strategy or guidance for defining and implementing plans to modernize or replace/retire their legacy IT Systems, and
(2) had not developed a sufficient process for identifying and tracking legacy systems that enables the creation of a comprehensive strategy.

Specifically, for practice-related findings, we noted, in some instances, SSA had not

(1) maintained modernization planning/execution and cost documentation for sampled system transition projects, and
(2) determined whether cost and return on investment goals were being realized.

Based on the testing results, some of SSA's controls are not designed and operating as intended. We outline the findings and recommendations in this report that, if implemented, could reduce the risks to the confidentiality, integrity, and availability of the Agency systems and data and its IT investment management.

2.2 Identify

The Framework defines the goal of the Identify Function is to develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

[14] OMB, Circular No. A-130, *Managing Information as a Strategic Resource* (July 2016).
[15] OMB, Circular No. A-11, *Preparation, Submissions, and Execution of the Budget* (July 2024).
[16] OMB, Capital Programming Guide, Supplement to Circular No. A-11, Version 3.1 (July 2024)
[17] OMB, *Federal Cloud Computing Strategy* (June 2019).
[18] OMB Memorandum M-18-12, *Implementation of the Modernizing Government Technology Act* (March 2018)
[19] For related NIST guidance, refer to each finding.

To evaluate the Identify Function, we evaluated SSA's modernization strategies to determine whether SSA had:

- adequately define modernization and cloud execution plans, funding sources/associated costs, and benefits from the associated progress; and
- implemented risk management controls over legacy systems.

During our testing, we identified processes implemented to support the Identify Function within the framework. However, we identified findings and their recommendations with portions of objectives related to the Identify Function.

Governance-related Findings

Procedure Finding #1 – Management does not have an approved strategy or guidance for defining and implementing plans to modernize or replace/retire their legacy IT Systems.

Criteria

OMB Circular A-11, Section 240.18, notes[20]: "Once an agency's Performance Plan is established, agencies should ensure that the enterprise architecture planning documents are consistent with achieving the agency goals and objectives. This will require direct alignment of the capital and enterprise architecture planning efforts to meet the strategic objectives and performance goals in agency strategic and annual performance plans, to the extent that information technology resources are critical to the achievement of those objectives and goals."

OMB Circular A-130 outlines the following Agency requirements for planning documents, Information Resource Management Strategic (IRM) Plans, and Enterprise Architectures[21]:

- *Section 5 Policy, Section a: Planning and Budgeting, Number 1) Strategic Planning,* notes: "In support of agency missions and business needs, and as part of the agency's overall strategic and performance planning processes, agencies shall develop and maintain an IRM Strategic Plan that describes the agency's technology and information resources goals, including but not limited to, the processes described in this Circular. The IRM Strategic Plan must support the goals of the Agency Strategic Plan required by the Government Performance and Results Modernization Act of 2010 (GPRA Modernization Act). The IRM Strategic Plan shall demonstrate how the technology and information resources goals map to the agency's mission and organizational priorities. These goals shall be specific, verifiable, and measurable, so that progress against these goals can be tracked. The agency shall review its IRM Strategic Plan annually alongside the Annual Performance Plan reviews, required by the GPRA Modernization Act, to determine if there are any performance gaps or changes to mission needs, priorities, or goals. As part of the planning and maintenance of an effective information strategy, agencies shall meet the following requirements, in addition to all other requirements in this Circular:
  a) Inventories – Agencies shall:
     i. Maintain an inventory of the agency's major information systems, information

[20] Office of Management and Budget, Executive Office of the President (OMB), Circular No. A-11, *Preparation, Submissions, and Execution of the Budget* (July 2024).
[21] OMB, Circular No. A-130, *Managing Information as a Strategic Resource* (July 2016).

holdings, and dissemination products, at the level of detail that OMB and the agency determine is most appropriate for overseeing and managing the information resources; and

ii. Maintain an inventory of the agency's information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII to allow the agency to regularly review its PII and ensure, to the extent reasonably practicable, that such PII is accurate, relevant, timely, and complete; and to allow the agency to reduce its PII to the minimum necessary for the proper performance of authorized agency functions.

b) Information Management – Agencies shall:

i. Continually facilitate adoption of new and emerging technologies, and regularly assess the following throughout the life of each information system: the inventory of the physical and software assets associated with the system; the maintainability and sustainability of the information resources and infrastructure supporting the system; and actively determine when significant upgrades, replacements, or disposition is required to effectively support agency missions or business functions and adequately protect agency assets; and

ii. Ensure the terms and conditions of contracts and other agreements involving the processing, storage, access to, transmission, and disposition of Federal information are linked to the IRM strategic plan goals and are sufficient to enable agencies to meet their policy and legal requirements.

c) Risk Management – Agencies shall:

i. Consider information security, privacy, records management, public transparency, and supply chain security issues for all resource planning and management activities throughout the system development life cycle so that risks are appropriately managed.

ii. Develop plan, in consultation with Chief Information Officers (CIOs), Senior Agency Officials for Records Management (SAORMs), and Senior Agency Officials for Privacy (SAOPs), for information systems and components that cannot be appropriately protected or secured and ensure that such systems are given a high priority for upgrade, replacement, or retirement.

iii. Regularly review and address risk regarding processes, people, and technology; and

iv. Consult National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) and NIST Special Publications (SPs) (e.g., 500, 800, and 1800 series guidelines)."

- *Section 5 Policy, Section a: Planning and Budgeting, Number 2) Enterprise Architecture,* requires that Agencies: "…develop an enterprise architecture (EA) that describes the baseline architecture, target architecture, and a transition plan to get to the target architecture. The agency's EA shall align to their IRM Strategic Plan. The EA should incorporate agency plans for significant upgrades, replacements, and disposition of information systems when the systems can no longer effectively support missions or business functions. The EA should align business and technology resources to achieve strategic outcomes. The process of describing the current and future state of the agency and laying out a plan for transitioning from the current state to the desired future state,

> helps agencies to eliminate waste and duplication, increase shared services, close performance gaps, and promote engagement among Government, industry, and citizens."

Paperwork Reduction Act of 1995, Section 3506 Federal Agency Responsibilities, notes[22]: "With respect to general information resources management, each agency shall— (1) manage information resources to — (A) reduce information collection burdens on the public; (B) increase program efficiency and effectiveness; and (C) improve the integrity, quality, and utility of information to all users within and outside the agency, including capabilities for ensuring dissemination of public information, public access to government information, and protections for privacy and security; (2) in accordance with guidance by the Director, develop and maintain a strategic information resources management plan that shall describe how information resources management activities help accomplish agency missions; (3) develop and maintain an ongoing process to— (A) ensure that information resources management operations and decisions are integrated with organizational planning, budget, financial management, human resources management, and program decisions; (B) in cooperation with the agency Chief Financial Officer (or comparable official), develop a full and accurate accounting of information technology expenditures, related expenses, and results; and (C) establish goals for improving information resources management's contribution to program productivity, efficiency, and effectiveness, methods for measuring progress towards those goals, and clear roles and responsibilities for achieving those goals; (5) in consultation with the Director and the Director of the Office of Personnel Management, conduct formal training programs to educate agency program and management officials about information resources management."

Clinger Cohen Act of 1996 - Section 11315 Agency Chief Information Officer, notes[23]:

> (b) "General Responsibilities - The Chief Information Officer of an executive agency is responsible for - (3) promoting the effective and efficient design and operation of all major information resources management processes for the executive agency, including improvements to work processes of the executive agency."
> (c) "Duties and Qualifications.- The Chief Information Officer of an agency listed in section 901 (b) of title 31— (1) has information resources management duties as that official's primary duty; (2) monitors the performance of information technology programs of the agency, evaluates the performance of those programs on the basis of the applicable performance measurements, and advises the head of the agency regarding whether to continue, modify, or terminate a program or project; and (3) annually, as part of the strategic planning and performance evaluation process required (subject to section 1117 of title 31) under section 306 of title 5 and sections 1105 (a)(28), 1115–1117, and 9703 (as added by section 5(a) of the Government Performance and Results Act of 1993 (Public Law 103–62, 107 Stat. 289)) of title 31- (A) assesses the requirements established for agency personnel regarding knowledge and skill in information resources management and the adequacy of those requirements for facilitating the achievement of the performance goals established for information resources management; (B) assesses the extent to which the positions and personnel at the executive level of the agency and the positions and personnel at management level of the agency below the executive level

[22] Paperwork Reduction Act of 1995, Pub. L. No. 104-13,44 U.S.C § 3506 (May 22, 1995)
[23] Clinger-Cohen Act of 1996 Pub. L. No. 104-106, 40 U.S.C § 11315 (February 10, 1996).

meet those requirements; (C) develops strategies and specific plans for hiring, training, and professional development to rectify any deficiency in meeting those requirements; and (D) reports to the head of the agency on the progress made in improving information resources management capability."

Condition

SSA does not have an approved comprehensive strategy or guidance for defining and implementing plans to modernize or replace/retire their legacy IT Systems. Specifically, we noted the following:

- SSA does not have a comprehensive plan in place for modernizing its legacy systems.
- Enterprise Architecture planning documents have not been updated since 2019.
- SSA has not maintained an updated Information Resource Management (IRM) Strategic Plan. In addition, SSA did not update their IRM Strategic Plan alongside the Annual Performance Plan as required by OMB Circular A-130, nor does it provide guidance on legacy system modernizations.

Cause

1. SSA has undergone leadership changes which has prevented a comprehensive modernization plan from being approved, finalized and implemented. SSA is working with the Commissioner to ensure the next modernization plan, the Digital Modernization Strategy (DMS), reflects the Agency's strategic direction for FY2024-2027, prior to its approval and public release.
2. SSA is currently working with the new Chief Information Officer and business stakeholders to develop updated Enterprise Architecture planning documents that incorporate their new target architecture.
3. SSA has not maintained an updated IRM Strategic Plan. In addition, SSA did not update their IRM Strategic Plan alongside the Annual Performance Plan as required by OMB Circular A-130, nor does it provide guidance on legacy system modernizations.

Effect

1. Without a comprehensive plan, the Agency is at risk of inadequately planned updates which can result in an IT environment with incompatible systems or one that does not account for future growth. Further, lack of a structured approach to addressing modernization leaves Agency systems open to vulnerabilities, increasing the likelihood of security breaches.
2. Failure to maintain an updated Enterprise Architecture and related plans hinders SSA's ability to understand and modernize their IT landscape, which can lead to a misalignment between Agency strategic goals and result in difficulties adapting to changing business needs and security requirements.
3. Failure to maintain an updated Information Resource Management (IRM) Plan hinders SSA's ability to manage information resources effectively to support the Agency's mission/goals. An outdated IRM Strategic Plan that does not align with current Agency mission/goals might result in inefficient allocation of resources, potentially leaving

critical systems unprotected and vulnerable to attacks.

Recommendations

1. Ensure timely steps are taken to approve and implement a modernization strategy which covers SSA modernization efforts and comprehensively addresses legacy system risks for the upcoming years.
2. Ensure timely steps are taken to develop Enterprise Architecture planning documents that directly align with strategic objectives and performance goals noted in the Agency's strategic and Annual Performance Plans.
3. Review the IRM Strategic Plan annually and ensure it supports the goals of the Agency Strategic Plan, as required by the Government Performance and Results Modernization Act of 2010, OMB Circular A-130, the Paperwork Reduction Act of 1995, and the Clinger-Cohen Act of 1996.

Management Response: Management concurred with our recommendations.

Practice Finding #1 – Management did not maintain modernization planning/execution and cost documentation for sampled system transition projects.

Criteria

OMB Circular A-130 outlines the following Agency requirements for planning documents and investment management[24]:

- *Section 5 Policy, Section a: Planning and Budgeting, Number 1) Strategic Planning, Section c) Risk Management,* requires that Agencies “Develop plan, in consultation with Chief Information Officers (CIOs), Senior Agency Officials for Records Management (SAORMs), and Senior Agency Officials for Privacy (SAOPs), for information systems and components that cannot be appropriately protected or secured and ensure that such systems are given a high priority for upgrade, replacement, or retirement.”
- *Section 5 Policy, Section d: IT Investment Management, Number 3) Investment Planning and Control,* notes “Agencies are responsible for establishing a decision-making process that shall cover the life of each information system and include explicit criteria for analyzing the projected and actual costs, benefits, and risks, including information security and privacy risks, associated with the IT investments. Agencies shall designate IT investments according to relevant statutes, regulations, and guidance in OMB Circular A-11, and execute processes commensurate with the size, scope, duration, and delivery risk of the investment. The IT investment processes shall encompass planning, budgeting, procurement, management, and assessment. For further guidance related to investment planning, refer to OMB Circular A-11, including the Capital Programming Guide.”

Condition

SSA’s process for tracking costs and system transitions was limited to only a subset of modernization projects. Specifically, for a selection of legacy system transition projects tested,

[24] OMB, Circular No. A-130, *Managing Information as a Strategic Resource* (July 2016).

SSA could not provide the following documentation in relation to IT modernization efforts:

- Modernization planning and execution documents, detailing considerations for the system's disposition.
- Legacy operational costs, projected cost savings, and expected increase in efficiencies, to prioritize modernization efforts maximizing impact of organizational investment.

Cause
Due to inadequate record-keeping practices and lack of management oversight, SSA was unable to provide evidence demonstrating the decommissioning or disposition of these systems, including cost-savings or efficiencies gained from decommissioning.

Effect
Without appropriate planning/oversight and record-keeping systems for costs and other data for legacy system modernization in accordance with Federal mandates, the Agency is at risk of experiencing potential cost overruns, delays in project timelines, inadequate resource allocation, and an increased likelihood of project failure.

Recommendation
Management should ensure legacy system modernization plans include a detailed description of the work needed for modernization, considerations for the disposition of the system, and tracking cost data that covers all aspects of the project.

Management Response: Management concurred with our recommendation.

Identify-related Findings
Procedure Finding #2 – Processes for identifying and tracking legacy systems does not enable the creation of a comprehensive strategy to improve its cybersecurity posture by implementing plans to modernize or replace and retire its legacy IT systems.

Criteria
The NIST, Security Control PM-5 element requires Agencies to "Develop and update an inventory of organizational systems.[25]"

Further, OMB Circular A-130 outlines the following Agency requirements for system inventories and risk assessments[26]:

- *Section 5 Policy, Section a. Planning and Budgeting, Number 1) Strategic Planning, Section a) Inventories,* notes: "Agencies shall: i. Maintain an inventory[27] of the agency's

[25] NIST SP 800 53, Security and Privacy Controls for Information Systems and Organizations.
[26] OMB, Circular No. A-130, *Managing Information as a Strategic Resource* (July 2016).
[27] "The inventory of agency information resources shall include an enterprise-wide data inventory that accounts for data used in the agency's information systems." OMB, Circular No. A-130, *Managing Information as a Strategic Resource* (July 2016).

major information systems[28], information holdings, and dissemination products, at the level of detail that OMB and the agency determine is most appropriate for overseeing and managing the information resources; ii. Maintain an inventory of the agency's information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII to allow the agency to regularly review its PII and ensure, to the extent reasonably practicable, that such PII is accurate, relevant, timely, and complete; and to allow the agency to reduce its PII to the minimum necessary for the proper performance of authorized agency functions.[29]"

- *Section 5 Policy, Section a: Planning and Budgeting, Number 1) Strategic Planning, Section b) Information Management, i*, notes: "Agencies shall: Continually facilitate adoption of new and emerging technologies, and regularly assess the following throughout the life of each information system: the inventory of the physical and software assets associated with the system; the maintainability and sustainability of the information resources and infrastructure supporting the system; and actively determine when significant upgrades, replacements, or disposition is required to effectively support agency missions or business functions and adequately protect agency assets."
- *Section 5 Policy, Section a: Planning and Budgeting, Number 1) Strategic Planning, Section c) Risk Management, ii*, notes: "Agencies Shall: Develop plan, in consultation with Chief Information Officers (CIOs), Senior Agency Officials for Records Management (SAORMs), and Senior Agency Officials for Privacy (SAOPs), for information systems and components that cannot be appropriately protected or secured and ensure that such systems are given a high priority for upgrade, replacement, or retirement[30]"
- *Section 5 Policy, Section a: Planning and Budgeting, Number 1) Strategic Planning, Section c) Risk Management*, iii, notes: "Agencies Shall: Regularly review and address risk regarding processes, people, and technology."

Condition

SSA's current process for identifying and tracking legacy systems does not enable the creation of a comprehensive strategy to improve its cybersecurity posture by implementing plans to modernize or replace and retire its legacy IT systems. Specifically, the following was identified:

- SSA did not perform IT Investment risk management activities for legacy systems as required by OMB Circular A-130.
- SSA provided inventory includes 819 systems listed as legacy, 415 systems as modern, and 22 unknowns. However, EY determined classification information to be not reliable because a system listed as modern may have legacy and modernized components. In

[28] "The inventory of major information systems is required in accordance with 44 U.S.C. § 3505(c). All information systems are subject to the requirements of the Federal Information Security Modernization Act (44 U.S.C. Chapter 35) whether or not they are designated as a major information system." OMB, Circular No. A-130, *Managing Information as a Strategic Resource* (July 2016)

[29] "Agencies shall ensure that physical devices, software applications, hardware platforms, and systems within the organization are inventoried initially when obtained and updated on an ongoing basis." OMB, Circular No. A-130, Managing Information as a Strategic Resource (July 2016).

[30] "Includes hardware, software, or firmware components no longer supported by developers, vendors, or manufacturers through the availability of software patches, firmware updates, replacement parts, and maintenance contracts." OMB, Circular No. A-130, Managing Information as a Strategic Resource (July 2016).

addition, SSA was able to provide only a list of 67 business applications that retired/replaced systems/applications. Therefore, SSA's system inventory does not contain sufficient information for effective information resources management related to legacy systems. Further , SSA's inventory did not track risk information such as system criticality, security risks due to age of systems, age of the systems and whether hardware is out of warranty.

Cause

1. Evidence of conducting risk management activities for legacy systems was not provided.
2. EY noted the Agency maintains an inventory of business applications along with their respective technology stacks. However, the current inventory does not encompass data elements specifically related to application changes as a result of modernization efforts, such as retiring or replacing applications.

Effect

1. By not performing legacy system risk assessments, SSA is limiting their ability to track and mitigate risks associated with outdated or unsupported applications, as well as impair SSA’s ability to design information security controls to detect, prevent, and mitigate threats to the Agency's environment. Further, this can hinder SSA's ability to prioritize modernization efforts effectively based on legacy risks, leading to increased exposure to vulnerabilities.
2. Failure to maintain an accurate inventory of applications that have undergone modernization efforts can lead to difficulties in effectively managing and prioritizing modernization efforts, potentially resulting in misused or obsolete resources, or delays in achieving modernization goals.

Recommendations

1. Regularly perform risk assessments for legacy systems, as required by OMB Circular A-130, Section 5(a)(1)(b)(i) and (c)(ii). Performing regular risk assessments will help management identify information systems and components that cannot be appropriately protected or secured, helping to ensure that such systems that may be costly or difficult to maintain, are given high priority for upgrade, replacement, or retirement.
2. Continue to refine its inventory of business applications to ensure data elements specifically related to changes, such as retiring or replacing applications, resulting from modernization efforts are tracked/flagged appropriately.

Management Response: Management concurred with our recommendations.

Practice Finding #2 – Efforts and plans to modernize legacy systems and migrate to cloud services were insufficient to determine whether cost and return on investment goals were being realized.

Criteria

OMB Circular A-130 outlines the following Agency requirements for Investment Planning and Budgeting[31]:

- *Section 5 Policy, Section d: IT Investment Management, Number 3) Investment Planning and Control*, notes "Agencies are responsible for establishing a decision-making process that shall cover the life of each information system and include explicit criteria for analyzing the projected and actual costs, benefits, and risks, including information security and privacy risks, associated with the IT investments. Agencies shall designate IT investments according to relevant statutes, regulations, and guidance in OMB Circular A-11, and execute processes commensurate with the size, scope, duration, and delivery risk of the investment. The IT investment processes shall encompass planning, budgeting, procurement, management, and assessment. For further guidance related to investment planning, refer to OMB Circular A-11, including the Capital Programming Guide. At a minimum, agencies shall ensure that:
    a) All IT resources (see "Information Technology Resources" definition) are included in IT investment planning documents or artifacts.
    b) Decisions related to major IT investments are supported by business cases with appropriate evidence.
    c) IT investments implement an agile development approach, as appropriate.
    d) IT investments support and enable core mission and operational functions and processes related to the agency's missions and business requirements.
    e) IT capital investment plans and budgetary requests are reviewed to ensure that Government-wide requirements, as well as any associated costs, are explicitly identified and included, with respect to any IT resources. This includes IT resources that will be used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII; and
    f) Decisions to improve, enhance, or modernize existing IT investments or to develop new IT investments are made only after conducting an alternatives analysis that includes both government-provided (internal, interagency, and intra-agency where applicable) and commercially available options, and the option representing the best value to the Government has been selected."
- *Section 5 Policy, Section a: Planning and Budgeting, Number 3) Planning, Programming, and Budgeting,* states: "Identifying gaps between planned and actual cost, schedule, and performance goals for IT investments and developing a corrective action plan to close such gaps."
- *Section 5 Policy, Section b: Governance,* states: "2c) Appropriate measurements are used to evaluate the cost, schedule, and overall performance variances of IT projects across the portfolio; 2d) There are agency-wide policies and procedures for conducting IT investment reviews, operational analyses, or other applicable performance reviews to

[31] OMB, Circular No. A-130, *Managing Information as a Strategic Resource* (July 2016).

> evaluate IT resources, including projects in development and ongoing activities; 6) It shall be the CIO and program managers' shared responsibility to ensure that legacy and ongoing IT investments are appropriately delivering customer value and meeting the business objectives of the agency and the programs that support the agency."

SSA IT Guide to Capital Planning and Investment Control, Section 11.5 - Post Implementation Reviews (PIR), notes[32]: "The Office of Management and Budget requires SSA to assess IT investment performance. SSA defines that assessment as completing Post-Implementation Reviews (PIRs) of implemented or cancelled IT investments, examining the degree to which each IT investment realized its planned mission impact, business assumptions, cost, return on investment & value, risk, schedule, enterprise architecture goals, and functional requirements. The purpose of an investment PIR is to track and measure the impact and outcomes of implemented or cancelled IT Investments to ensure they meet the program mission and/or obtain lessons learned. Within the CPIC process, PIRs become a driving force for assessing IT investments agency-wide to improve related strategies, operations, value levers, and key outcomes. Footnote 14: SSA performs PIRs projects once they are complete. In addition, SSA conducts PIRs on investments for a more holistic approach.

A PIR is performed on IT systems typically 6-18 months after they are fully deployed. This review is important not only to determine the future viability of the IT Investment[33], but also to assist IT managers in improving IT proposal business case requirements to better inform future IT selection decision-making. The PIR, in essence, closes the loop regarding the IT CPIC process by facilitating feedback on an investment's overall processes and its refinement. The need to evaluate an investment's ability to effectively meet the organization's mission needs, both functionally and economically, does not end at investment deployment. Rather, it is a continuous process to ensure that the investment still supports both the users' and mission needs."

Further, *OMB's Capital Programming Guide: Supplement to Circular A-11, Version 3.1, Section III Management In-Use, III.3) Operational Analysis Process and Outcome, 3.2) Post-Implementation Review (PIR)*, states[34]: "The Post-Implementation Review (PIR) usually occurs either after a system has been in operation for about six months or immediately following investment termination. The review should provide a baseline to decide whether to continue the system without adjustment, to modify the system to improve performance or, if necessary, to consider alternatives to the implemented system. Some common elements reviewed during the PIR include:

- Mission alignment
- IT architecture including security and internal controls.
- Performance measures.
- Project management.
- Customer acceptance.

[32] SSA, SSA IT Guide to Capital Planning and Investment Control (May 31, 2023).

[33] "SSA performs PIRs projects once they are complete. In addition, SSA conducts PIRs on investments for a more holistic approach." SSA's IT Capital Planning Investment Control Guide (May 29, 2023).

[34] OMB Circular No. A-11, *Preparation, Submissions, and Execution of the Budget* (July 2024).

- Business process support.
- Financial performance.
- Return on investment.
- Risk management.
- Gaps or deficiencies in the process used to develop and implement the initiative.
- Best practices that can be applied to other investments or the capital planning process.

To minimize inadequate returns on low value or high-cost IT investments, the agency will conduct periodic reviews of operational systems to determine whether they should be retained, modified, replaced, or retired. With the emergence of new business and process requirements, and new and updated technology, systems should be assessed to determine the extent to which they continue to support the agency's mission and business objectives."

Condition
SSA's current efforts and plans to modernize legacy systems and migrate to cloud services were insufficient to determine whether cost and return on investment goals were being realized. Specifically, we noted:

- SSA currently does not have a process in place to distinguish funding related to modernization efforts from general investments.
- SSA does not utilize cost data for data driven decisions to help aid with prioritization of modernization efforts based on savings to the organization or expected Return on Investments.
- The current PIR process being followed at SSA does not match the defined PIR timeframe listed within SSA's IT Capital Planning and Investment Control Guide (CPIC, last updated on May 31, 2023). Additionally, SSA could not provide information that the Agency achieved the goals and benefits of the sampled IT modernization projects consistent with an established modernization program.

Cause

1. SSA's difficulty in distinguishing modernization funding and considering costs from a risk perspective are due to the lack of both an approved modernization plan and conducted risk assessments.
2. SSA indicated that post implementation reviews are carried after the conclusion of an investment for a sample of investments, which is not consistent with their recently updated CPIC Guide. In addition, although SSA identified performance metrics, they did not track metrics for the majority of the sampled systems.

Effect

1. Without proper management of investment costs and funding sources, the Agency is at risk of potential financial waste, misallocation of resources, or might face challenges with tracking the effectiveness of investments.
2. Lack of performing a post implementation review will result in SSA not being aware of whether projects are achieving their mission, goals, and benefits.

Recommendations

1. Implement cost monitoring mechanisms to help with the tracking and management costs related to modernization. Additionally, management should conduct cost analyses for modernization projects, considering cost from a risk perspective.
2. Regularly perform PIRs on all IT investments.

Management Response: Management concurred with our recommendations.

Section 3
Appendices

Appendix A
Audit Scope and Methodology

3 Section 3: Appendices

3.1 Appendix A: Audit Scope and Methodology

Scope

The purpose of the Legacy Systems Modernization and Movement to Cloud Services Performance Audit is to determine the extent to which (1) the Social Security Administration (SSA) has improved its cyber-security posture by defining and implementing plans to modernize or replace and retire its legacy information technology (IT) systems; and (2) SSA's current efforts and plans to move to cloud services are consistent with Federal guidance.

Methodology

We evaluated SSA's implementation of its modernization program in accordance with specified areas mapped to the NIST Framework, Version 1.1 dated April 16, 2018.

- Identify:
  - Governance: Determine if modernization strategies adequately define modernization and cloud execution plans, funding sources/associated costs, and benefits from the associated progress.
  - Risk Management Strategy: Determine if management has implemented risk management controls over legacy systems.

We considered criteria outlined in OMB Circular A-130 *Managing Information as a Strategic Resource*, OMB Circular A-11 *Preparation, Submission, and Execution of the Budget,* OMB Federal Cloud Computing Strategy, and OMB M-18-12 *Implementation of the Modernizing Government Technology Act* to determine the effectiveness of SSA's Modernization programs.

To accomplish our objectives, we performed the procedures outlined in our Statement of Work[35] (SOW)'s Planned Scope and Methodology section. Additionally, we conducted walkthroughs with SSA personnel to understand the agency's modernization program and identified relevant policies, procedures, and processes.

We conducted these procedures in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[35] Contract Number: GS-00F-290CA, Task Order Number 28321323FDX030009

Appendix B
Federal Requirements and Guidance

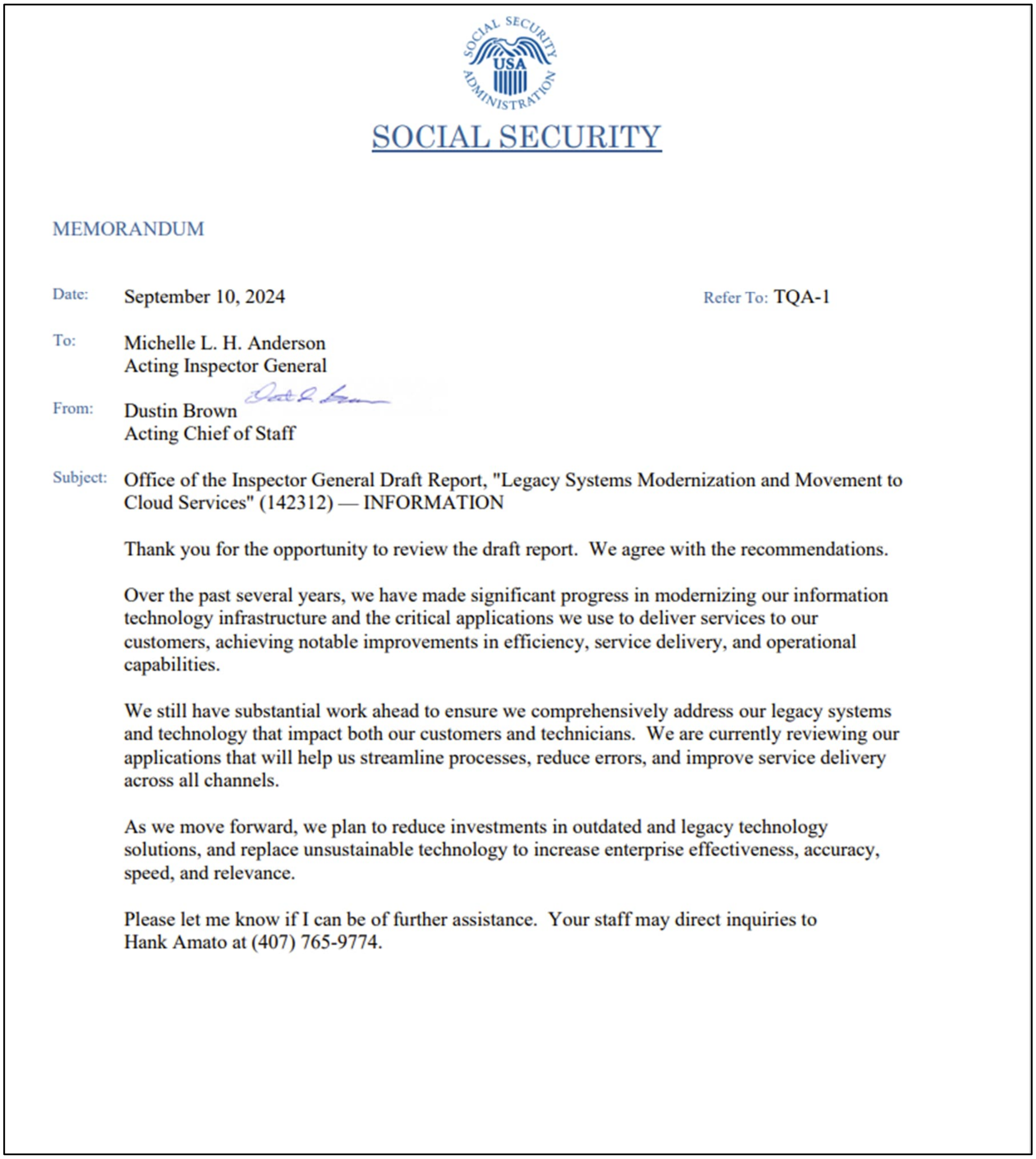
3.2 Appendix B: Federal Requirements and Guidance

The purpose of the Legacy Systems Modernization and Movement to Cloud Services Performance Audit is to determine the extent to which (1) the Social Security Administration (SSA) has improved its cyber-security posture by defining and implementing plans to modernize or replace and retire its legacy information technology (IT) systems; and (2) SSA's current efforts and plans to move to cloud services are consistent with Federal guidance. Below is a list of criteria used to conduct the Legacy Systems Modernization and Movement to Cloud Services performance audit:

- OMB Circular A-130 Managing Information as a Strategic Resource
- OMB Circular A-11 Preparation, Submission, and Execution of the Budget
- OMB Federal Cloud Computing Strategy
- OMB M-18-12 Implementation of the Modernizing Government Technology Act
- GAO Government Auditing Standards (GAS), Chapters 8 (Fieldwork Standards for Performance Audits) and Chapter 9 (Reporting Standards for Performance Audits)
- SSA Guidance/Policies
- Standards and guidelines issued by National Institute of Standards and Technology, including Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations, revision No. 5
- National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1
- Capital Programming Guide, Supplement to Circular No. A-11, Version 3.1.

Appendix C
Management's Response to Findings and Recommendations

3.3 Appendix C: Management's Response to Findings and Recommendations



SOCIAL SECURITY

MEMORANDUM

Date: September 10, 2024 Refer To: TQA-1

To: Michelle L. H. Anderson
Acting Inspector General

From: Dustin Brown
Acting Chief of Staff

Subject: Office of the Inspector General Draft Report, "Legacy Systems Modernization and Movement to Cloud Services" (142312) — INFORMATION

Thank you for the opportunity to review the draft report. We agree with the recommendations.

Over the past several years, we have made significant progress in modernizing our information technology infrastructure and the critical applications we use to deliver services to our customers, achieving notable improvements in efficiency, service delivery, and operational capabilities.

We still have substantial work ahead to ensure we comprehensively address our legacy systems and technology that impact both our customers and technicians. We are currently reviewing our applications that will help us streamline processes, reduce errors, and improve service delivery across all channels.

As we move forward, we plan to reduce investments in outdated and legacy technology solutions, and replace unsustainable technology to increase enterprise effectiveness, accuracy, speed, and relevance.

Please let me know if I can be of further assistance. Your staff may direct inquiries to Hank Amato at (407) 765-9774.

EY | Assurance | Tax | Transactions | Consulting

About EY

EY is a global leader in assurance, tax, transaction and consulting services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.