

**INDEPENDENT EVALUATION OF  
SBA'S INFORMATION SECURITY PROGRAM**

**REPORT NUMBER 3-37**

**SEPTEMBER 17, 2003**

**This report may contain proprietary information subject to the provisions of 18 USC 1905 and must not be released to the public or another agency without permission of the Office of Inspector General.**




**U.S. SMALL BUSINESS ADMINISTRATION  
OFFICE OF INSPECTOR GENERAL  
WASHINGTON, D.C. 20416**

**ADVISORY MEMORANDUM  
REPORT**

**Issue Date: September 17, 2003**

**Number: 3-37**

**To:** Hector V. Barreto  
Administrator

**From:**   
Robert G. Seabrooks  
Assistant Inspector General for Audit

**Subject:** Independent Evaluation of SBA's Information Security Program

The Federal Information Security Management Act (FISMA), permanently reauthorized and amended agency information security reporting requirements previously authorized under the Government Information Security Reform Act (GISRA). Like GISRA, FISMA lays out a framework for annual IT security reviews, reporting, and remediation planning. FISMA requires the Office of Inspector General (OIG) to perform an independent evaluation of the Small Business Administration's (SBA) information security program. This report presents the results of that evaluation in accordance with specific FISMA reporting instructions issued by the Office of Management and Budget (OMB).

**OBJECTIVES, SCOPE AND METHODOLOGY**

The objective of our review was to evaluate SBA's information security program in accordance with FISMA reporting requirements specified in OMB Memorandum M-03-19. We performed an independent evaluation of SBA's information security program to reach conclusions about the FISMA reporting areas. In making our evaluation, we considered prior audits related to SBA's information systems computer security program issued by our office.

Our assessment covered the 38 high-priority systems identified by SBA and its characterization of the susceptibility of those systems to unauthorized access as of August 31, 2003. As part of our evaluation, we accompanied Integrated Management Services Incorporated (IMSI), SBA's contractor, on selected reviews to identify and assess sensitive SBA systems. We interviewed SBA officials and reviewed documentation on SBA's information security program. Our evaluation was performed at SBA's headquarters office in Washington, D.C. from July 2003 through September 2003.

## OVERALL EVALUATION

Generally, SBA's information security program continues to improve for high priority financial management and general support systems. However, material weaknesses and security vulnerabilities continue to exist in: (1) computer intrusion detection and incident escalation procedures, (2) security controls in the systems development life-cycle, (3) system access controls, (3) system certification and accreditation, and (4) disaster recovery and contingency planning.

## EVALUATION RESULTS

**OMB Question A.2a. Identify the total number of programs and systems in the agency, the total number of systems and programs reviewed by the program officials and CIO's in FY03, the total number of contractor operations or facilities, and the number of contractor operations or facilities reviewed in FY03. Additionally, IG's shall also identify the total number of programs, systems, and contractor operations or facilities that they evaluated in FY03.**

Table 1.  
High Priority Systems Reviewed by OIG

| Bureau Name | FY03 Programs       |                 | FY03 Systems |                 | FY03 Contractor Operations or Facilities |                 |
|-------------|---------------------|-----------------|--------------|-----------------|--|-----------------|
|             | Total Number        | Number Reviewed | Total Number | Number Reviewed | Total Number                             | Number Reviewed |
|             | <b>Agency Total</b> | 7               | 7(1)         | 38              | 9  | 5               |

The Office of the Inspector General has overseen or performed independent audits or evaluations for this fiscal year on SBA general support systems and major applications that support SBA's program operations. These reviews or audits include:

- Monitoring of SBA's Disaster Credit Management System (OIG Draft Report)
- SBA Information System Controls for Fiscal Year 2002 (OIG Report 3-20)
- Critical Infrastructure Protection Program (OIG Report 3-03)
- SBA Acquisition, Development and Implementation of the Joint Accounting and Administrative Management System (OIG Report 3-32)

The Information System Control review was performed in accordance with the General Accounting Office (GAO) Federal Information System Controls Audit Manual. The SBA Acquisition, Development and Implementation of the Joint Accounting and Administrative Management System, and the Monitoring of SBA's Disaster Credit Management System reviews were systems development and implementation reviews utilizing Clinger-Cohen requirements and SBA's systems development requirements.

Comment 1 – SBA does not have major applications relating to all seven program areas. SBA does have general support systems such as agency-wide E-mail and SBA’s Local Area Network/Wide Area Network that support all seven program areas.

**Table 2.**  
**High-Priority Systems Reviewed by SBA**

| Bureau Name  | FY03 Programs  |                 | FY03 Systems |                 | FY03 Contractor Operations or Facilities |                 |
|--|--|-----------------|--------------|-----------------|--|-----------------|
|  | Total Number   | Number Reviewed | Total Number | Number Reviewed | Total Number                             | Number Reviewed |
| <b>Agency Total</b>  | 7  | 7               | 38           | 37              | 5  | 3               |
| <b>b. For operations and assets under their control, have agency program officials and the agency CIO used appropriate methods (e.g., audits or inspections) to ensure that contractor provided services or services provided by another agency for their program and systems are adequately secure and meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy?</b> | Yes  |                 | Yes          |                 |  |                 |
| <b>c. If yes, what methods are used? If no, please explain why.</b>  | The SBA used its certification and accreditation process, the NIST self-assessment guide and other contractor audits to evaluate whether contractor provided services or services provided by another agency were secure and meet the requirements of FISMA, OMB, NIST and SBA policy. |                 |              |                 |  |                 |
| <b>d. Did the agency use the NIST self-assessment guide to conduct its reviews?</b>  | Yes (2)  |                 | Yes (2)      |                 |  |                 |
| <b>e. If the agency did not use the NIST self-assessment guide and instead used an agency developed methodology, please confirm that all elements of the NIST guide were addressed in the agency methodology.</b>  | N/A  |                 | N/A          |                 |  |                 |
| <b>f. Provide a brief update on the agency’s work to develop an inventory of major IT systems.</b>   | (3)  |                 | (3)          |                 |  |                 |

Comment 2 – SBA’s Office of Chief Information Officer (OCIO) coordinated security self-assessments performed with the assistance of a contractor, IMSI, for all internal and contractor operated systems at SBA. These assessments followed the process and checklist found in the National Institute of Standards and Technology (NIST) Special Publication (SP) Number 800-26, “Security Self-Assessment Guide for Information Technology Systems.” OIG observed a sampling of self assessments and found the results to be reliable.

Comment 3 – SBA has identified its inventory of major IT systems. The inventory includes 38 total systems of which three are general support systems and 35 are major applications. Four of the 35 major applications are contractor provided systems and one is a contractor provided service.

**OMB Question A.3. Identify all material weaknesses in policies, procedures, or practices as identified and required to be reported under existing law in FY03. Identify the number of material weaknesses repeated from FY02, describe each material weakness, and indicate whether POA&Ms have been developed for all of the material weaknesses.**

In FY 2002, OIG reported six material weaknesses in SBA's computer security program regarding policies, procedures or practices. In FY 2003, two material weaknesses were eliminated and one material weakness was added to SBA's total. OIG eliminated two material weaknesses due to improvements in oversight of contractor operations in SBA's computer security program and the performance of security test and evaluations for seven SBA systems. OIG added one new material weakness due to a lack of adequate incorporation of security controls in the development of new systems at SBA.

**Table 3.  
Number of Material Weaknesses**

| Bureau Name  | FY03 Material Weaknesses |                                 |  | POA&Ms developed?<br>Y/N |
|--------------|--------------------------|---------------------------------|--|--------------------------|
|              | Total Number             | Total Number Repeated from FY02 | Identify and Describe Each Material Weakness |                          |
| Agency Total | 5                        | 4                               | See below.                                   | Yes                      |

The revised material weaknesses include:

- Inadequate incorporation of security controls for systems under development (new),
- Weak security controls including identification and authentication and separation of duties on individual systems,
- Incomplete planning and certification of major applications and general support systems,
- Weak intrusion detection monitoring and security incident escalation procedures, and
- Incomplete disaster recovery and contingency planning and testing.

**OMB Question A.4. Please assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestone process that meets the criteria below. Where appropriate, please include additional explanation in the column next to each criteria.**

OIG Assessment – Overall SBA has developed, implemented and managed an agency-wide POA&M process. We identified that not all SBA systems with significant weaknesses have a POA&M reported to OMB in the most recent reporting period.

We also reviewed a judgmental sample of twelve security weaknesses which had reportedly been corrected within the POA&M process. Eight security weaknesses reviewed were not corrected, even though those weaknesses were reported as being corrected by system owners. This was validated by OCIO which identified through its C&A process that reportedly corrected security weaknesses were actually not corrected by the system owner or contractor when a follow-up C&A review was performed on a contractor facility.

**Table 4**  
**SBA Plan of Action and Milestones**

|  |                 |        |
|--|-----------------|--------|
| Agency program officials develop, implement, and manage POA&Ms for every system that they own and operate (systems that support their programs) that has an IT security weakness.  |                 | No (4) |
| Agency program officials report to the CIO on a regular basis (at least quarterly) on their remediation progress.  |                 | No (5) |
| Agency CIO develops, implements, and manages POA&Ms for every system that they own and operate (systems that support their programs) that has an IT security weakness.   | Yes             |        |
| The agency CIO centrally tracks and maintains all POA&M activities on at least a quarterly basis.  | Yes             |        |
| The POA&M is the authoritative agency and IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses.   | Yes (6)         |        |
| System-level POA&Ms are tied directly to the system budget request through the IT business case as required in OMB budget guidance (Circular A-11) to tie the justification for IT security funds to the budget process.           | No (7)          |        |
| Agency IGs are an integral part of the POA&M process and have access to agency POA&Ms.   | See Comment (6) |        |
| The agency's POA&M process represents a prioritization of agency IT security weaknesses that ensures that significant IT security weaknesses are addressed in a timely manner and receive, where necessary, appropriate resources. |                 | No (8) |

Comment 4 – The contractor provided applications of Colson Services Corporation and USDA National Finance Center’s (NFC) Payroll system do not have POA&M’s. Major IT security weaknesses were identified in Colson’s most recent Risk Assessment and Security Test and Evaluation and the audit of SBA Information System Controls for Fiscal Year 2002 (OIG Report 3-20) found the USDA NFC Payroll system needed to be recognized as a major agency application.

Comment 5 – The OIG reviewed a judgmental sample of twelve security weaknesses which had reportedly been corrected within the POA&M process. Eight security weaknesses reviewed were not corrected, even though those weaknesses were reported as being corrected by system owners. This was validated by OCIO which identified through its C&A process that reportedly corrected security weaknesses were actually not corrected by the system owner or contractor when a follow-up C&A review was performed.

Comment 6 – The OIG receives and has access to the SBA POA&M as needed. However, the OIG does not use the POA&M as the authoritative tool to identify and monitor agency corrective actions for system weaknesses. The OIG does review the POA&M, but does not rely upon it exclusively as part of our audit evidence.

Comment 7 – A review of SBA’s POA&M from June 30, 2003 identified that no security weaknesses for any of SBA’s 38 individual systems or its information security program were tied to the SBA Capital Asset Plans or Exhibit 53.

Comment 8 – The SBA POA&M does not prioritize IT security weaknesses other than identify the weaknesses as “high” priority weaknesses.

**OMB Question B.1. Identify and describe any specific steps taken by the agency head to clearly and unambiguously set forth FISMA's responsibilities and authorities for the agency CIO and program officials. Specifically how are such steps implemented and enforced?**

The Administrator issued a memorandum in September 2002 which set forth duties and responsibilities for SBA program officials and the CIO under GISRA. The memorandum stated that the OCIO will continue to lead SBA's initiative to enhance the Agency's computer security program and its responsibilities. OCIO will assist program offices in fulfilling IT security responsibilities. Guidance will be provided through policy and procedural notices, and by conferring with managers on any special IT security needs in their respective areas. While the memorandum was issued for GISRA, the requirements are substantially the same as the current FISMA guidance.

Additionally, SBA Standard Operating Procedure 90 47, *Information System Security Program*, states the following responsibilities for the SBA Administrator:

The SBA Administrator is responsible for establishing a management control process to ensure that appropriate administrative, physical, and technical safeguards are incorporated into all new applications and into significant modifications to existing applications. The Administrator has delegated this responsibility to the Chief Information Officer (CIO).

**OMB Question B.2. Can a major operating component of the agency make an IT investment decision without review by and concurrence of the agency CIO?**

A major operating component of the agency cannot make a significant IT investment decision without review by and concurrence of the agency Business Technology Investment Council (BTIC). The Council is composed of senior agency executives and chaired by the CIO. The CIO ensures compliance with SBA infrastructure and architecture standards and advises the BTIC on technical matters. The BTIC is responsible for reviewing and making decisions on all major IT investments, including screening, scoring, and prioritizing new initiatives, monitoring ongoing investments, and evaluating implemented investments.

**OMB Question B.3. How does the head of the agency ensure that the agency's information security plan is practiced throughout the life cycle of each agency system?**

According to SBA Standard Operating Procedure (SOP) 90 47, *Information System Security Program*, the Administrator has delegated the creation of information security plans to the CIO. During the FY 2002 reporting period, the CIO in concert with SBA program officials prepared system security plans for seven additional SBA systems as compared to the FY 2002 GISRA reporting totals.

The Agency has not codified through an SOP how security will be enforced for SBA systems throughout a system's development life cycle. An information notice was issued in

November 2001 that requires all internally developed systems to follow the SBA's Systems Development Methodology (SDM). No SOP covers the continuation of SBA systems in a production status or Computer Off-The-Shelf (COTS) software acquisition and the specific development of COTS products.

**OMB Question B.4. During the reporting period, did the agency head take any specific and direct actions to oversee the performance of 1) agency program officials and 2) the CIO to verify that such officials are ensuring that security plans are up-to-date and practiced throughout the lifecycle of each system?**

During the reporting period there were 28 operational and up-to-date system security plans for 38 SBA systems through August 29, 2003.

The OIG issued two audits in FY 2003 which concluded that SBA is not ensuring that its security plan is practiced throughout the life cycle of each agency system. Two systems in particular, the Joint Accounting and Administrative Management System (JA<sup>2</sup>MS) and the Disaster Credit Management Modernization System (DCMS), did not follow the SBA SDM while those systems were in a development status.

**OMB Question B.5. Has the agency integrated its information and information technology security program with its critical infrastructure protection responsibilities, and other security programs (e.g., continuity of operations, and physical and operational security)? Please describe.**

SBA has a Chief Information Assurance Officer (CIAO) who is responsible for the Agency continuity of operations and information and information technology security programs. SBA also has a Deputy CIAO who is responsible for physical and operational security. SBA has not integrated its information and information technology security program with physical and operational security.

**OMB Question B.6. Does the agency have separate staffs devoted to other security programs, are such programs under the authority of different agency officials, if so what specific efforts have been taken by the agency head or other officials to eliminate unnecessary duplication of overhead costs and ensure that policies and procedures are consistent and complimentary across the various programs and disciplines?**

The SBA has separate staffs assigned to physical security and information system security. There is little or no duplication of effort. The two sections can work in concert on issues of mutual importance and periodically meet to discuss Critical Infrastructure issues.



**OMB Question B.7. Identification of agency's critical operations and assets (both national critical operations and assets and mission critical) and the interdependencies and interrelationships of those operations and assets.**

SBA underwent the discovery phase of a Project Matrix Review in 2002. According to the review, no SBA system impacts national security, national economic stability, or critical public health and safety. Therefore, SBA does not possess any nationally critical assets.

OIG recommended in its audit of SBA's Implementation of its Cyber-Based Critical Infrastructure Protection Plan (Report 3-03 issued January 10, 2003) that the CIO update SBA's Critical Infrastructure Protection Plan (CIPP) to include the exact boundaries of SBA's mission essential cyber-based infrastructure. This update would identify critical SBA systems by name and their relationship to the five broad boundaries of mission essential cyber-based infrastructure identified in previous CIPP reports.

SBA currently uses system security plans and a mix of full system risk assessments and FISMA self assessments to identify its critical systems. SBA has not developed an agency-wide integrated security plan for implementing and integrating SBA's computer security program across all general support systems and major applications. Therefore, full interdependencies and interrelationships between critical systems have not been fully established agency-wide.

For disaster recovery and contingency planning purposes, SBA has a Contingency of Operations Plan (COOP) for Agency operations. However, the plan does not identify the SBA systems by the timeframe needed for recovery. For example, the SBA COOP has not identified mission critical general support systems and major applications that must be recovered and in what order in the event of a full emergency in which all systems are disabled. A prioritized timeline for recovery of 0-3 days, 4-10 days, 11-30 days, and 30 or more days should be determined for all SBA systems. Then, appropriate disaster recovery and contingency planning could be incorporated into the SBA COOP.

**Table 5**  
**SBA Critical Operations and Assets**

|   |   |     |    |     |
|---|---|-----|----|-----|
| a. Has the agency fully identified its national critical operations and assets, including their interdependencies and interrelationships? | Yes   | N/A | No | N/A |
| b. Has the agency fully identified the interdependencies and interrelationships of those nationally critical operations and assets?       | Yes   | N/A | No | N/A |
| c. Has the agency fully identified its mission critical operations and assets?  | Yes   | X   | No |     |
| d. Has the agency fully identified the interdependencies and interrelationships of those mission critical operations and assets?          | Yes   |     | No | X   |
| e. If yes, describe the steps the agency has taken as a result of the review.   | N/A   |     |    |     |
| f. If no, please explain why.   | SBA has not identified the boundaries of its mission critical assets as identified in OIG Report 3-03. Once boundaries are identified, interdependencies and interrelationships can be established. |     |    |     |

**OMB Question B.8. How does the agency head ensure that the agency, including all components, has documented procedures for reporting security incidents and sharing information regarding common vulnerabilities?**

According to SBA Standard Operating Procedure 90 47, *Information System Security Program*, the Administrator has delegated reporting of security incidents to the CIO who then further delegated responsibility to the Agency Computer Security Program Manager. OCIO issued the SBA Computer Emergency Response Team (CERT) procedures manual to report security incidents to the Agency Computer Security Program Manager who would then report those incidents to FedCIRC.

The SBA and FedCIRC developed a Memorandum of Understanding in June 2000 that requires a quarterly report of security incidents to FedCIRC. In 2002, SBA began monthly reporting of security incidents. SBA improved its security operations in this area for FY 2003.

**Table 6  
Agency Components**

|   |  |   |    |  |
|---|--|---|----|--|
| a. Identify and describe the procedures for external reporting to law enforcement authorities and to the Federal Computer Incident Response Center (FedCIRC). | The SBA Computer Security Program Manager receives all security incident reports from SBA and forwards these security incidents to FedCIRC on a monthly basis.   |   |    |  |
| b. Total number of agency components or bureaus.  | One  |   |    |  |
| c. Number of agency components with incident handling and response capability.  | One  |   |    |  |
| d. Number of agency components that report to FedCIRC.  | One  |   |    |  |
| e. Does the agency and its major components share incident information with FedCIRC in a timely manner consistent with FedCIRC and OMB guidance?              | Yes  |   |    |  |
| f. What is the required average time to report to the agency and FedCIRC following an incident?   | The average for the reporting period was thirty (30) days. No security incident required immediate reporting to FedCIRC in the past year. Procedures are in place to report severe security incidents within three days to FedCIRC if necessary. |   |    |  |
| g. How does the agency, including the programs within major components, confirm that patches have been tested and installed in a timely manner?               | The Agency requires reports from all general support systems and major applications which require patching. The reports identify that specific patches are tested and installed as soon a practical.   |   |    |  |
| h. Is the agency a member of the Patch Authentication and Distribution Capability operated by FedCIRC?  | Yes  | X | No |  |
| i. If yes, how many active users does the agency have for this service?   | 20   |   |    |  |
| j. Has the agency developed and complied with specific configuration requirements that meet their own needs?  | Yes  | X | No |  |
| k. Do these configuration requirements address patching of security vulnerabilities?  | Yes  | X | No |  |

**OMB Question B.9. Identify by bureau, the number of incidents (e.g., successful and unsuccessful network penetrations, root or user account compromises, denial of service attacks, website defacing attacks, malicious code and virus, probes and scans, password access) reported and those reported to FedCIRC or law enforcement.**

Table 7  
**Incident Reporting**

| Bureau Name | Number of incidents reported | Number of incidents reported externally to FedCIRC | Number of incidents reported externally to law enforcement |
|-------------|------------------------------|--|--|
| SBA (9)     | 169,556                      | 169,556  | 3,385  |

Comment 9 – The security incident reporting period was the twelve month period of August 1, 2002 through July 31, 2003.

**OMB Question C.1. Have agency program officials and the agency CIO: 1) assessed the risk to operations and assets under their control; 2) determined the level of security appropriate to protect such operations and assets; 3) maintained an up-to-date security plan (that is practiced throughout the life cycle) for each system supporting the operations and assets under their control; and 4) tested and evaluated security controls and techniques? By each major agency component and aggregated into an agency total, identify actual performance in FY03 according to the measures and in the format provided below for the number and percentage of total systems.**

Table 8  
**SBA Systems and System Risk Assessments**

| Bureau Name         | Total Number of Systems | Number of systems assessed for risk and assigned a level or risk |              | Number of systems that have an up-to-date IT security plan |    | Number of systems certified and accredited |    | Number of systems with security control costs integrated into the life cycle of the system |           | Number of systems for which security controls have been tested and evaluated in the last year |            | Number of systems with a contingency plan |    | Number of systems for which contingency plans have been tested |    |
|---------------------|-------------------------|--|--------------|--|----|--|----|--|-----------|---|------------|---|----|--|----|
|                     |                         | No. of Systems   | % of Systems | No.  | %  | No.  | %  | No.  | %         | No.   | %          | No.                                       | %  | No.  | %  |
| <b>Agency Total</b> | 38                      | 28   | 74           | 28   | 74 | 28   | 74 | 0<br>(10)  | 0<br>(10) | 8   | 29<br>(11) | 15  | 39 | 15   | 39 |

Comment 10 – SBA’s Exhibit 53 for FY 2003 was compared to Agency information on security costs for certain individual systems. We found that no records exist at SBA to quantify exactly how much was actually spent as individual line items on security for each SBA system in FY 2003. This was due to the fact that SBA’s financial accounting systems were not structured to report computer security expenditures by system, but were aggregated into the infrastructure or OCIO computer security budget.

Comment 11 – SBA completed eight Certification and Accreditation (C&A) reviews between August 2002 and August 2003. SBA has instituted Security Test and Evaluation (ST&E) reviews as a part of each new C&A package.

**OMB Question C.2. Identify whether the agency CIO has adequately maintained an agency-wide IT security program and ensured the effective implementation of the program and evaluated the performance of major agency components.**

**Table 9**  
**SBA Agency-wide IT Security Program**

| Has the agency CIO maintained an agency-wide IT security program?<br>Y/N | Did the CIO evaluate the performance of all agency bureaus/components?<br>Y/N | How does the agency CIO ensure that bureaus comply with the agency-wide IT security program? | Has the agency CIO appointed a senior agency information security officer per the requirements in FISMA? | Do agency POA&Ms account for all known agency security weaknesses including all components? |
|--|---|--|--|---|
| Yes  | N/A   | C&A's, ST&E's, and Self-Assessments  | Yes  | No (12)   |

Comment 12 – We reviewed OIG audits issued before May 1, 2003 which should have incorporated security weaknesses into the June 30, 2003 SBA POA&M. Only four of 22 security weaknesses were incorporated in SBA's most recent POA&M that was issued on June 30, 2003.

**OMB Question C.3. Has the agency CIO ensured security training and awareness of all agency employees, including contractors and those employees with significant IT security responsibilities?**

**Table 10**  
**SBA Security Training and Awareness**

| Total number of agency employees in FY03 | Agency employees that received IT security training in FY03 |            | Total number of agency employees with significant IT security responsibilities | Agency employees with significant security responsibilities that received specialized training |            | Briefly describe training provided | Total costs for providing training in FY03 |
|--|---|------------|--|--|------------|------------------------------------|--|
|  | Number  | Percentage |  | Number   | Percentage |                                    |  |
| 4124                                     | 3802  | 91         | 142  | 110  | 76         | (13)                               | \$179,368                                  |

Comment 13 – SBA requires all employees to annually complete end-user computer security awareness training. SBA requires additional training modules for employees who are a Functional Program Manager, Designated Security Officer (DSO)/Information Resources Manager (IRM), and/or System Administrator (S/A).

**OMB Question C.4. Has the agency CIO fully integrated security into the agency's capital planning and investment control process? Were IT security requirements and costs reported on every FY05 business case (as well as in the exhibit 53) submitted by the agency to OMB?**

**Table 11  
IT Capital Planning and Investment**

| Bureau Name | Number of business cases submitted to OMB in FY05 | Did the agency program official plan and budget for IT security and integrate security into all of their business cases? Y/N | Did the agency CIO plan and budget for IT security and integrate security into all of their business cases? Y/N | Are IT security costs reported in the agency's exhibit 53 for each IT investment? Y/N |
|-------------|---|--|---|---|
| SBA         | 9   | Partially Yes, Partially No (13) and Partially Unknown (14)  | Unknown (14)  | Yes   |

Comment 13 – One of eight business cases reviewed did not have IT security integrated into the system life cycle. The business case identified was the GCBD: 8(a) Internet Application Form .

Comment 14 – SBA had one business case representing all OCIO and agency program systems in the steady state phase of their life cycle. This business case known as the SBA Meta Capital Asset Plan was not ready for our review as of September 15, 2003. Therefore, this question could not be answered by the conclusion of our review.

\* \* \*

This report does not contain any recommendations. OCIO reviewed a draft version of this report before it was issued and requested clarification on one issue relating to tracking security costs in the life cycle of SBA systems. Should you or your staff have any questions, please contact Robert G. Hultberg, Director, Business Development Programs Group at (202) 205-7577.

Attachment

**ATTACHMENT**

**REPORT DISTRIBUTION**

| <u>Recipient</u>   | <u>Number of Copies</u> |
|--|-------------------------|
| Associate Deputy Administrator for Management and Administration ..... | 1                       |
| Chief Information Officer .....  | 1                       |
| General Counsel .....  | 3                       |
| General Accounting Office .....  | 1                       |
| Chief Financial Officer .....  | 1                       |
| Attention: Jeff Brown  |                         |