AUDIT REPORT

THE SMITHSONIAN ASSOCIATES
STUDY TOURS RESERVATION PROCESS

Number A-02-03

June 12, 2002

SUMMARY

The Office of the Inspector General audited the controls over The Smithsonian Associates (TSA) study tours reservation process. The purpose of the audit was to evaluate the study tour reservation process internal controls and the reservation system's general controls that address access controls, application program change controls, segregation of duties, and service continuity planning.

Overall, TSA did have some internal controls in place regarding the study tour reservations process. However, the reservation system safeguards were inadequate and the risk to system access and data integrity was high. During our audit, TSA management promptly required passwords to be changed and initiated action to develop business continuity plans. Smithsonian policy states and good business practices suggest that controls should be established to maintain accountability for the custody and use of resources and to provide reasonable assurances that assets are safeguarded against loss or unauthorized use. Therefore, we made recommendations to improve internal and general controls over the study tour reservation process to include:

- Adopting and implementing a reservation system continuity of operations plan,
- Performing an operations risk assessment,
- Formalizing the system maintenance contract,
- Developing procedures for secure storage of patron data,
- Obtaining patron affirmative consent, and
- Formalizing agreements for the use of patron information.

The Director of The Smithsonian Associates agreed with most of our recommendations. We recommended that the Director reconsider and provide additional comments to the disagreed recommendations. Overall, we believe that the corrective actions taken are responsive to the recommendations. For those recommendations requiring additional implementation plans, we plan to follow up with the Director.

Office of the Inspector General

Office of the Inspector General

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

GAO	General Accounting Office
SD	Smithsonian Directive
TSA	The Smithsonian Associates

INTRODUCTION

A. Purpose

The purpose of the audit was to evaluate The Smithsonian Associates (TSA) study tour reservation process internal controls and systems general controls that address access controls, application program change controls, segregation of duties, security, and service continuity for the study tour reservation information system.

B. Scope and Methodology

The audit was conducted from February 26, 2002, through May 10, 2002, in accordance with generally accepted government auditing standards. The audit methodology consisted of the following:

- Identifying and reviewing applicable policies and procedures relating to internal controls, computer system security and integrity of reservation data;
- Assessing TSA's study tour reservation system (SELECT)[1] regarding computer security plans, policies, and procedures for compliance with Institution policies;
- Evaluating controls to assess safeguards to protect sensitive data and ensure that patron data is reliable and complete;
- Assessing the adequacy of controls to prevent or detect unauthorized activities, including external intrusion, theft, or misuse of patron data, and destruction of hardware, software, and data;
- Evaluating the SELECT reservation system and security plans, controls, procedures, practices, standards, and policies covering the General Accounting Office's Federal Information System Controls Audit Manual (FISCAM[2]); and,
- Utilizing guidance issued by the National Institute of Standards and Technology relating to information system disaster recovery and business continuity planning.

We reviewed:

- Policies, procedures, and controls relating to system security and integrity of reservation data,
- Controls over sensitive patron data, and
- Controls to prevent or detect unauthorized activities, including theft, misuse or destruction of hardware, software, and patron data.

We conducted interviews regarding the daily administration of the study tour reservation process that included TSA Management, Registration and Customer Service, Study

[1] During June 2001, software modifications were made to SELECT information system to incorporate the ability to process study tour reservations as well as Resident Associate Program reservations and memberships. The SELECT system is the information system used within TSA to process Resident Associate Programs ticketing, Memberships, and Study Tour reservations.

[2] The FISCAM manual is designed for evaluations of general and application controls over financial information systems that support agency business operations. FISCAM control areas include access controls, application program change controls, segregation of duties, operating system security, and service continuity.

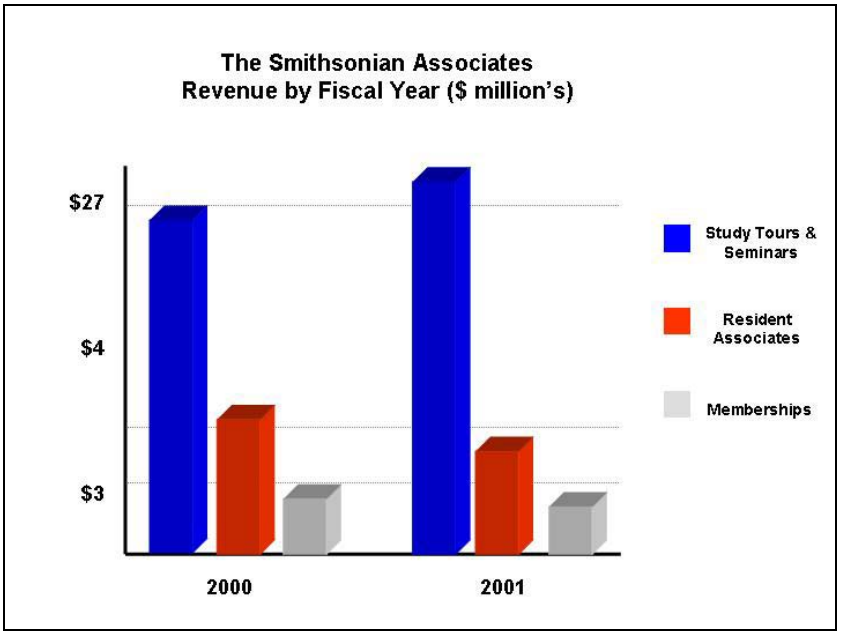
Tours, Business Office, Information Technology, Marketing and Membership staff, and a consultant supporting the TSA reservation system. Through interviews, we gained an understanding of the practices employed concerning reservation system access limitations, password security, business continuity and disaster recovery plans, and maintenance and modifications. And finally, we interviewed staff concerning the collection and leasing of patron data.

C. Background

TSA consists of three major programs: the Smithsonian Study Tours, the Resident Associate Program, and the Membership Programs. The Study Tours consist of International Tours, Odyssey Tours, seminars, and national and local day and overnight tours. The Resident Associate Program is a comprehensive non-credit curriculum in liberal studies, which is offered to the 55,000 Resident Associate member households and to the public. TSA membership programs generate revenue from the collection of fees of the Resident Associate and Young Benefactors.

This audit concentrated on TSA study tours, which represents the majority of revenue generated by TSA. As shown below, TSA study tours generated in FY 2001 approximately $103,342 each day[3].

Table 1



TSA's study tours program offers participants the opportunity to travel and learn through trips designed by Smithsonian experts. Study tours are divided into US/Canada tours (including local tours), International tours, and Seminars (both international and domestic). The majority of all Study Tour reservations are processed by the Select system.

[3] FY 2001 revenue of $26,868,920 / 52 weeks / 5 days = $103,342.

RESULTS OF AUDIT

A. Disaster Recovery and Continuity of Operations Plans

TSA has not implemented disaster recovery and continuity of operations plans for restoring its SELECT reservation system. Because of budget and other staff priorities, management has not taken steps to develop and implement disaster recovery and continuity of operations plans. Without these plans, TSA could face study tour financial losses alone of approximately $103,342 each day the SELECT system is not in operation. In addition, management is unprepared in the event operations are rendered inoperative due to a system failure, compromise, or a disaster situation.

Background

The scope of our review consisted of evaluating the existing disaster recovery and business continuity plans in place for the SELECT reservation system. We interviewed TSA management and information technology staff to gain an understanding of TSA operations and reliance on the SELECT reservation system.

"Smithsonian Institution Computer Security Handbook," September 9, 1993, provides computer security policies and procedures for all Smithsonian components to develop disaster recovery and business continuity plans. Disaster recovery safeguards consist of developing a contingency plan, storing the plan offsite, regularly backing up files and software, identifying an alternate offsite processing site, and testing the contingency plan. According to the Handbook, the purposes of a contingency plan are to determine actions that will, minimize the effects, of undesirable occurrences, document emergency response actions, restart the system, and establish procedures for recovering from losses.

The National Institute on Standards and Technology has published ***"The Contingency Planning Guide for Information Technology Systems (December 2001),"*** which provides instructions, recommendations, and considerations for government IT contingency planning. According to National Institute on Standards and Technology guidance, some type of documented procedures should be in place to provide for the recovery of files, address disaster recovery, and identify critical processing (data). The plan should allow for periodic testing (at least annually) and should ensure that personnel understand their respective roles during a disaster.

Results of Review

Our review determined that TSA has not documented and implemented disaster recovery and business continuity of operations plans for the SELECT system. TSA uses the SELECT system to record, process, store, and manage its study tour reservation transactions. In fiscal year 2001, study tours alone generated approximately $26.9 million or $103,342 per day in revenue. In addition, patron data is stored within the system and is extensively used for preparing management reports and for marketing purposes. Disaster recovery and contingency plans assess the adequacy and ensure continuity of operations if either a complete system failure or the failure of system components occurs.

Management has not taken steps to develop and implement disaster recovery and continuity of operations plans because of budgeting and staff priorities. In September 2001, the SELECT system was becoming fully operational. During this time, study tour reservations significantly declined from September through the remainder of 2001. Because of this decline, management redirected its attention concerning office and budget priorities.

During the audit, management noted that the Office of the Chief Information Officer also did not have detailed guidance on developing disaster recovery and business continuity plans. TSA management stated that plans were recently considered to identify an offsite file backup location and possible alternative site for maintaining telephone reservation operations. Offsite telephone operations would permit study tours to continue to accept reservations that would subsequently be entered into SELECT at the main TSA office or at a restored SELECT center location.

Without disaster recovery and continuity of operations plans, TSA could face financial losses of approximately $103,342 each day the SELECT system is not in operation. Disaster recovery and continuity of operations plans would add assurance that the recovery of files, software, and equally important business operations will continue with the least amount of disruptions. During the audit we provided TSA with draft guidance from the U.S. Department of Commerce, National Institute on Standards and Technology, Special Publication 800-34: "***Computer Security, Contingency Planning Guide for Information Technology System (December 2001).***" To their credit, TSA has a system backup tape process; however, the tapes are stored locally. Additional assurances can be gained if the backup tapes of critical information and materials are kept both on and off-site TSA began taking steps to develop its disaster recovery and business continuity operations plans, including establishing an off-site storage location during the audit.

Conclusion

Because the SELECT system is essential and critical to TSA's daily operations, it is important that disaster recovery and continuity of operations plans be in place. Without implemented disaster recovery and business continuity plans, TSA is unprepared and could face substantial financial losses in the event SELECT system operations are rendered inoperative. Recovery and continuity of operations plans should address, at a minimum, the identification of critical system processes and off-site storage for back-up tapes.

Recommendation

We recommended that the Director of The Smithsonian Associates adopt and implement disaster recovery and continuity of operations plans for the SELECT system.

Management Comments

Agreed. Management has begun researching, planning, and implementing disaster recovery and continuity of operations plans for the SELECT system. Management intends to complete the plan by September 30, 2002.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation. We will follow up with the Director in October 2002 to obtain the status of this recommendation.

B. Reservation Process Internal Controls

TSA study tour reservation internal controls can be strengthened. Currently, TSA staff has greater reservation system access than necessary to fulfill their responsibilities. In addition, there are no system procedures that prevent staff from making unauthorized modifications. This occurred because after TSA fully transitioned to the SELECT system, it did not perform a system operations risk assessment. As a result, TSA did not identify and establish policies and procedures that define user groups with access levels tied to their functional responsibilities, remove unauthorized users, or formalize procedures for processing refunds. As a result, the lack of adequate internal controls increases the opportunity for unauthorized modification of files and programs and significantly decreases the integrity of the system.

Background

The scope of our review consisted of evaluating the reservation system process, system access, and record modification procedures in place from February 2002through May 2002. We interviewed TSA management, reservation and information technology staff, and a system support consultant.

Smithsonian Directive 115, ***Management Controls***, revised July 23, 1996, lists standards that shall apply to Institution units. In particular, the directive requires manager's to take systematic and proactive actions to develop and implement appropriate, cost effective management controls. It also requires that controls established shall provide reasonable assurance that assets are safeguard against waste, loss, unauthorized use, and misappropriation. In addition, management should separate key duties and responsibilities relating to authorizing, processing, recording, and reviewing official agency transactions. Managers are also required to exercise appropriate individuals and assign accountability for the custody and use of resources.

"Smithsonian Institution Computer Security Handbook," September 9, 1993, provides computer security policies and procedures for all Smithsonian components. The goals of the computer security program are to perform a risk assessment to prevent unauthorized disclosure of sensitive information, and protect data from accidental or malicious alteration or destruction. In addition, computer systems must undergo a risk analysis to identify potential threats to the computer system. Risk analysis can determine the appropriate and cost effective security measures that computer systems should maintain.

Results of Review

We determined that internal controls regarding system administrative access, password assignments, and refund processing could be strengthened. The TSA study tour reservation process consists of reservations coordinators taking study tour phone reservations, entering patron bookings that include names, addresses, credit card information, and processing credit card charges in SELECT. Our review of the SELECT user access listing showed there were 131 user accounts that either were in multiple user groups or had more than one access account to the SELECT reservation system.

In the hierarchy of user groups, the highest level of system and data access is the administrative level. Administrative access provides the user with the ability to add or

delete SELECT system users, modify or delete master patron records, and access different reports. Other non-administrative groups have access rights that can also alter master patron file records and information. Our review of the user listing determined that many TSA users have administrative access rights with more than one logon account. These users' duties may not necessarily require such a high level of system access. For example, administrative system rights are given to business office staff who perform accounting and other administrative duties, as well as reservation staff that are authorized to grant patron refunds. We believe that separation of duties is necessary between those staff members that have the ability to change and modify master files and those who perform accounting and revenue recording duties. To their credit, TSA has established several different user groups with different levels of system access. However, these user groups were established for processing sales and did not necessarily consider computer security.

We reviewed the process for granting access and removing users from the SELECT system. We determined that logon names were initially assigned to staff in a manner inconsistent with the Institution password policy. For instance, users are provided a logon name that closely resembles their personal name and then assigned a password that is also closely identified to their name. Assigning user accounts with closely matching passwords is a serious weakness that can undermine the security and data integrity of a system. As noted in the "***Smithsonian Institution Computer Security Handbook,"*** passwords are often the first line of defense in protecting computer systems from unauthorized use and disclosure. Easily guessed passwords is the weakness most frequently exploited by unauthorized users. If the unauthorized user knows the account holder, guessing the password is often just a matter of entering a name. Difficult passwords drastically reduce vulnerability from unauthorized users. Although the SELECT system can allow users to reset their passwords, staff were seldom advised to reset their passwords. With regard to removing user accounts from SELECT, TSA staff stated that there is no formal internal process for identifying users who no longer require SELECT access. Users are removed only when a supervisor informs a designated SELECT system administrator or because a TSA administrator notices that a staff member has left.

Also, in evaluating the study tour reservation internal controls, we identified the process of applying refunds to patrons as a control point within the reservation process that should be strengthened. Study tour refunds can arise when TSA cancels a study tour or when a patron either cancels or changes a study tour reservation. Although TSA's refund policy varies according to the type of tour, refunds are usually not permitted within a certain number of days before a tour begins. We noted that the credit card process performs address verification when a study tour charge is placed but not when a refund credit is processed. This occurred because the bank credit card processor is unable to institute address verification for credit refunds.

Management had taken action to strengthen internal controls in the reservation refund process by specifically identifying the reservations manager as the individual who will have the authority and responsibility to process refunds. The process requires the reservation coordinators to inform the patrons that their cancellation or refund request will be noted and they are required to submit a written request for a refund to TSA. The patron's refund, however, will not be processed and credited until the written request is received by TSA. TSA policy is to apply the refund to the credit card initially charged. Management stated that the process was communicated orally to staff during a staff meeting. Study Tour staff have also prepared step-by-step procedures for canceling a

reservation in the SELECT system. Although the refund process was strengthened, we determined that SELECT users could circumvent the controls and process refunds undetected.

TSA staff informed us that, since migrating the study tour reservation process over to the SELECT system, management has not performed a risk assessment of its operations. A risk assessment of its newly modified reservation system coupled with a staff operational process review would have given management an opportunity to establish user access groups, comply with password policy, and strengthen system controls to prevent unauthorized record modifications. In addition, during the migration period, TSA's attention was redirected because of a significant number of study tour cancellations due to the tragic events of September 11, 2001.

Generally, an absence of reliability and accountability in computer systems compromises access and service to legitimate users. Without adequate access and record modification safeguards in place, patron data could be compromised or misused and refund transactions could be unauthorized and undetected. Because of weak passwords, there is no assurance that all user transactions were made by the apparent users. SELECT data integrity risk increases when inaccurate data could be used to make imprecise business or management decisions. Moreover, any compromise of patron data could lead to possible legal action or negative publicity for the Institution. During the audit, TSA management stated that they will comply with the password policy and quickly required passwords to be changed to a scheme that was not easily identifiable.

Conclusion

We determined that after fully transitioning to the SELECT system, TSA had not performed a risk assessment of its operations. An operations risk assessment coupled with defining staff functional responsibilities with respective SELECT access, could have strengthened internal controls for making study tour reservations.

Recommendations

We recommended that the Director of The Smithsonian Associates:

1. Perform a risk assessment that removes unnecessary accounts and establishes user access groups that more closely identify operational responsibilities with respective SELECT access requirements.
2. Comply with Institution password policy and require all users to reset their SELECT passwords to conform to the policy.
3. Modify the SELECT system to limit the ability to process refunds to a designated user group and lockout the ability to process refunds after the prohibited refund date.

Management Comments

Agreed. The Director has already taken action to remove unnecessary accounts and assigned the reservations manager the responsibility to review all account changes. In addition, a review of user groups that includes evaluating access levels by each group will be completed by June 20, 2002.

Agreed. The Director has already required passwords to be changed to a more stringent scheme and has implemented written password policy.

Agreed. The Director plans to modify the SELECT system to permit only the reservations manager to process refunds.

Office of the Inspector General Response

We believe that the Director's actions are responsive to the recommendations. Recommendations two and three are considered closed and we will follow up with the Director in July 2002 concerning recommendation one.

C. Reservation System Contracting

TSA has not formalized its support contract for SELECT software maintenance and development upgrades. In addition, TSA does not have a process for documenting and maintaining its SELECT system changes. The software maintenance and development support contract was not established because management had not identified the scope required for system support. Management further relied on a software support provider to maintain the documents and records (software modifications) made to the system. Without a formal written contract in place, there is an increased risk that the legal interests and intellectual rights of the Institution may not be fully protected. In addition, without a software change and configuration documentation process, management has no assurances that the system will be kept operational and that future changes will be performed efficiently.

Background

The scope of our review consisted of evaluating the process employed by TSA to maintain change and configuration management of the SELECT reservation system changes in place during September 2001 through May 2002. We interviewed TSA management, information technology staff, and the system support consultant.

Smithsonian Directive 115, ***Management Controls***, revised July 23, 1996, requires that Institution managers take systematic and proactive measures to develop and implement appropriate, cost effective management controls that provide reasonable assurance that assets are safeguarded.

The Office of Contracting's ***Informational Briefing: Making Small Purchases at the Smithsonian Institution, FY 2001***, provides basic policies and procedures for purchasing. In addition, the Office of Contracting has established restrictions on certain types of purchases that include custom developed software.

Results of Review

As part of evaluating the SELECT software change and configuration controls, we noted that TSA did not have a formal contract in place for software maintenance and development services. During the audit, we discovered that TSA was paying a consultant for system software maintenance and modifications. Additionally, TSA was not maintaining software changes made by the consultant. TSA management had not formalized its SELECT contract support because they did not know the extent and type of contract required, as well as the level of support needed to maintain the system. Since migrating study tour reservation processing to the SELECT system, management had not defined its contract support requirements.

In addition, TSA management did not maintain the software programming changes because the system is written in a unique software programming language in which TSA staff is not well versed. According to TSA staff, the consultant who supports the system specializes in supporting the SELECT system. As a result, management relied on the software support provider to maintain the documents and records related to the SELECT system.

Absent a formal written contract, there is an increased risk that the legal interests and intellectual property rights of the Institution may not be fully protected. Without a software change management process, TSA may not be able to maintain critical reservation system data processing and could experience unnecessary delays if the consultant decides not to support the SELECT system. Furthermore, each reservation software change must be maintained by TSA in a systematic and controlled manner in order to keep the reservation system operating efficiently. During the audit, TSA management began drafting a statement of work to support the system changes.

Conclusion

TSA does not have a support contract in place for SELECT software maintenance and development upgrades or a process for documenting and maintaining its system changes. At a minimum, a formalized contract will identify the scope of work, length, and costs for services, and required system and data access to meet service requirements. Additionally, the contract should also identify the process needed to ensure that all system changes are documented, maintained, and evaluated.

Recommendations

We recommended that the Director of The Smithsonian Associates:

1. Define and put in place, with support of the Office of Contracting, a contract for the maintenance of and modifications to the SELECT system.

2. Obtain the system documentation, including changes, from the SELECT consultant and establish a change and configuration process for future modifications.

Management Comments

Agreed. The Director plans to determine TSA SELECT contract needs and require that the contract include provisions for system documentation and a change and configuration management process for future system changes by June 30, 2002. Once determined, the Director plans to obtain assistance in writing the contract from the Office of Contracting.

Office of the Inspector General Response

The Director's actions are responsive to the recommendations. We will follow up in July 2002 on the status of this recommendation.

D. Patron Data Protection

TSA needs to improve the security of sensitive patron data obtained by study tour operations. Sensitive patron data is kept in binders in open workstations, unlocked cabinets, electronic mail accounts, and in personal computers. This occurred because TSA has not identified nor implemented data handling and storage procedures. Without adequate safeguards for protecting patron data, the risk that the data could be compromised, accessed or used without authorization, lost, or misplaced increases. Also, the Institution could face unnecessary litigation or negative publicity if TSA fails to implement safeguards to protect patron data.

Background

The scope of our review consisted of evaluating the study tour reservation process to include the type and extent of information collected, as well as the storage and protection of, and access to patron data. We interviewed Study Tour Reservation Coordinators, Program Coordinators, and Marketing and Business Office staff.

Smithsonian Directive 115, ***Management Controls***, revised July 23, 1996, requires Institution managers, to take systematic and proactive measures to develop and implement appropriate, cost effective management controls that provide reasonable assurance that assets are safeguarded against loss or unauthorized use, and maintain accountability for the custody and use of resources.

"Smithsonian Institution Computer Security Handbook," September 9, 1993, provides computer security policies and procedures for managers of computer systems. The goals of the computer security program are to prevent unauthorized disclosure of sensitive information and protect data from accidental or malicious alteration or destruction.

Results of Review

During our review of the TSA study tour reservation process, we determined that sensitive patron data is being insecurely kept in binders at staff workstations, in unlocked file cabinets, within electronic mail accounts and in personal computers. Sensitive patron data consists of patron names, addresses, credit card information, and banking and checking account information. TSA's practice is to store patron data in the office for several years after a study tour trip. TSA also receives sensitive patron data via its website and in electronic mail messages for study tours reservations. Although management has implemented protection methods of encrypting the patron data as it is transmitted from its website to TSA, once the messages are de-encrypted they are stored online in an Institution network electronic mail folder. The patron information is transferred from electronic mail to a Microsoft Word document and subsequently transmitted to others within TSA for study tour reservation processing. The individual Microsoft Word document is then saved and stored in personal computers. As a result, numerous documents containing patron information are being collected and stored throughout TSA without some level of protection.

This occurred because TSA had not performed a recent operational risk assessment since reorganizing its operations and migrating study tour reservations to SELECT. An

operational risk assessment should include evaluating and implementing data handling and storing procedures to ensure that patron data is secure.

Without implementing adequate safeguards for protecting patron data, the risk that the data could be compromised, accessed, or used without authorization, lost, or misplaced increases. According to SD 115, TSA has an obligation to protect patron data and could face unnecessary litigation and negative publicity if they fail to implement safeguards to do so.

Conclusion

TSA can benefit by implementing stronger controls regarding patron data collected by the study tour reservation process. Adequate security controls and safeguards over sensitive electronic and hard copy patron data obtained by study tour operations reduces the risk of patron data being compromised, accessed, or used without authorization, and even lost or misplaced.

Recommendation

We recommended that the Director of The Smithsonian Associates develop and implement office procedures for the secure storage of electronic and hard copy forms of patron data.

Management Comments

Agreed. The Director in May 2002 changed its online shopping cart software and process to decrypt and save web orders over to a secure server with limited staff access. The Director also began implementing office procedures to secure storage of electronic and hard copy forms of patron data. By July 31, 2002, a review of both paper and electronic records will be performed to eliminate any unnecessary or redundancy of storage.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation. We will follow up in August 2002 to obtain the status of this recommendation.

E. Study Tour Solicitations

TSA is marketing and leasing, to list rental companies, patron information without affirmative consent. In addition, TSA does not have a formal agreement with list rental companies that define the use and restrictions of leased patron information. Also, TSA is using patron information to inform patrons of future TSA promotions without obtaining their affirmative consent. This is occurring because officials have not sought patron consent permitting TSA to use internally, or market patron information. Because of a decrease in interest in leasing patron information, management had not planned to formalize its lease rental company agreements. As a result, TSA patrons may not always affirmatively give TSA rights to use this data for internal purposes or to market it to third parties.

Background

The scope of our review consisted of evaluating the data collected and used by TSA study tour reservation process from January 2002 through May 2002. We interviewed TSA management, information technology, and marketing staff.

Smithsonian Directive 115, ***Management Controls***, revised July 23, 1996, requires that Institution managers take systematic and proactive measures to develop and implement appropriate, cost effective management controls that provide reasonable assurance that assets are safeguarded.

Smithsonian Internet Privacy Policy states that the Institution "will never share your name or information outside the Smithsonian unless you affirmatively authorize us to do so by opting-in." Opting-in is the means by which patrons give permission to the Institution to share their information with third parties.

Results of Review

As part of our review of the TSA study tour process, we evaluated patron data collected and how this data was protected and used within TSA. Through discussions with TSA marketing staff and the Webmaster, we determined that TSA is collecting, marketing, and selling TSA patron information to list rental companies without fully disclosing to patrons how their personal information is being used. TSA gathers patron personal information from a variety of sources and has established a marketing database populated with patron information from study tours, as well as the Resident Associate and Memberships Programs. TSA uses its marketing database for both TSA internal promotional efforts, as well as a source of revenue by leasing patron listings to list rental companies. Although management stated that interest in lease listing has decreased, in fiscal years 1999 through 2001, TSA generated $146,000 in revenue from the rental of its marketing database. Internal TSA solicitation efforts have consisted of postal mailings of literature as well as targeted electronic mail advertisements. TSA provides the electronic mail addresses, develops the advertisement content, and provides the information to an electronic mailer. The electronic mailer then distributes the electronic advertisements. For postal solicitations, TSA did not ensure that a formal agreement is established with its list rental companies. Although, TSA management stated the list rental companies impose restrictions to the third party marketers, without a formal agreement with the list

rental companies, there is no assurance or requirement that the list rental companies will impose any TSA restrictions on successor third parties.

This occurred because TSA has not sought to obtain patron consent to market patron collected information. Specifically, TSA has not sought to obtain patron consent through its website or paper documents provided to study tour patrons. In addition, no formal agreement exists between TSA and third parties because, according to TSA management, listings have decreased and management was not planning on actively leasing patron information. TSA also relied on verbal and electronic mail to communicate any price and usage restrictions. In FY 2001, 5,800 patrons traveled on TSA study tours. TSA management indicated that information requesting consent had been included in previous publications. However, a review of documents sent to patrons who have booked recent tours, did not reveal any type of disclosures or requests for permission to sell patron information to third parties nor was there an opportunity on the TSA website that allowed patrons to affirmatively consent to share their personal information outside of the Institution.

As a result, study tour patrons that receive unsolicited TSA promotions and third party marketing advertisements may negatively perceive that TSA is marketing and sharing their information with third parties without their consent. Without a formal written agreement in place between TSA and the third party marketers, there is an increased risk that the interests and rights of TSA and its patrons may not be fully protected. In addition, TSA is at risk of not complying with the Institution's Internet privacy policy by not obtaining patrons' consent to market their information outside of the Institution.

Conclusion

The gathering and usage of patron information for solicitation purposes requires adequate disclosures to mitigate any negative patron reactions when receiving unsolicited advertisements. Although the Institution may not, as some contend, legally be required to abide by federal restrictions on the gathering and usage of personally identifiable information, the public may nevertheless perceive the Institution and TSA as a federal entity. TSA should allow patrons the opportunity to authorize TSA to store and market their personal information. Additionally, the execution of a formal agreement between TSA and the third party marketers should, at a minimum, define limits on the use and time period the leased listings can be used, and whether the listing can be subsequently sold to others.

Recommendations

We recommended that the Director of The Smithsonian Associates:

1. Establish disclosures within their reservation study tour documents and website that offers patrons the choice to allow their personal information to be used for marketing purposes internally or to third parties.

2. Formalize agreements with those companies that lease TSA patron lists that include, at a minimum, pricing and usage restrictions.

Management Comments

Partially agreed. The Director agrees that patrons be given the choice of whether their information is used for marketing purposes by third parties. To accomplish this, a review is planned of all marketing materials used to ensure that a check-off is included for use of an individual's name by third parties. The review will be completed by August 30, 2002, and needed changes implemented. However, the Director strongly disagreed with the recommendation that individuals should give TSA approval before TSA can contact them with information about TSA programs. According to the Director, maintaining and mining TSA mailing lists is essential to TSA's financial health.

Disagreed. The Director disagreed with the recommendation because each transaction that involves the list rentals is already formalized by an agreement, which includes pricing and usage restrictions, between the list rental company and subsequent third parties.

Office of the Inspector General Response

The Director's plan to review all materials used for marketing to be sure that a check-off is included for use of an individual's name by third parties is responsive to our recommendations. We will follow up in September 2002 to obtain the status of this recommendation.

We disagree with the Director's comments that an agreement is already in place with third party marketers. Although an agreement may be used by the list rental companies, TSA has no assurance that these companies are always including and requiring any third parties to comply with any restrictions. Without a formal agreement with the list rental companies that specifically addresses patron usage restrictions and requiring "flow-down" to third parties, TSA may have no legal oversight to the list rental companies or third party marketers. As a result, we believe the Director should consult with the Office of the General Counsel to ensure that TSA is meeting legal requirements for patron data usage. Subsequently, we request the Director to provide additional comments by July 31, 2002, regarding the recommendation.

WRITTEN COMMENTS BY THE DIRECTOR, THE SMITHSONIAN ASSOCIATES

The Smithsonian Associates — Memo

Mara Mayor
Director

TO: Thomas D. Blair
Inspector General

FROM: Mara Mayor MM

SUBJECT: TSA's response to the Audit draft report, Number A-02-03

DATE: June 6, 2002

CC: Herma Hightower

Thank you for an opportunity to respond to the draft report of the recent audit of TSA's study tours reservations processed, dated May 14, 2002.

In general, the report is accurate in its information and facts. However, there are a few clarifications we wish to make, as noted in the individual sections below. In addition, for each section we have provided a response to the specific recommendations.

Introduction:
Clarification:
Footnote #1. We began to use Select Ticketing for Study Tours reservations in June of 2001.
Page 2, C. Our tour program is called "Smithsonian Study Tours," not "Smithsonian Study Tours and Seminars."
Page 2., C. As of February 15, 2002, TSA was staffed with 100 trust employees (90 full time and 10 part-time).
Page 3. For staff organizational purposes, study tours are divided into US/Canada tours (including local tours), International tours, and Seminars (which may be international or US). We do not have a division within the office for US and Canada Tours and Seminars.
We offer cruises on oceans and rivers both internationally and within the US. We do not charter cruise ships.
Not all study tour reservations are processed by our staff in Select. During the period of this audit, our Odyssey tours with Saga Holidays were registered by Saga staff in Boston, per our contract with Saga.
Footnote #3. In calculating the dollar loss per day were our systems to be down, the

SMITHSONIAN INSTITUTION
Ripley Center Suite 3077
1100 Jefferson Avenue SW
Washington DC 20560-0701
202.357.2696 Telephone
202.633.8909 Fax
mayorma@tsa.si.edu E-mail

WRITTEN COMMENTS BY THE DIRECTOR, THE SMITHSONIAN ASSOCIATES

calculation was based on the total revenue for all Study Tours. However, the orders for our Odyssey line were actually processed elsewhere (in Boston), so that revenue should be subtracted. It doesn't make a big difference in the number, but it is more accurate to say that the loss per day would be $103,342.

Finding A: Disaster Recovery and Continuity of Operations Plan
We concur with the audit recommendations.

Based on your recommendations, we will research, plan, and implement a disaster recovery and continuity of operations plan for the Select system. We had begun work to this end by contacting SI Catalogue in Chantilly, Virginia. We knew they had space, computers and telephones that we might have used to continue our operations off the Mall. However, since they are now moving out of the DC area, we are working on an alternate plan.

The target date for completing this plan is September 30, 2002.

Finding B: Reservation Process Internal Controls
Clarifications:
Page 6, results of review. We call staff who process tour applications "reservations coordinators," not "reservationists."
Page 7, paragraph 4. We have always required a written request from an individual before a cancellation is processed. This is not a new process. What is new is that refunds to individuals are made by only one person, our reservations manager.
Page 8, paragraph 1. Cancellation and refund policies and processes are documented.

We concur with the audit recommendations, with one revision.

1. We have already removed unnecessary accounts and have made it the responsibility of the reservations manager to review the accounts on the first day of each month to ensure that all necessary changes have been made.

By June 30, we will review the current user groups, determine the levels of access needed by each, and make necessary changes.

2.We have already forced new passwords and implemented a policy (with written documentation) to use undetectable pass phrases. Passwords will be automatically prompted for change every 6 months.

3. The modifications to our user groups will ensure that the ability to process refunds is

SMITHSONIAN INSTITUTION
Ripley Center Suite 3077
1100 Jefferson Avenue SW
Washington DC 20560-0701
202.357.2696 Telephone
202.633.8909 Fax
mayorma@tsa.si.edu E-mail

WRITTEN COMMENTS BY THE DIRECTOR, THE SMITHSONIAN ASSOCIATES

limited to a designated user group. However, we must maintain the ability to process refunds after the prohibited refund date. While we adhere in most cases to the cancellation policy, there may be exceptions, and we must have flexibility in processing refunds. We can modify the recommendation so that only the reservations manager has the ability to process a refund after that prohibited refund date, and that only with approval from the Study Tour Manager. Additionally, we will close out tours when final accounting has taken place, so that no subsequent financial transactions can take place. These changes will be in place, with written instructions to staff, by June 30.

Finding C: Reservations System Contracting
We concur with the audit recommendations.

During the month of June, we will determine our needs for a support contract for Select software maintenance and development, and by June 30, we will meet with OCon to request their assistance in writing the contract. Actual production of the contract will depend on OCon's schedule and their ability to take on our project. As part of the contract, we will require that the Select consultant produce system documentation, including changes. The contract will also include a change and configuration process for future modifications.

Finding D: Patron Data Protection
Clarification:
Page 12, results of review: In May, 2002, we changed our shopping cart software, and the process to decrypt and save web orders in Word no longer exists. With the new software, all orders are stored on a secure server, and only users with a user word and password for this server are permitted access to the orders.

We concur with the audit recommendations.

As of May 15, 2002, TSA has begun to implement office procedures for the secure storage of electronic and hard copy form of patron data. We issued both desk and file cabinet keys to appropriate reservation coordinators and gave them written directions that all files and tour applications, plus correspondence giving patron data, are to be locked up when the office is closed.

We will review our existing web order procedures to eliminate unnecessary distribution of patron data. As part of our review, we will determine if it is necessary to keep paper and/or electronic records of orders, and eliminate duplication where possible.

The target date for completion and documentation of these changes is July 31, 2002.

SMITHSONIAN INSTITUTION
Ripley Center Suite 3077
1100 Jefferson Avenue SW
Washington DC 20560-0701
202.357.2696 Telephone
202.633.8909 Fax
mayorma@tsa.si.edu E-mail

WRITTEN COMMENTS BY THE DIRECTOR, THE SMITHSONIAN ASSOCIATES

Finding E: Study Tours Solicitations

Clarification: There is some misunderstanding about our agreements with companies that lease TSA names. All requests to rent our names come through two list rental companies with which we work – Trinity Direct and MSGI. When we agree to a proposed lease or exchange, the list rental company sends an agreement to the third party purchaser that clearly spells out the limits of use, including the fact that this is a one-time usage and that the list cannot be duplicated or retained. A copy of the standard agreement for each such order is attached. TSA does not work directly with any third party in the leasing of TSA names.

There is also a misunderstanding with regard to sending e-mails about upcoming programs. We create "e-flyers" that are sent only to our own names. The software we use is a product provided by a company called Enspot Entertainment. It is analogous to using any software program. The company updates the software, but we actually use it. The agreement with Enspot makes it absolutely clear that our list is confidential information, and exclusively for our use. It states they "will not compile, buy, sell, rent or trade Client's E-mail list(s), or send unauthorized E-mail to Client's list." A copy of a standard agreement is attached.

With regard to the recommendations:

1. TSA agrees that patrons should be given the choice of whether their information is used for marketing purposes by third parties. To accomplish this, we will review all materials we use for marketing to be sure that a check-off is included for use of an individual's name by third parties. We will complete the review by August 30, 2002 and implement needed changes as pieces are subsequently printed.

However, we strongly disagree with the recommendation that individuals should give us approval before we can contact them with information about our own programs. It is a conclusion that is not supported by the materials described in the background and results sections of this part of the audit, and to leap to such an inference would be hugely damaging to TSA. Acquiring names is a basic function of marketing. We try to find as many people as possible who are prospects – that is, who express interest in learning more about our programs. Once an individual becomes a prospect for study tours, for example, we must be able to send them information about upcoming programs of all sorts. Typically it takes 18 months and a good number of mailings before a prospect finds just the right tour, and actually enrolls. Maintaining and mining our own mailing list is essential to our financial health.

2. With regard to the second recommendation, each transaction that involves the rental of our list to a third party is already formalized by an agreement that includes pricing and

SMITHSONIAN INSTITUTION
Ripley Center Suite 3077
1100 Jefferson Avenue SW
Washington DC 20560-0701
202.357.2696 Telephone
202.633.8909 Fax
mayorma@tsa.si.edu E-mail

WRITTEN COMMENTS BY THE DIRECTOR, THE SMITHSONIAN ASSOCIATES

usage restrictions.

In the case of e-flyers, there is no third party involved using our list, and the software company, Enspot Entertainment, specifically agrees, in writing with each use, to the restrictions noted above.

SMITHSONIAN INSTITUTION
Ripley Center Suite 3077
1100 Jefferson Avenue SW
Washington DC 20560-0701
202.357.2696 Telephone
202.633.8909 Fax
mayorma@tsa.si.edu E-mail

WRITTEN COMMENTS BY THE DIRECTOR, THE SMITHSONIAN ASSOCIATES

[illegible] This purchase order confirmation copy provides instructions for the proper execution by the owner/manager or broker/mailer [illegible] as terms mutually acceptable to all parties in this transaction.
If the instructions are revised in any way or the terms are not acceptable to either the mailer or owner, please contact MKTG Services immediately, and confirm in writing.

PROVIDE U.S. names only. Omit APO, FPO, military, foreign, Canada, and Puerto Rico, unless otherwise stated.

AVOID DUPLICATION: Keep a record of the names used to avoid duplication on future mailings to this list.

ALL NAMES must be sid-4 coded and in zip sequence at no charge. Postal coded for Canada.

PROVIDE STATE COUNTS with shipment at no charge.

ATTENTION LIST/PACKAGE OWNER:
Please forward written acknowledgment of this purchase order (not applicable for management orders) prior to return date, or terms indicated will be deemed approved.
If written confirmation cannot be provided, a copy of our purchase order with authorized signature is also acceptable.
On package insert orders please provide samples of the mailer's and other accompanying inserts.
Brokerage Division: We will invoice the mailer on behalf of the list or package owner.
Management Division: We will invoice the broker/mailer on behalf of the list or package owner.
Both divisions: Upon receipt of payment, remit promptly. We act only as agents of the list/package owner and do not guarantee payment from the mailer.

ATTENTION/LIST PACKAGE USER:
All orders are subject to final approval of list/package owner. List owner will not be held liable for any damage resulting from [illegible] delays in delivery.
Please forward acknowledgement of this purchase order (not applicable for management orders). If order is on a net name basis, please provide [illegible] so proper invoicing can be executed.
Cancellations or order revisions before mail date are subject to work-in-process charges.
Decoy names are added to monitor usage.
Please remit payment within 30 days of mail/insert date to the following:

MKTG SERVICES
P.O. BOX 34043
NEWARK, NJ 07189-0043

We believe the information stated to be accurate, but neither the list/package owner nor MKTG Services can guarantee the outcome of the mailing.
All list rentals are FOB point of origin.
Magnetic tapes are to be returned, where applicable, to point of origin at mailer's expense.
In addition to any other payment required hereunder, the mailer will bear the burden of all sales and use or similar taxes as may be imposed with respect to the transactions hereunder.
Mailer shall pay all expenses incurred for the enforcement of terms and conditions of orders, including, but not limited to, cost of collection, litigation and reasonable attorney's fees.

MAILER GUARANTEE:
Mailer will provide sample mailing piece for list/package owner approval. On continuation orders, if previously approved mailing piece is different, mailer must provide sample mailing piece for list owner approval.
Mailer agrees not to disclose, transfer, duplicate, retain, resell or reuse all or any portion of the list in any form or manner, nor permit any third party, agent, employee or contractor and their respective agents and employees to do so, without prior written approval from the list owner.
Except for the mailing specified, the mailer agrees not to telephone or otherwise contact persons named on the list or at the address for any reason, or disclose the source of the list or identify the list owner in any manner without prior written approval from the list owner.
Mailer and/or its service organizations agree not to use any method to detect, alter or eliminate decoy names from rented list.
Mailer agrees that these names are to be used one time only as specified for the offer and on the date indicated, unless otherwise stated.
Mailer may be subject to full rental charges if order is cancelled after names are put into merge.
Mailer guarantees full payment if cancelled after mail date.
Package user guarantees not to cancel with less than 90 days notice from materials due date, or full payment will be made.

LIST/PACKAGE OWNER GUARANTEE:
List owner will provide mailer one week protection before and after mail date from all competitive mailers using this list, unless otherwise stated.
List owner will not charge for previously supplied names, intra-file dupes, edit drops, and pandered names, unless otherwise stated.
On continuation orders, please advise MKTG Services if list owner's media mix or product line has changed since previous order.
Package owner will give package user right of first refusal for this offer in subsequent packages during the same distribution period. Package owner will not include competitive offers in same package.

WRITTEN COMMENTS BY THE DIRECTOR, THE SMITHSONIAN ASSOCIATES

EnFlyer!™ Service Agreement

Please fax the completed agreement to your sales agent.

Client/Billing/Setup Contact

Contact: Bob Anastasio
Title: Director of Marketing
Company: Smithsonian Institute
Address: 1401 900 Jefferson Drive, SW
City/St/ZIP: Washington, DC 20560-0413
E-mail: anastro@tsa.si.edu

Phone: (202) 786-3246
Fax: (202) ~~357-2586~~ 786-2536
#Licenses: 1

Office Use Only
Agent ID: Louis Wing

Payment Method: [ ] Check [ ] Charge (Please complete Charge Authorization Section)

Charge Authorization: I authorize EnFlyer to charge my charge card for the EnFlyer Services as agreed to on this Agreement.

Card Type: [ ] Visa [ ] Master Card [ ] AmEx
~~Name on Card~~: #12303
~~Card Number~~: PURCHASE ORDER #
Exp Date: _____
Card Verification Value*: _____
* A three-digit value printed in the signature panel on the back of most credit cards immediately following the credit card account number

EnFlyer Support: Phone: 305-643-6776, Fax: 305-675-0948, E-mail: Support@EnFlyer.com

Terms and Conditions

Whereas Client requires EnFlyer Services, and whereas EnSpot.com, Inc., ("EnFlyer") is willing to provide said services upon the following terms, the parties agree as follows:

EnFlyer License: EnFlyer shall provide Client with use of EnFlyer. Client shall pay to EnFlyer the Setup and Monthly Service fees per license as set forth below, as well as any fees related to additional Service Orders requested by Client. Setup fees are invoiced upon receipt of this agreement by EnFlyer. Monthly service fees shall begin upon receipt of this agreement by EnFlyer (Effective Date) and are invoiced in arrears for the previous calendar month. All fees shall be due and payable at the offices of EnFlyer upon receipt of invoice. Client's use of EnFlyer shall be deemed to be Clients agreement to the Terms of Service, available at EnFlyer.com. Fees are based on a single license per location. All services shall be deemed to have been provided at the offices of EnFlyer.

One Time Setup Fee: $299 (includes account setup, custom database setup, 500 Customer Cards including data entry, and 1 hour training session).

Monthly Service Fee: Based on number of E-mails in Client's E-mail list for the corresponding month: 0-2000 E-mails = $99 Fee; 2001-10000 E-mails = $199 Fee; 10001-25000 E-mails = $299 Fee; Each Add'l 25,000 E-mails = $250 Fee

Term: 12 Months, automatically renewable unless cancelled in writing prior to start of new term.

90-Day Cancellation Guarantee: We are 100% confident that EnFlyer will produce results. Try it for up to 90 days. If EnFlyer does not produce results, Client may cancel this agreement by giving written notice to EnFlyer within the first 90 days of the Effective Date with no additional obligation. Client must include reason for cancellation on notice.

Additional Service Orders: Client may request EnFlyer to perform additional services for an additional fee. Please see rate card for current services and prices. All Service Orders between EnFlyer and Client shall be accomplished electronically and client shall be bound by those orders.

Client's List is Confidential

Client's E-mail list(s) will be held by EnFlyer as confidential information to be used exclusively by Client for the benefit of Client. EnFlyer will not compile, buy, sell, rent, or trade Client's E-mail list(s), or send unauthorized E-mail to client's list.

EnSpot may include the following on each EnFlyer - Unsubscribe information and procedures, forwarding and contest information, EnFlyer service statement & link, and Copyright information.

Warranty and Liability – Client warrants that it owns, has the right to use and the right to authorize EnFlyer's use of the material (lists, images, sounds, copy) provided to EnFlyer, and that all e-mails on the lists are acquired by Client using legal means and are opt-in only. Client specifically agrees not to use EnFlyer for the purpose of "Spamming" e-mail addresses. Client shall indemnify and hold EnFlyer harmless from any liability or loss incurred for breach of this warranty. Client specifically agrees that EnFlyer's sole and exclusive liability hereunder is to re-perform any non-performed services or, at EnFlyer's option, refund the amount paid by Client for the non-performed service. EnFlyer reserves the right to cancel this agreement at any time by giving written notice to Client via E-mail.

Non-Payment: Any fees not paid within 30 days of invoice shall result in denial of access to EnFlyer until paid in full. The prevailing party in any collection/dispute shall be entitled to recover its reasonable professional fees and costs.

By completing this EnFlyer Agreement and sending it to EnFlyer, you represent that you are authorized to enter into binding agreements on behalf of your company and are now completing such a binding agreement. Facsimile signatures shall be binding. This agreement constitutes the entire agreement between the parties and all other additional or contrary documents, or representations, written or oral, are hereby rejected and shall not be binding upon the parties.

Client
Signature: Robert Anastasio
Name: ROBERT ANASTASIO
Title: DIRECTOR OF MARKETING
Date: 9/24/01

EnFlyer
Signature: _____
Name: Kenneth Arnold
Title: Sales Manager
Date: 9/24/01