SOCIAL SECURITY

MEMORANDUM

Date: September 30, 2009 Refer To:

To: The Commissioner

From: Inspector General

Subject: Implementation of the Social Security Administration's Security Performance Metrics Program (A-14-10-11002)

The attached final quick response evaluation presents the results of our review. Our objective was to determine whether the Social Security Administration's plan for developing and implementing a security performance metrics program met applicable Federal requirements. Specifically, this evaluation focused on the concerns expressed by the Information Security and Privacy Advisory Board and to ensure the Agency complied with the National Institute of Standards and Technology Special Publication 800-55 Revision 1, *Performance Measurement Guide for Information Security*. This evaluation provides a status of the Agency's efforts to implement a security performance metrics program.

If you wish to discuss the final report, please call me or have your staff contact Steven L. Schaeffer, Assistant Inspector General for Audit, at (410) 965-9700.

Patrick P. O'Carroll, Jr.

Attachment

QUICK RESPONSE EVALUATION

Implementation of the Social Security Administration's Security Performance Metrics Program

A-14-10-11002

September 2009

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.

Background

OBJECTIVE

Our objective was to determine whether the Social Security Administration's (SSA) plan for developing and implementing a security performance metrics program met applicable Federal requirements. We performed this evaluation to address information security concerns expressed by the Information Security and Privacy Advisory Board (ISPAB)[1,2] and to ensure the Agency complied with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-55 Revision 1, *Performance Measurement Guide for Information Security*.[3] This evaluation provides a status of the Agency's efforts to implement a security performance metrics program.

BACKGROUND

Information security performance metrics are used to facilitate decision making and improve performance and accountability through the collection, analysis, and reporting of relevant performance-related data. The purpose of measuring performance is to review the status of monitored activities and facilitate improvement in those activities by applying corrective actions based on observed measurements. Implementing a security metrics program will

- increase accountability for information security performance,
- improve effectiveness of information security activities,
- demonstrate compliance with laws, rules and regulations, and
- provide quantifiable inputs for resource allocation decisions.

Performance metrics are used to weigh the benefits of adding security measures to information technology (IT) operations and measure the benefits of using these security metrics against costs. The requirement to measure information security performance is driven by regulatory, financial, and organizational reasons. A number of existing laws, rules, and regulations cite information performance measurements in general, and information security performance measurements in particular, as a requirement. These laws include the:

---

[1] ISPAB was originally created by the *Computer Security Act of 1987* (Pub. L. No. 100-235) as the Computer System Security and Privacy Advisory Board. As a result of the *Federal Information Security Management Act* (FISMA) (Pub. L. No. 107-347, Title III, Section 301 *et seq*.), the Board's name was changed, and its mandate was amended.

[2] FISMA letter to the Honorable Jim Nussle, Director, Office of Management and Budget (OMB), July 2008. The letter offers ISPAB recommendations to OMB regarding the efficacy of security metrics in regard to FISMA.

[3] NIST SP 800-55 Revision 1, *Performance Measurement Guide for Information Security*, issued July 2008.

- *Clinger-Cohen Act,*[4]
- *Government Performance and Results Act,*[5]
- *Government Paperwork Elimination Act,*[6] *and*
- FISMA.[7]

On July 30, 2008, the Chairman of ISPAB sent a letter to OMB expressing concerns with current information security performance metrics developed under FISMA. ISPAB[8] questioned whether the metrics OMB developed under FISMA improved an agency's understanding and performance of Government security. The letter stated that this process has become overly compliance-driven, with excessive attention to fulfilling certification and accreditation and other reporting processes at the expense of implementing, measuring, and improving true security performance.[9,10] As Congress considers new legislation, one of the fundamental questions is whether FISMA's current reporting requirements address the core question of whether agencies' security measures are functioning as intended.[11]

ISPAB recognized three worthwhile metrics within the FISMA framework that include traditional perimeter measures, such as intrusion detection,[12] penetration

[4] Pub. L. No. 104-106.

[5] Pub. L. No. 103-62.

[6] Pub. L. No. 105-277.

[7] Pub. L. No. 107-347. FISMA requires that Federal agencies develop, document, and implement an agency-wide information security program to provide security for the information and information systems that support the agencies' operations and assets.

[8] See Footnote 2.

[9] See Footnote 2.

[10] NIST SP 37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, pp. 1-2, May 2004. Certification is the comprehensive assessment of the management, operational, and technical security controls in an information system. Accreditation is the official management decision to authorize operation of an information system.

[11] Senator Tom Carper introduced U.S. Senate bill S.921-*United States Information and Communications Enhancement Act of 2009* in April 2009 that would replace FISMA.

[12] NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems*, section ES-1, February 2007. Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing these events for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices.

testing,[13] and incident response.[14] However, when these measures are obtained, the results are lost amidst the need to comply with the much larger set of FISMA-related procedural requirements.[15]

ISPAB made the following recommendations to improve the security performance metrics program for Government agencies.

- Revise FISMA and related policy and guidance so that agency and contract incentives will be able to measure and improve actual security.

- OMB and NIST should work with agency Chief Information Officers (CIO) to review FISMA policy and guidance to measure and improve security in a way that manages risk and improves program delivery and eliminates all unnecessary provisions.

- FISMA policy and guidance should encourage accountability for security program performance, through rewards for progress and the maintenance of strong outcomes and consequences for deterioration and continued weak outcomes.

- OMB should issue metrics required under a new FISMA program as early as possible in the fiscal year for which reports are made, rather than late in the year given the many competing demands of the IT calendar.

- OMB should use its procurement policy authority to amend the Federal Acquisition Regulation, so agency contract documents give industry incentives to build and measure security based on the same outcome-oriented metrics that are issued in OMB policy and NIST guidance and so that these documents do not require unrelated security activities that add costs and burden to the acquisition system with little or no return.

In July 2008, NIST SP 800-55 Revision 1[16] was issued to assist Government agencies in the development, selection, and implementation of measures that indicate the effectiveness of information security controls.

---

[13] NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*, section 5-2, September 2008. Penetration testing is security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network.

[14] Appendix III OMB Circular No. A-130, *Security of Federal Automated Information Resources,* p. 3. Incident response capability ensures that there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats.

[15] Letter to the Honorable Jim Nussle, Director, OMB, July 2008. The letter offers ISPAB recommendations to OMB regarding the efficacy of security metrics in regard to FISMA.

[16] NIST SP 800-55 Revision 1, *Performance Measurement Guide for Information Security*, p. 1.

In October 2008, we issued a memorandum to SSA advising it of ISPAB's concerns. In response to our memorandum, SSA indicated its intentions to comply with any Federal legislation or directives related to incorporation of performance-based metrics. Given that SSA had not implemented its plan for an information security performance metrics program at that time, we were unable to determine whether the Agency's plans met applicable Federal requirements. As a result, we performed this evaluation to provide a status of the Agency's efforts to develop a performance metrics program for its security program as well as offer suggestions for management's consideration.

Results of Review

Based on our evaluation, SSA has been responsive to our October 2008 memorandum and has initiated steps to develop a security performance metrics program. The proposed program builds on the Agency's current reporting model, which is based on FISMA, and envisions including critical elements for a more comprehensive program.

SSA's Current Information Security Performance Metric Reporting Efforts

Under FISMA, the Agency conducts numerous activities to safeguard information systems and resources. SSA conducts rigorous testing of its information systems and oversees a range of ongoing IT security activities. Some of the security activities conducted and performance metrics reported under the FISMA framework are as follows.

- The Agency performs annual testing of its IT security controls as part of the annual FISMA evaluation and financial statement audit. Identified weaknesses and deficiencies are documented using an automated tracking tool. A Plan of Action and Milestones (POA&M) is created to resolve each identified weakness. POA&Ms are reported annually and quarterly to OMB.
- All SSA personnel receive IT security awareness training annually. The Office of the CIO (OCIO) works with the Office of Acquisition and Grants to provide awareness training to SSA contractor personnel. Additionally, SSA provides specialized training to personnel with significant security responsibilities.
- SSA conducts extensive network and workstation scanning to identify and remove harmful or inappropriate files that violate the Agency's IT security policies.

In addition to FISMA-related activities, SSA complied with other directives issued by OMB designed to strengthen Federal IT security programs. One example of a current OMB initiative is the Federal Desktop Core Configuration (FDCC). FDCC provides secure common desktop configurations for Windows operating systems.

SSA's Efforts to Develop a More Comprehensive Security Performance Metrics Program

In October 2008, we issued a memorandum to SSA emphasizing the importance of implementing a Security Performance Metrics program (see Appendix B). The memorandum highlighted the Government information security community's focus on information security performance metrics—specifically the concerns raised by ISPAB. The ISPAB memorandum indicated that outcome-based metrics would make Agency security performance more transparent and emphasized a concrete set of actions needed to improve the underlying trustworthiness of IT systems. Furthermore, these metrics should (1) focus on risk management rather than compliance; (2) have a line-of-

sight to business and program goals rather than IT operations; and (3) assess both status and progress.

SSA began developing a more comprehensive information security metrics program. One of the key steps taken by SSA to assist with developing the Agency's security metrics program was OCIO's Office of Information Technology and Security Policy (OITSP) awarding a task order to Booz Allen Hamilton (BAH) in September 2008.[17] BAH's objective was to analyze and define IT security measures and metrics to track the impact of risk management goals through identifying practices that evaluate security control implementation across the SSA enterprise. BAH was to develop a handbook recommending program and system-level metrics for SSA that would establish a direct relationship between the corresponding program activities and SSA's mission.

In April 2009, BAH provided the Agency with an initial draft handbook. This document analyzed SSA's current IT security metrics collection processes and summarized the actions needed for mature metrics development including steps needed to create and maintain an IT security performance measurement program. SSA expressed concerns with the initial handbook because BAH included highly sensitive information that described the Agency's current collecting and reporting processes for its security metrics that feed into four quarterly reports.[18] SSA requested BAH remove this information from the handbook to protect the privacy of the Agency's data collecting and reporting processes.

In May 2009, BAH submitted a revised draft handbook. This handbook provided the information security management and system owners with the necessary guidance and procedures for collecting, storing, analyzing, and reporting on security performance metrics. Both draft handbooks outlined steps to implement a metrics program as defined by the NIST SP 800-55 Revision 1*, Security Metrics Guide for Information Technology Systems.* The Agency was generally satisfied with BAH's revised draft handbook. In July 2009, the OCIO provided the BAH draft handbook to other Agency components for comment. SSA plans to implement the BAH final handbook in January 2010. The Agency stated that the security performance metrics handbook will serve as the OCIO's synthesis of the high level requirements from NIST and OMB for the Agency. Given the existing disparate and federated management structure of SSA, the security performance metrics handbook is not intended to provide specific granular and authoritative metrics for the Agency. SSA intentionally designed the security performance metrics handbook to provide examples of best practices for component

[17] The BAH task order was $107,000 under contract #SS-00-08-40029 Task # 4.

[18] *SSA Security Metrics Handbook*, Version 1.1, April 6, 2009, section 3, p. 9. OITSP currently collects security metrics from a variety of sources to prepare the four quarterly reports. These sources include FISMA Information Security, POA&Ms, Senior Agency Officials for Privacy, and OIG reports. Additionally, OITSP provides input to SSA's e-Government IT Security Scorecard and completes the data collection and updates on a quarterly basis as required by OMB guidelines. These quarterly activities help prepare the program office for the larger Agency annual report which feeds directly into SSA's IT Security report card grade for the year. This grade, provided by Congress, evaluates the implementation of FISMA requirements.

reconciliation and application. SSA needs to ensure that guidance and direction is sufficient to provide for the development and implementation of a sound information security performance metrics program.

Further Development of SSA's Information Security Metrics Program

An information security measures development process consists of two major activities:

- Identification and definition of the current information security program.

- Development and selection of specific measures to gauge the implementation, effectiveness, efficiency, and impact of the security controls.[19]

While we acknowledge the Agency's proactive efforts by having BAH develop the performance metrics handbook, we encourage SSA to ensure that the above activities are an integral part of its process for developing IT security performance metrics.

SSA acknowledged the need and has taken steps to develop a more comprehensive information security metrics performance program. However, based on our analysis, we identified some areas the Agency should be aware of as it moves forward in developing a more comprehensive security metrics program.

NIST recommended specific steps in the measure development process.[20] The measure development process involves the following phases.

- Stakeholder interest identification.
- Goals and objective definition.
- Information security policy, guidelines, and procedures review.
- Information security program implementation review.
- Measures development and selection.

SSA identified relevant stakeholders for the information security performance metrics program. However, NIST states an organization should identify and document system security performance goals and objectives.[21] SSA provided the Agency's strategic goals and objectives in both BAH drafts; however, the information security goals and objectives were missing in the latest version of the BAH draft handbook. Information security performance goals state the desired results of an information program

[19] NIST SP 800-55 Revision 1, *Performance Measurement Guide for Information Security*, Sec. 5, p. 25.

[20] NIST SP 800-55 Revision 1, *Performance Measurement Guide for Information Security,* Sec. 5, p. 25. The measures development process identifies relevant stakeholders and their interests in information security measurement.

[21] NIST SP 800-55 Revision 1, *Performance Measurement Guide for Information Security*, Sec. 5, p. 26. The measures development process identifies and documents information system security performance goals and objectives that would guide security control implementation for the information security program of a specific information system.

implementation, such as, “All employees should receive adequate information security awareness training.” Information security performance objectives enable accomplishment of goals by identifying practices defined by information security policies and procedures that direct consistent implementation of security controls across the organization. NIST guidance provides an example of how an agency would link its security performance goal, “*All new employees receive new employee training”* to the supporting objectives. The example shows that employee training objectives include providing a summary of the Rules of Behavior as well as a summary of, and a reference to, the organization’s information security policies and procedures. In reviewing the BAH draft handbook, the information security goals were identified; however, the specific corresponding objectives and means of accomplishing the information security goals were not yet fully defined.

In the measures development process, an organization should establish policies, guidelines, and procedures that focus on organization-specific information security practices. SSA is in the process of establishing the policies, guidelines, and procedures for its information security metrics program with an anticipated completion date of January 2010. These policies, guidelines, and procedures should describe how implementing security controls, requirements, and techniques lead to accomplishing information security performance goals and objectives.

Further, SSA has not yet fully addressed the information security program implementation review and measures development and selection steps. The information security program implementation review allows an organization to identify any existing measures and data repositories that can be used to derive measures data for review. In the measures development and selection stage, measures dealing with overall information security program performance should:

- Be mapped to information security goals and objectives that may encompass performance of information security across the spectrum of security controls.
- Use data describing the information security program performance to generate required measures.

We believe SSA should define the goals and objectives for the information security performance metrics program according to NIST guidance. The Agency should also address the remaining three steps of the measures development process as outlined in the NIST guidance.

Moreover, we recently issued an audit report that identified weaknesses that could prevent an information security performance metrics program from being successful.[22] This report found that SSA's OCIO did not have sufficient delegated authority or resources to carry out its security monitoring and management responsibilities. SSA should consider these issues while developing and implementing its information security performance metrics program and address them, as appropriate.

Measuring performance provides managers crucial information on which to base their organizational and management decisions. The development and implementation of a sound information security performance metrics program will help ensure SSA moves toward a reliable, resilient, and trustworthy digital infrastructure for the future.[23]

SSA's information security performance metrics program should focus on measuring the impact and effectiveness of the Agency's security activities and not merely compliance with laws and regulations. Otherwise, SSA will not be able to determine whether its information security program is truly meeting its goals and protecting the Agency's sensitive information.

[22] OIG, *Follow up: Social Security Administration's Computer Security Program Compliance* (A-14-09-19048), issued September 24, 2009.

[23] Melissa Hathaway, former Cybersecurity Chief at the National Security Council, *Cyberspace Policy Review*, May 2009.

Matters for Consideration

SSA has one of the largest data processing centers with one of the largest collections of sensitive personal data. The Agency's computer system contains demographic, earnings, and/or benefit information for almost every American. Moreover, SSA processes over 75 million business transactions per day and stores almost 250 million medical records, while adding 2 million more each week. Its databases contain sensitive personally identifiable information, such as names, addresses, dates of birth, mothers' maiden names, earnings, and Social Security numbers. In addition, the Agency exchanges over 1 billion data files annually with Government and business entities for benefit management and homeland security purposes.

Given the characteristics and volume of data maintained and processed at SSA, it is imperative that SSA bolster its existing information security program by establishing metrics to reflect how well the program is achieving its goal of information protection. The need for making information security and its performance metrics a priority is supported by a recent Presidential report, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. In this report, the Special Advisor to the President on Cybersecurity recommended designating cybersecurity as one of the President's key management priorities and establishing performance metrics.[24] The report provides a formal cybersecurity program assessment framework where "Departments and agencies would define their specific program's purpose and goal as well as identify metrics to evaluate whether the goals are achieved."

The attacks on networks in the United States and South Korea are the latest reminder that cybersecurity remains a pressing concern in the 21st century. As evidenced by a recent report, a series of cyber attacks on computer networks in South Korea and the United States was apparently the work of North Korean hackers. While SSA may not have been a direct target of the North Korean attacks, these attacks demonstrate the need to continuously monitor information systems and the security measures employed to protect them.

Pending legislation introduced by Senator Tom Carper[25] further emphasizes performance metrics as a requirement that involves continuous testing and evaluation of information security controls and techniques to ensure they are effectively implemented.

[24] Melissa Hathaway, former Cybersecurity Chief at the National Security Council, *Cyberspace Policy Review*, May 2009. The President directed a 60-day, comprehensive, "clean-slate" review to assess U.S. policies and structures for cybersecurity. Cybersecurity policy includes strategy, policy, and standards regarding the security of and operations in cyberspace. It encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.

[25] S.921, *United States Information and Communications Enhancement Act of 2009*, April 28, 2009.

It is apparent that the concerns of the Administration and Congress are well-justified. To that end, their recommendations, as well as those of the ISPAB for establishing effective information security performance metrics, offer a viable approach to track the success of an information security program.

We understand the Agency is developing an information security performance metric program. We acknowledge and applaud SSA for being proactive in developing this program despite it not being required or mandated at this time. We encourage the Agency to continue these efforts and take the necessary steps to fully develop its information security performance metrics program.

Based on the present state of the Agency's metrics program, we are providing the following comments for SSA's consideration. These comments should help improve the Agency's program and ensure its success. To assist SSA in addressing applicable Federal guidance for developing and implementing an Agency-wide security metrics program, we believe SSA should consider:

- Ensuring the information security metrics performance program addresses the key measure development steps recommended by NIST.
- Implementing an Agency-wide information security performance metrics program in accordance with applicable Federal guidance. These measures should be measurable, repeatable, consistent, and actionable.

Appendices

Acronyms

BAH	Booz Allen Hamilton
CIO	Chief Information Officer
FDCC	Federal Desktop Core Configuration
FISMA	Federal Information Security Management Act
FY	Fiscal Year
ICE	Information and Communication Enhancement
ISPAB	Information Security and Privacy Advisory Board
IT	Information Technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OITSP	Office of Information Technology and Security Policy
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
Pub. L. No.	Public Law Number
SP	Special Publication
SSA	Social Security Administration

Efficacy of Federal Security Performance Metrics Memorandum

SOCIAL SECURITY

MEMORANDUM

Date: October 20, 2008 Refer To:

To: See Below

From: Assistant Inspector General
for Audit

Subject: Efficacy of Federal Security Performance Metrics

The Government information security community has focused increased attention on information security performance metrics. In July 2008, the Information Security and Privacy Advisory Board (ISPAB) issued a memorandum to the Office of Management and Budget (OMB) on the efficacy of Government security performance metrics and the extent to which such metrics can serve as indicators of security progress and performance (see Attachment A). Specifically, ISPAB questions whether metrics developed by OMB under the *Federal Information Security Management Act of 2002* (FISMA) are focused in a way that improves agency understanding and performance of Government security. Almost concurrent with ISPAB's memorandum to OMB was the National Institute of Standards and Technology's issuance of the Performance Measurement Guide for Information Security (Special Publication 800-55 Revision 1). This guidance is recognized as a means to assist in the development, selection and implementation of measures to indicate the effectiveness of information security controls.

The ISPAB found that the FISMA metrics program did enhance focus on agency security activities. However, this process has become overly compliance-driven, with excessive attention to fulfilling Certification & Accreditation and other reporting processes at the expense of implementing, measuring, and improving true security performance. According to ISPAB, agencies often write or contract for security documentation after the fact, rather than embedding and documenting security during development to ensure security is built into programs and systems up front.

ISPAB recommended that FISMA, and related policy and guidance, be revised to establish agency and contract incentives to measure and improve security. Outcome-based metrics would make agency security performance more transparent and point to a concrete set of actions related to improvements, as well as increase underlying trustworthiness of information technology systems. These metrics should (1) focus on risk management, rather than compliance; (2) have a line of sight to business and program goals rather than information technology operations; and (3) assess both status and progress.

In light of the increased focus on information security performance metrics and the Government Accountability Office's current audit of SSA's information security metrics, we are providing copies of the ISPAB memorandum (Attachment A) and the National Institute of Standards and Technology publication (Attachment B http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf). To help us understand the Agency's posture for responding to these items, we are requesting that you provide a written response indicating whether SSA has already taken or plans to take action to address the concerns identified in the ISPAB memorandum. We would appreciate a response by November 7, 2008. If you have any questions or concerns please contact me at 410-965-9700.

/s/
Steven L. Schaeffer

Addressees:
Deputy Commissioner for Budget, Finance and Management
Chief Information Officer
Deputy Commissioner for Systems

Attachments

cc:
P. O'Carroll
D. Foster
J. Kissko

INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987
[Amended by the Federal Information Security Management Act of 2002]

JUL 30 2008

The Honorable Jim Nussle
Director
The Office of Management and Budget
725 17th Street, NW
Washington, DC 20503

Dear Mr. Nussle:

I am writing to you as the Chair of the Information Security and Privacy Advisory Board (ISPAB). The ISPAB was originally created by the Computer Security Act of 1987 (P.L. 100-35) as the Computer System Security and Privacy Advisory Board, and amended by Public Law 107-347, The E-Government Act of 2002, Title III, The Federal Information Security Management Act (FISMA) of 2002. One of the statutory objectives of the Board is to identify emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy.

On numerous occasions over the past several years, the Board has heard briefings and held discussions around the issue of whether metrics developed under FISMA to assess Government security have, in fact, focused attention in a way that improves agency understanding and performance in this critically important area. At the same time, the Board has also examined the efficacy of security metrics more generally, and the extent to which such metrics can serve as indicators of security progress and performance.

As a result of these inquiries, the Board has found that the FISMA metrics program served a salutary role in enhancing focus on agency security activities. The metrics program, as implemented by OMB policy and NIST guidance, has led to:

- Increased attention throughout the government on the importance of good process;
- Better documentation of security programs and plans;
- Improvements in third-party reviews, especially from the Inspector General community; and
- Stronger engagement by senior management in security activities

The record set before the Board, however, points to a less positive yet highly significant finding as well. Considerable evidence demonstrates that FISMA implementation has become overly compliance-driven, with excessive attention to the fulfilling Certification & Accreditation (C&A) and other reporting processes at the expense of implementing, measuring, and improving true security performance. Agency senior executives, CIOs, CISOs, and even Inspectors General have all indicated that voluminous documentation requirements have gone too far, leading to a check-the-box set of activities that reward compliance rather than outcomes. Private sector experts have echoed and amplified this view. Agencies often write or contract for security documentation after the fact, rather than embedding and documenting security during development to insure that security is built into programs and systems up front – an industry best practice.

The Board has identified examples of worthwhile metrics within the FISMA framework, including traditional perimeter measures like intrusion detection, penetration testing, and incident response. But even when they have been obtained, such results are lost amidst the need to comply with the much larger set of FISMA-related procedural requirements; as a result, agencies lack time and resources to develop and implement needed improvements in their security program. While a comprehensive documentation assessment approach may have had value in setting the FISMA baseline (i.e., during the first several reporting cycles), the Board believes that the benefit of measuring detailed processes has become far outweighed by the burden this places on agencies, and the opportunity cost of resources devoted to compliance rather than performance.

Accordingly, the Board recommends that FISMA and related policy and guidance be revised so that agency and contract incentives are to measure and improving actual security. We recognize that perfect security, as well as perfect security measurement, is an aspiration rather than an attainable state; indeed, the Board has heard important briefings about the limits of security measurement, and does not suggest that a sound metrics program will address all potential vulnerabilities or enable a sound response to all threats. However, an explicit, outcome-based set of metrics would make agency security performance more transparent, would point to a concrete set of actions related to improvement over time, and would increase underlying trustworthiness of and with agency IT systems. These metrics should focus on risk management, rather than compliance; should have a line of sight to business and program goals, rather than IT operations; and should assess both status and progress.

The Board holds that an improved FISMA metrics program would address management, operational, and technical controls, as outlined under current OMB policy and NIST guidance, but would neither measure nor reward process documentation. As a result, agencies could spend more time and resources understanding their actual security posture, and taking steps to improve. To accomplish this, we recommend that OMB and NIST work with agency CIOs to review FISMA policy and guidance, and eliminate all provisions not necessary to measure and improve security in a way that manages risk and improves program delivery. Metrics to eliminate might

include percent of systems C&Aed, as most systems have gone through this baseline; number of training sessions conducted, since much of this training is superficial at best; and duplication of measures between the CIO and IG.

The Board also recommends that the metrics required under a new FISMA program be issued by OMB guidance as early as possible in the fiscal year for which reports are made, rather than late in the year as has often been the case given the many competing demands of the IT calendar. The security of Federal systems has become a mission critical element in assuring good program performance; measuring the way that security enables or hinders that performance should be a systematic and continuous activity, rather than one that comes late in the year and is thus largely divorced from ongoing program operations. On a longer term basis, a revised FISMA process could mandate that OMB, NIST, and the CIOs could periodically review metrics (e.g., every 2 years), with an eye towards updating them based on perceived success. This process would create an institutional imperative for FISMA to stay current, and promote positive adaptation in a world where attacks change, defenses change, and baseline systems improve.

The Board further recommends that the OMB use its procurement policy authority to amend the Federal Acquisition Regulation (FAR), so that agency contract documents (e.g., RFPs, RFQs, contract compliance reports) incentivize industry to build and measure security based on the same outcome-oriented metrics that are issued in OMB policy and NIST guidance – and so that these documents do not require unrelated security activities that add cost and burden to the acquisition system with little or no return. The Administration has made some progress on policy in this area, and has developed related FAR clauses. However, implementation is sketchy at best; the Board's industry members echo comments we have heard from industry briefers, who contend that contracted security resources would be far better able to solve real problems if contract requirements focused on substantive rather than procedural security activities.

The Board has also heard from NIST officials about their long-term research efforts on security metrics. We commend NIST for undertaking this effort, though we have questions about its applicability to agency security programs given its emphasis on mathematical modeling. We believe that continued actions to link metrics R&D with law, policy and guidance will make the benefits of NIST activities more applicable to agency program improvement. We recommend that OMB and NIST work with interested stakeholders, including CIOs, CISOs, IGs, program officials, and private sector experts, to review and enhance the metrics program over time.

Finally, the Board recommends that FISMA policy and guidance encourage accountability for security program performance, through rewards for progress and the maintenance of strong outcomes, and consequences for deterioration and continued weak outcomes. Improving security in agencies requires more than a good set of metrics. Managing this change will need to address behaviors and the political, career executive, program management, and operational levels.

We appreciate the opportunity to offer the Board's views on this critically important issue. Please let me know if the Board can answer any questions or take additional actions to support improvements in Federal information security metrics.

Sincerely,

Daniel J. Chenok
Information Security and Privacy Advisory Board Chairman

cc: Karen Evans

Scope and Methodology

To accomplish our objective, we:

- Reviewed applicable Federal laws, directives, and other guidance, as well as industry standards and best practices.
- Obtained and reviewed the Social Security Administration's (SSA) Information Security Performance Metrics program.
- Reviewed *Federal Information Security Management Act* (FISMA) Fiscal Year 2008 guidance.
- Reviewed the Office of the Inspector General's (OIG) FY 2008 FISMA report and other relevant OIG reports.
- Interviewed personnel from SSA's Office of the Chief Information Officer.
- Reviewed documentation from other Federal agencies' information security performance metrics program.

The results of our review are based on the above information provided by SSA. We performed our review during July and August 2009 in Baltimore, Maryland. The entities reviewed were the Offices of the Chief Information Officer and Deputy Commissioner for Systems. We conducted our review in accordance with the President's Council on Integrity and Efficiency's[1] *Quality Standards for Inspections.*

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

OIG Contacts and Staff Acknowledgments

OIG Contacts

Brian Karpe, Acting Division Director, Information Technology Audit Division

Phil Rogofsky, Audit Manager

Acknowledgments

In addition to those named above:

Mary Ellen Moyer, Audit Manager

Tina Nevels, Auditor

Cheryl Dailey, Auditor

For additional copies of this report, please visit our web site at www.socialsecurity.gov/oig or contact the Office of the Inspector General's Public Affairs Staff Assistant at (410) 965-4518. Refer to Common Identification Number A-14-10-11002.

DISTRIBUTION SCHEDULE

Commissioner of Social Security

Office of Management and Budget, Income Maintenance Branch

Chairman and Ranking Member, Committee on Ways and Means

Chief of Staff, Committee on Ways and Means

Chairman and Ranking Minority Member, Subcommittee on Social Security

Majority and Minority Staff Director, Subcommittee on Social Security

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

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

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

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

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

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

Chairman and Ranking Minority Member, Committee on Finance

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

Chairman and Ranking Minority Member, Senate Special Committee on Aging

Social Security Advisory Board

Overview of the Office of the Inspector General

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

Office of Audit

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

Office of Investigations

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

Office of the Counsel to the Inspector General

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

Office of External Relations

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

Office of Technology and Resource Management

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