

DECEMBER 7, 2010

AUDIT REPORT

OFFICE OF AUDITS

PREPARING FOR THE SPACE SHUTTLE
PROGRAM'S RETIREMENT:
A REVIEW OF NASA'S DISPOSITION OF INFORMATION
TECHNOLOGY EQUIPMENT

OFFICE OF INSPECTOR GENERAL



National Aeronautics and
Space Administration

Final report released by:

A handwritten signature in black ink, appearing to read 'PKMJA'.

Paul K. Martin
Inspector General

Acronyms

CIO	Chief Information Officer
DOD	Department of Defense
FY	Fiscal Year
IT	Information Technology
ITAR	International Traffic in Arms Regulations
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
ODIN	Outsourcing Desktop Initiative for NASA
OIG	Office of Inspector General
USA	United Space Alliance

OVERVIEW

PREPARING FOR THE SPACE SHUTTLE PROGRAM'S RETIREMENT: A REVIEW OF NASA'S DISPOSITION OF INFORMATION TECHNOLOGY EQUIPMENT

The Issue

After 38 years and more than 130 missions, the Space Shuttle Program is nearing retirement and therefore the disposition of Program equipment, including the Shuttles themselves, spare parts, and processing and information technology (IT) equipment, poses a significant challenge. Given the scope of these activities, the NASA Office of Inspector General (OIG) is reviewing NASA's controls over the disposition of Program property. This report focuses on the disposition of Shuttle-related IT equipment, much of which contains sensitive information regarding Space Shuttle operations and maintenance procedures.¹

NASA requires the sanitization of any electronic storage media that has ever contained NASA information before it is reassigned, transferred, or discarded.² Sanitization is the process of removing data from media and may involve the overwriting, degaussing, or destruction of the media so that it is impossible or nearly impossible to recover the data previously stored there.³ In addition, NASA requires testing to verify that sanitization procedures are effective by periodically attempting to access and recover information from IT equipment that has been sanitized.⁴

During our audit, we discovered significant weaknesses in the sanitization and disposal processes for IT equipment at four NASA Centers – Kennedy and Johnson Space Centers and Ames and Langley Research Centers. Because of the criticality and time-sensitive

¹ Sensitive information is information that requires protection due to the risk and magnitude of the harm or loss that could result from unauthorized release. Sensitive information includes, but is not limited to, personally identifiable information and export-controlled information.

² NASA Procedural Requirements (NPR) 2810.1A, "Security of Information Technology," May 16, 2006, Section I, "NASA IT Security Program."

³ Degaussing is the process by which magnetic media is demagnetized, thereby deleting the information stored on the media.

⁴ NASA Standard Operating Procedure, ITS-SOP-0035, "Digital Media Sanitization," September 15, 2008.

nature of these issues, we immediately brought them to the attention of NASA managers.⁵ In addition, we are reporting on these IT findings apart from our broader review of the disposition of all Shuttle-related property. We will report our findings on the disposition of other types of Shuttle property when we complete our audit work.

Results

We found significant weaknesses in the sanitization and disposition processes at each of the four Centers we reviewed. For example, we found that Kennedy managers were not notified when computers failed sanitization verification testing; that no verification testing was being performed at Johnson or Ames; and that Kennedy, Johnson, and Ames were using unapproved sanitization software. We also found that while hard drives are destroyed at Langley before computers are released to the public, personnel did not properly account for or track the removed hard drives during the destruction process. In addition, we found computers at the Kennedy disposal facility that were being prepared for sale on which NASA Internet Protocol information was prominently displayed. Internet Protocol information could provide a hacker with the details needed to target specific NASA network assets and exploit weaknesses, resulting in the compromise of sensitive information.

Figure 1. IT Equipment Confiscated by OIG Personnel from Kennedy’s Property Disposal Facility



Source: OIG photograph (June 11, 2010)

We found that some of these weaknesses had resulted in the inappropriate release of NASA data. Specifically, Kennedy released to the public 10 computers that had failed verification testing and therefore still contained NASA data. We confiscated four other computers (pictured in Figure 1) that had also failed the testing but were still being prepared for release or sale from the Kennedy Reutilization, Recycling, and Marketing Facility (property disposal facility). When we tested the confiscated computers, we

⁵ The issues we identified at Kennedy required immediate attention. Accordingly, when we advised Kennedy personnel of our findings, they established a “Tiger Team” to review the disposition process and took immediate action to prevent unauthorized releases.

discovered that one contained data subject to export control by the International Traffic in Arms Regulations (ITAR).⁶

Inadequate Oversight of Center-Level IT Sanitization Process. We attribute these deficiencies to the fact that NASA management did not adequately oversee the media sanitization process at the four Centers we visited. Specifically, we found that:

- appropriate Center or contractor personnel were not notified when computers failed sanitization testing,
- IT equipment was not properly accounted for or tracked during the disposition process, and
- excess computers awaiting final disposition contained external markings that included NASA Internet Protocol information.

Three of the Centers we visited used software to sanitize excess IT equipment, but only Kennedy had implemented a process to verify the effectiveness of its sanitization procedures as required by NASA policy. Kennedy's verification process called for an independent contractor to test samples of excess IT equipment awaiting disposal at Kennedy's property disposal facility. Between June 2009 and June 2010, the contractor tested 730 pieces of excess IT equipment and identified 14 computers that still contained Agency data. In accordance with the Kennedy verification process, the contractor labeled the failed computers and returned them to the property disposal facility. Although the contractor reported the failures to the contracting officer's technical representative, no one informed the original owner of the equipment or personnel at the property disposal facility of the failures. Moreover, despite clear markings indicating that the computers had failed verification testing, no one took action to remove the remaining data from the computers or to prevent their sale.

We attempted to determine the Agency's risk exposure from the sale of the ten computers. We concluded that nine of the computers had been released for disposition by two NASA contractors.⁷ One of the contractors provides base operations support for Kennedy and the other works on several NASA programs that involve sensitive space-related technologies. Although we could not definitively determine whether the nine computers that were sold actually contained sensitive information, our analysis of the computers we confiscated – one of which contained information subject to export control by ITAR – and the type of work performed by these contractors raises serious concerns about the information that may have remained on the computers.

⁶ ITAR governs the export of defense-related material and includes Space Shuttle-related technology. The regulation makes it unlawful to share such technology with anyone except a U.S. person unless a license and approval is obtained from the Department of State. ITAR violations can result in a fine, imprisonment, or both.

⁷ We determined that the other computer posed little risk because it had been used at a kiosk at Kennedy's visitor center to provide general information to the public.

In addition, we found a lack of accountability for excess hard drives at two of the four Centers. Most concerning was the discovery at Kennedy of hard drives, removed from excess computers, stored in an unsecured dumpster accessible to the public. We also found that Langley did not properly account for or track hard drives that had been removed from excess computers. Specifically, we identified control weaknesses that could allow Langley personnel to remove hard drives from excess computers without complying with procedures intended to track and account for the drives.

We also found several pallets of computers (approximately 44 computers per pallet) at Kennedy's property disposal facility prepared for sale that contained external markings with NASA Internet Protocol addresses. Releasing an Internet Protocol address outside of NASA's custody is a potential IT security weakness that could enable unauthorized access to NASA's internal computer network.

Inadequacies in NASA Policy. IT management personnel at Kennedy, Johnson, and Ames did not ensure the proper sanitization of excess IT equipment before releasing it from NASA custody in part because NASA's existing policies are inadequate. For example, NASA's policies require verification testing to ensure that sanitization processes are effective. However, the policies do not include specific guidance regarding how and when such testing should be conducted.

Failure to Comply with NASA Policy. IT and property management personnel at Kennedy, Johnson, and Ames were not complying and were unfamiliar with NASA sanitization policy. For example, we found that the primary Space Shuttle Program contractor at Kennedy, United Space Alliance (USA), was using unapproved software to sanitize its IT equipment. In addition, officials at Johnson and Ames had no verification testing process in place as required by NASA policy.

The weaknesses we identified in NASA's IT sanitization policy and procedures put NASA at risk of releasing sensitive information that could cause harm to its mission and violate Federal laws and regulations that protect such information. Accordingly, we recommended that NASA take the steps outlined below.

Management Action

We acknowledge the swift actions taken at Kennedy in response to the issues we raised with Center management during our audit. However, because we found weaknesses in the sanitization and disposition processes for IT equipment at the three other Centers we visited, we recommended that NASA's Chief Information Officer (CIO) initiate a review of sanitization procedures at all Centers to identify deficiencies, take corrective actions, and share best practices. In addition, we recommended that the CIO coordinate with the Assistant Administrator for Strategic Infrastructure to ensure that Center property disposal offices have the requisite knowledge to ensure that excess IT equipment has been adequately sanitized before it is released to the public. We also recommended that the

CIO revise NASA's IT disposition policy to include a sampling methodology for verifying sanitization of equipment, identify an acceptable risk level, and specify the percentage of equipment and frequency of testing needed to achieve the specified risk level.⁸ In addition, we recommended that the Centers be required to document their sampling methodology, identify responsible officials in writing, and maintain testing records and results.

In response to our recommendations, the CIO stated that NASA's policies would be updated and a new handbook created by the third quarter of fiscal year 2011 (see Appendix C). However, overall we do not consider the proposed actions to be responsive to our recommendations. Moreover, we are troubled that management's response does not reflect the sense of urgency we believe is required to address the serious security issues uncovered by our audit. Accordingly, we consider the recommendations to be unresolved.

With respect to our recommendation to initiate a review of sanitization procedures at the Centers, the CIO stated that she would initiate a review of the procedures and issue a new handbook to replace existing policy. She asserted that the process of drafting this handbook would lead to the identification of deficiencies in current policy and procedures. The CIO also stated that NASA's Office of Strategic Infrastructure could use the revised policy to amend existing contracts to compel contractor compliance with new Agency policy and include these requirements in all new contracts with vendors who conduct media sanitization.

In our judgment, the CIO's proposed actions do not address our concern that there may be unidentified weaknesses at Centers that were not part of our audit. Given what we found at the four Centers we visited, we believe that identifying weaknesses in sanitization procedures requires conducting on-site reviews of the processes and procedures the Centers are using to sanitize IT equipment. In our judgment, simply reviewing policy and procedures and then drafting a handbook will not be adequate to identify and correct potential serious deficiencies at the Centers.

In response to our recommendation to coordinate with the Assistant Administrator for Strategic Infrastructure to ensure that Center property disposal personnel have the requisite knowledge to ensure that excess IT equipment has been adequately sanitized before being released to the public, the CIO again stated that NASA policy would be updated after which existing contracts would be amended. For its part, the Office of Strategic Infrastructure nonconcurred with the recommendation, stating that property disposal personnel are not responsible for ensuring adequate sanitization of equipment and in any event lack the expertise to do so.

⁸ Office of Management and Budget Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources," describes adequate security as security commensurate with risk. This risk includes both the likelihood of occurrence and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

We find management's response to this recommendation to be inadequate. First, revising policy does not necessarily equate to coordination between the two offices. Second, although we agree that property disposal personnel are not responsible for actually sanitizing equipment or ensuring that the sanitization process used is adequate, they are responsible for ensuring that policy and procedures are followed to ensure that, for example, IT equipment marked "fail" as shown in Figure 1 is not prepared for sale or released to the public.

In response to our recommendations to revise disposition policy to include a sampling methodology for verifying sanitization of equipment, identify an acceptable risk level, and specify the percentage of equipment and frequency of testing needed to achieve that risk level, the CIO agreed to take all recommended steps except for developing a sampling methodology. She stated that a sampling methodology is neither required by the guidance cited in our audit nor cost-effective for NASA.

While the guidance we cited does not explicitly require a sampling methodology, in our judgment establishing a sampling methodology is not only prudent but a recognized best practice. NASA policy already requires periodic testing (*see* Standard Operating Procedure, ITS-SOP-0035, "Digital Media Sanitization," September 15, 2008), and other agencies have incorporated a sampling methodology in their procedures (*see* Department of Defense Memorandum, "Disposition of Unclassified DoD Computer Hard Drives," June 4, 2001). In addition, when we contacted National Institute of Standards and Technology (NIST) personnel, they confirmed that a minimum sample size for sanitization verification should be 20 percent of total excess IT equipment. In light of our finding that the Agency's current procedures failed to prevent the disposal of IT equipment containing sensitive information, we continue to urge NASA to develop a sampling methodology that conforms to the 20 percent standard recommended by NIST.

CONTENTS

INTRODUCTION

Background	1
Objectives	4

RESULTS

NASA Did Not Ensure that Excess Information Technology Equipment Was Properly Sanitized	5
--	---

APPENDIX A

Scope and Methodology	17
Review of Internal Controls	19
Prior Coverage	20

APPENDIX B

NASA Policy and Best Practice Guidance	21
--	----

APPENDIX C

Management Comments	23
---------------------	----

APPENDIX D

Report Distribution	27
---------------------	----

INTRODUCTION

Background

NASA's Space Shuttle Program transition and retirement effort is clearing the path for the future of spaceflight while preserving the legacy of one of the most successful human spaceflight programs in history. The transition and retirement activities are extensive and one of the largest such efforts the Agency has ever undertaken. In addition to the Shuttles themselves, the disposition of information technology (IT) equipment is a significant component of the Space Shuttle Program retirement effort. United Space Alliance (USA), the prime Space Shuttle contractor, expects a "bow wave" of computers needing disposition beginning in late 2010.

Much of Shuttle-related property is located at and will be disposed of by personnel at Kennedy and Johnson Space Centers. Accordingly, we initiated and conducted most of our work at those two Centers. However, after we uncovered significant issues relating to the disposition of IT equipment at those Centers, we expanded our work to include a limited review of the disposition procedures in use at Ames and Langley Research Centers for IT equipment in an effort to determine the scope of the problem.⁹

NASA requires all electronic storage media that has ever contained NASA information to undergo a sanitization process before it is reassigned, transferred, or discarded.¹⁰ Sanitization is the process of removing data from the media to the degree that there is reasonable assurance that the data cannot be retrieved or reconstructed.¹¹ NASA requires the use of one of three approved software products to sanitize IT equipment: Secure Erase, Darik's Boot and Nuke (DBAN), and WipeDrive/WipeDrive Pro.¹² In addition,

⁹ Contractors that are located on or near NASA Centers frequently use the disposition procedures in place at the Center to dispose of their Government-furnished IT equipment. Consequently, we also reviewed the sanitization procedures in place at several of these contractors whose IT equipment was likely to contain Space Shuttle Program data, including USA and Lockheed Martin's Outsourcing Desktop Initiative for NASA (ODIN).

¹⁰ NASA Standard Operating Procedure, ITS-SOP-0035, "Digital Media Sanitization," September 15, 2008.

¹¹ Sanitization methods include overwriting or wiping, degaussing (the process of demagnetizing magnetic media), and destruction of the storage media.

¹² NPR 1400.1D "NASA Directives Procedural Requirements, with Change 5," February 18, 2007, allows the responsible Headquarters office for the Agency-level directive to waive requirements contained in its directives. None of the Centers or contractors we visited had requested or received such a waiver relating to sanitization software.

NASA requires verification testing of equipment that has been sanitized to ensure that sanitization procedures are effective.^{13,14}

NPR 4300.1A, “NASA Personal Property Disposal Procedural Requirements (Revalidated 2/17/06 with Change 1),” provides guidance for the utilization and disposal management of NASA-owned excess, surplus, and exchange/sale property, including IT equipment. NASA’s Logistics Division, within the Office of Strategic Infrastructure, has the Agency-level responsibility to ensure Centers comply with the Agency policy. The NPR states that the Center Director is the official responsible for appointing a Property Disposal Officer to ensure the proper use, transfer, sale, or other disposition of NASA personal property. The NPR encourages NASA Centers to customize disposal management procedures to meet local requirements. Accordingly, disposal policies and procedures vary among NASA Centers. The following sections summarize disposition procedures at the four Centers we visited.

IT Disposition Process at Kennedy. During the course of the audit, we noted that Kennedy did not have a Center-specific written policy covering the IT equipment disposition process, but rather generally followed applicable NASA directives.¹⁵ At Kennedy, property users are responsible for sanitizing excess IT equipment before sending it to the Center’s Reutilization, Recycling, and Marketing Facility (property disposal facility). Depending on the user, sanitization is accomplished using various software products, not all of which have been approved by NASA. A contractor, Abacus Technology Corporation, conducts verification testing of users’ sanitization efforts. Property disposal personnel periodically select and deliver to Abacus computers that have undergone sanitization. Abacus then attempts to recover data from these computers to test the effectiveness of the sanitization process. If Abacus personnel are able to recover data from a “sanitized” computer, they attach a label to the outside of the computer with the word “fail” written in large letters with red ink. Abacus returns all computers it tests, including those that have failed, to the property disposal facility. Other than affixing the “fail” label to the equipment, Abacus was not required to and did not notify either the property users or disposal personnel about computers that had failed its testing procedures.

¹³ Verification involves periodically attempting to access and recover information from a sample of IT equipment that has undergone sanitization.

¹⁴ NASA’s Standard Operating Procedure incorporates practices set forth in National Institute of Standards and Technology (NIST) Special Publication 800-88, “Guidelines for Media Sanitization,” September 2006, and Department of Defense (DOD) “National Industrial Security Program Operating Manual” (NISPO), 5220.22-M, February 28, 2006, although the Procedure incorrectly referenced it as “DOD 5520.22-M.” According to NIST, organizations should sanitize IT equipment using approved software, techniques, and procedures, as well as track, document, and verify IT equipment sanitization and destruction actions and periodically test sanitization equipment and procedures.

¹⁵ However, on October 13, 2010, Kennedy issued disposition policy, “Personal Property Transfer/Excess Process” (KDP-KSC-P-3716).

IT Disposition Process at Johnson. Johnson has a Center-specific disposal policy, requiring that computers, disk drives, servers, and related IT equipment be wiped (sanitized) of all stored memory data to ensure no sensitive or privacy information remains (Work Instruction 4300.1, “JSC [Johnson Space Center] Instructions for Excess and Disposal of Government Property,” September 28, 2009).¹⁶ Depending on the type of property, a user electronically notifies the appropriate property custodian through NASA’s property database system that they have excess IT equipment or the user completes Form JF 25A, “Request for Turn-In or Issue of Excess Property.” Property custodians ensure that the request includes all required information and indicate approval of the disposition request by placing a label on the equipment indicating that it is excess. While the Property Disposal Officer manages the final disposal function, the property user may wipe the equipment prior to delivering it to the Property Disposal Officer. In such instances, the user is supposed to tag the computer as having been wiped. Equipment that has been wiped by the user is not re-wiped or otherwise tested by disposal warehouse personnel.

IT Disposition Process at Ames. Ames has a Center-specific IT disposal policy that requires sanitizing all internal hard drives and storage devices before disposal or removal (Ames Procedural Requirements 2815.1, “Excessing Government Owned Computer,” July 26, 2010). At Ames, the user of the IT equipment initiates a request to the appropriate system administrator to have the equipment sanitized and then requests that the responsible Center property custodian dispose of the sanitized equipment. The policy states that system administrators are to overwrite data using DOD-compliant sanitizing software and provide the property custodian with the date the overwriting was performed, the name of the sanitization software used, and the name of the system administrator who performed the overwrite. The property custodian collects all of the information required for disposal and validates that the information regarding sanitization is correct before sending the equipment to the Property Disposal Officer. The Property Disposal Officer validates that the appropriate disposal documents are submitted and complete and stores the equipment until final disposition. In addition, IT Security Operations personnel are required to conduct random reviews of excess computers to ensure they are clear of NASA-related information, and Protective Services Office and Information Technologies Security Office personnel are required to perform periodic audits of the process and conduct joint investigations of compliance irregularities. However, these offices have not performed a review or audit in the past 2 years.

IT Disposition Process at Langley. Langley sanitizes excess computers by removing their hard drives. Tessada & Associates, Inc., a support contractor, processes the Center’s excess computers according to the contractor’s Procedure No. 4.5.2-1, “Processing Computer Equipment for Donation,” April 1, 2002. The procedure requires that a computer technician remove the hard drives from computers submitted for disposition

¹⁶ Sensitive information is information that requires protection due to the risk and magnitude of the harm or loss that could result from unauthorized release. Sensitive information includes, but is not limited to, personally identifiable information and export-controlled information.

and transport the hard drives to the “steam plant” for destruction via incineration. The procedure also requires that the computer technician maintain a daily production log, which serves as a record of computers from which hard drives have been removed. However, no log is maintained of the hard drives delivered to the steam plant or of the verification of their destruction.

The following table summarizes the disposition procedures in place at the four Centers we visited.

Summary of Disposition Procedures at Four NASA Centers			
<u>Center</u>	<u>Center-Specific Policy</u>	<u>Sanitization Software</u>	<u>Verification Process</u>
Kennedy	no ¹	unapproved ²	yes
Johnson	yes	unapproved ²	no
Ames	yes	unapproved ²	no
Langley	yes	not applicable	not applicable

¹ Prior to release of this report, Kennedy issued “Personal Property Transfer/Excess Process,” (KDP-KSP-P-3716) on October 13, 2010.

² We identified specific instances in which unapproved software was used. This does not mean that all sanitization at the Center was done with unapproved software.

Objectives

This report stems from a larger audit examining NASA’s controls over the disposition of various types of Space Shuttle Program property as the Program nears retirement. Our overall objective is to determine whether NASA has implemented effective controls over property disposition. During the course of our audit, we discovered weaknesses in NASA’s process for the disposition of IT equipment that required immediate corrective action by NASA management. Accordingly, we promptly notified management of these weaknesses and are providing this separate report concerning our IT-related findings. We will provide a report on our audit results relating to the disposition of other types of Shuttle-related property when we have completed the remainder of our audit work. We also reviewed internal controls related to the audit objective. See Appendix A for details of the audit’s scope and methodology, our review of internal controls, and a list of prior coverage.

NASA DID NOT ENSURE THAT EXCESS INFORMATION TECHNOLOGY EQUIPMENT WAS PROPERLY SANITIZED

We found that when disposing of excess information technology (IT) equipment, NASA did not consistently protect sensitive information from unauthorized release. This occurred because NASA managers are not adequately overseeing sanitization and disposition processes, NASA's sanitization policies are incomplete, and responsible personnel did not consistently follow or were unaware of applicable policy.

NASA Policy and Industry Best Practices

NASA has developed policies to protect information from unauthorized disclosure, destruction, or modification while the information is being collected, processed, transmitted, stored, or disseminated. The Office of the Chief Information Officer, which is responsible for unclassified information, and the Office of Protective Services, which is responsible for classified information, share responsibility for Agency information security. In addition, the National Institute of Standards and Technology (NIST) and the Department of Defense (DOD) have published industry guidelines specific to the sanitization of IT equipment. See Appendix B for a listing of applicable sanitization policies.

NASA Is Not Properly Sanitizing IT Equipment

NASA did not ensure the proper sanitization of excess IT equipment before releasing it outside of Agency control. Three of the four Centers we reviewed were using software to sanitize equipment prior to disposition, and we found that only Kennedy had a verification testing process in place as required by NASA policy.¹⁷ However, we discovered several flaws in Kennedy's verification process that resulted in the release or near release of 14 computers that had failed verification testing to ensure the machines did not contain sensitive information.

Between June 2009 and June 2010, Kennedy contractor personnel tested 730 pieces of IT equipment to verify proper sanitization. Fourteen of these pieces of IT equipment, were computers that failed testing, indicating that they still contained NASA data. Ten of the failed computers were sold to the public with no further remedial action having been

¹⁷ Such testing was not required at Langley because at that Center hard drives were removed from computers before they were dispositioned.

taken to ensure that all NASA data had been removed. We confiscated the four other computers during our audit before they could be sold. When we examined these four computers, we discovered that one contained Space Shuttle-related technology subject to export control by the International Traffic in Arms Regulations (ITAR).¹⁸ Another computer's hard drive had been removed after undergoing sanitization testing, but was not accounted for. The remaining two computers contained corrupted and unreadable data.¹⁹

We were not able to retrieve the hard drives of the ten computers that were sold to the public after failing verification testing. Accordingly, we could not definitively determine whether they contained sensitive information. However, we were able to determine where at Kennedy the computers had been used before being excessed. One of the computers was used by visitors at a public kiosk in the Kennedy visitor center and therefore was unlikely to have contained sensitive data. The other nine computers had been dispositioned by contractors that either provide base operations support for Kennedy or are involved with NASA programs that involve sensitive space-related technologies. We interviewed the contractor personnel who excessed the nine computers, and they told us that before sending five of the nine to the disposition facility, they removed and replaced their original hard drives. Nevertheless, because sanitization testing indicated that the computers still contained some NASA data, we are concerned about the information that may have remained on the computers.²⁰

Notification of Failed Computers. We determined that Kennedy did not have a process in place to notify IT security officials or the property user when a computer failed sanitization testing. As noted earlier, Abacus performs the verification testing and places a failed label on the outside of any computer that does not pass its testing procedures. Abacus returns all the computers it tests, including those that have failed, to Kennedy's property disposal facility and, apart from affixing the label to the computer, does not notify either the property users or IT security personnel of any failures. USA's Director of IT informed us that USA was last notified of a failed computer 7 years ago. The Kennedy IT Security Manager also confirmed that he had not been notified of any failed computers recently.

In May 2010, we examined a pallet of 49 computers that had been delivered to Abacus for verification testing. Each of those computers had a label certifying that the disposing organization had sanitized the hard drives. Abacus' verification testing confirmed that the hard drives were wiped. We falsely marked one of these computers with a "fail" label

¹⁸ ITAR governs the export of defense-related articles and information, such as Space Shuttle-related technology, and makes it unlawful to share that technology with anyone except a U.S. person without obtaining a license and approval from the Department of State. ITAR violations can result in fines, imprisonment, or both.

¹⁹ Although sophisticated software programs can potentially "fix" corrupt or unreadable data, the risk that someone could obtain sensitive information from the corrupted computers is relatively low.

²⁰ The testing indicated only that some data remained, not the sensitivity of that data.

and placed it in the middle of the pallet for return to the property disposal facility. We subsequently located that pallet at the disposal location and found that the “failed” computer was being prepared for sale along with the other computers on the pallet. When we contacted Kennedy IT Security and USA personnel, they informed us that they were not aware that a computer on the pallet had been marked as having failed verification testing. In our judgment, the contractor’s practice of placing a failed label on equipment without notifying responsible personnel about the failure increases the risk that NASA will inadvertently release equipment containing sensitive information.

Selection Process Not Statistically Valid. Kennedy’s property disposal personnel did not have a statistically valid process for selecting computers for validation testing. Specifically, Kennedy had no guidelines for when or how to select a sample for testing.²¹ Rather, Kennedy’s property disposal personnel selected a pallet of sanitized equipment for testing when they determined that a “sufficient” number of pallets had been filled. However, they could not determine what percentage of excess IT equipment the selected pallets represented and therefore had no assurance that their sample was statistically valid.

Lack of Any Verification Process. As noted earlier, Johnson and Ames did not have a verification process to test previously sanitized IT equipment. Without verification testing, those Centers have no assurance that their sanitization process is adequate and effective. Personnel at both Centers told us that they were unaware that NASA policy requires verification testing.²²

Inadequate Oversight of Disposition Processes

Management at each of the Centers we visited did not adequately oversee IT disposition procedures to prevent the improper release of Agency data. Specifically, we found that IT equipment was not properly accounted for or tracked during the disposition process and that excess computers submitted for disposition had external IT markings that included NASA Internet Protocol information. Failing to properly account for hard drives during the disposition process increases the risk that NASA will inadvertently release IT equipment that contains sensitive information. In addition, the release of Internet Protocol information could lead to unauthorized access to NASA’s internal networks.

Accountability of Removed Hard Drives. Kennedy and Langley did not properly account for and track hard drives that were removed from excess computers. We

²¹ As noted previously, during the audit, Kennedy followed NASA’s sanitization policy that does not address sample selection. In addition, Kennedy’s recently released policy does not address sample selection.

²² Ames has a Center-specific policy that requires some verification review and testing; however, no such testing has been performed in the last 2 years.

identified instances at Kennedy and Langley of excess computers arriving at the disposal site without a hard drive but with no documentation to account for the missing drive.

IT personnel at Kennedy stated that when they cannot sanitize a hard drive using available software, they remove the drive from the computer and send it to the property disposal facility for destruction. They told us that the removed hard drives have no markings linking them to the computers from which they were removed and that the hard drives are not tracked once they are removed.

Kennedy disposal personnel informed us that they receive hard drives in lots that sometimes contain hundreds of drives. They stated that they track the hard drives by lot upon arrival at the warehouse, but had no way to determine which drives belonged to which computers. Moreover, they informed us and we observed that the removed hard drives were stored in an unsecured dumpster at the property disposal facility, which is easily accessible to non-NASA personnel during normal working hours. After hours, only a locked fence protects the dumpster (see Figure 2).

Figure 2. Hard Drives Stored in Publicly Accessible Dumpster



Source: OIG photographs (June 9, 2010)

We found that at Langley employees are permitted, with management approval, to remove and retain their hard drives prior to dispositioning excess computers. Employees are required to document such removals on NASA Form 1617, “Request for Cannibalization/Modification of Controlled Equipment,” and a copy of the form is to be attached to the excess computer before it is sent to the disposition contractor. If a computer arrives without a hard drive and does not have the requisite form, the contractor is supposed to suspend disposition of the computer. However, the disposal supervisor told us that contractor personnel do not suspend disposition when computers arrive without the proper paperwork. Consequently, Langley cannot ensure that it is accounting for all hard drives. Due to the sensitivity of data that hard drives may contain, NASA should ensure that disposition procedures adequately account for and track all hard drives removed from excess computers.

IT Equipment Submitted for Disposal with Sensitive Markings. During our review of Kennedy’s disposal processes, we identified several pallets of computers being prepared for disposition on which NASA Internet Protocol addresses were easily visible (see Figure 3).

Figure 3. Computer Marked with Internet Protocol Address

An Internet Protocol address provides a numerical description of the location of networked computers and distinguishes one computer from another on the Internet. It is similar to a street address or a phone number in that it provides a specific location to a specific computer that is



Source: OIG photograph (April 14, 2010)

on the Internet the same way a street address identifies the location of a specific house or a phone number identifies a specific phone. Release of NASA Internet Protocol addresses is a potential security weakness because these addresses could provide a hacker a means to gain unauthorized access to NASA’s internal network. Knowing a specific Internet Protocol address allows a hacker to target a particular computer, test the system for vulnerabilities, and possibly load malicious software programs or access information on the computer or network.

Inadequate NASA Policy on IT Sanitization

NASA's IT sanitization policy is incomplete and does not provide clear guidance on how to ensure IT equipment is properly sanitized before leaving NASA custody.

NPR 2810.1A, "Security of Information Technology," May 16, 2006, states that all excess IT equipment is to be properly sanitized during the disposal process. The NPR also requires all NASA information system owners to conduct the appropriate reviews and tests on excess IT equipment, as called for by NIST. The NPR further states that NASA computer support and operations are to ensure that all excess IT property is properly sanitized following the current NASA memorandum on the Sanitization of NASA Equipment prior to leaving NASA's custody. However, the NPR does not provide any further identifying information regarding the NASA memorandum it mentions, such as the date of the memorandum or a Standard Operating Procedure number. The Deputy Chief Information Officer for IT Security stated that the current NASA memorandum on the sanitization of equipment is NASA Standard Operating Procedure, ITS-SOP-0035, "Digital Media Sanitization," September 15, 2008.

NASA's Standard Operating Procedure states that "it is necessary to periodically test the sanitization equipment and procedures to ensure they are performing as intended." However, NASA policy does not establish how excess IT equipment should be selected for testing, describe a representative sample, or define an acceptable level of risk for failed computers.²³ Establishing an acceptable risk level should include mitigation strategies that define how much additional testing is required once a piece of IT equipment or a representative sample of equipment fails sanitization testing. For example, if the failure rate exceeds a certain percentage of the tested equipment, additional testing of the dispositioned equipment should be required.

DOD has established requirements for testing a representative sample of IT equipment to verify proper sanitization. The DOD memorandum, "Disposition of Unclassified DoD Computer Hard Drives," June 4, 2001, specifies methods and procedures for sanitization, provides guidance on the disposition of hard drives, and requires that 20 percent of sanitized hard drives be examined as a representative sample. We also contacted NIST IT security specialists to inquire about industry best practices for verification sampling, and they responded that a minimum sample size for sanitization verification should be 20 percent of total excess IT equipment.²⁴

²³ Office of Management and Budget Circular A-130, Appendix III, describes adequate security as security commensurate with risk. This risk includes both the likelihood of occurrence and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

²⁴ NIST Special Publication 800-88, which is referenced in the NASA procedure, does not discuss sample size or the frequency of sanitization testing. However, it does state that "A representative sampling of media should be tested for proper sanitization to assure the organization that proper protection is maintained. Verification of the process should be conducted by personnel without a stake in any part of the process." As a result of our inquiry, NIST IT security personnel said they will evaluate whether this information should be included in the next update of the publication scheduled for release in FY 2011.

NASA can decrease the risk of inadvertently releasing IT equipment that contains sensitive information by revising its policy and procedures and referencing those from other agencies that provide best practices. NASA can also improve its policy by including instructions for sampling IT equipment for sanitization testing. The procedures should explain how to develop a sampling plan and establish a minimum percentage of sanitized IT equipment to be tested. In addition, NASA policy should define the acceptable level of risk before additional mitigation strategies are implemented.

Failure to Use Approved Software

Contractor personnel involved in the IT sanitization and disposition process at Kennedy, Johnson, and Ames were not sufficiently familiar with and did not follow NASA sanitization policy. Specifically, we identified instances at each of these three Centers where personnel used unapproved software to sanitize IT equipment.

Use of Unapproved Sanitization Software. NASA's Standard Operating Procedure lists only three approved sanitization software products: Secure Erase, Darik's Boot and Nuke (DBAN), and WipeDrive/WipeDrive Pro. However, we found instances at Kennedy, Johnson, and Ames of personnel using or recommending sanitization software not on the NASA-approved list:

- USA used DataGone by Symantec to sanitize excess IT equipment at both Kennedy and Johnson. DataGone has not been approved by NASA or certified for use by other Federal agencies, including DOD and the National Security Agency.
- Johnson's disposition contractor, L&M Technologies, Inc., used both a NASA-approved software program (DBAN) and Active@KillDisk, which is not approved by NASA. When we informed L&M Technologies of the requirements in NASA's Standard Operating Procedure, it stopped using the unapproved software.
- The Ames IT Security Manager recommended that Center personnel use a sanitization software program called BCwipe, which is DOD-compliant and therefore permissible for use under Ames' procedures. However, it is not on the NASA list of approved software.

IT personnel at each of the three Centers stated that they were not aware that some of the sanitization software they were using had not been approved by NASA. The use of unapproved software is a significant concern because unapproved software was used on some of the computers at Kennedy that failed verification testing.

Management Actions Taken during the Audit

We worked closely with Center IT security personnel during our audit so that they could take action to remedy the weaknesses we identified as quickly as possible. After we shared our findings with Center managers, the Kennedy IT Security Manager established a “Tiger Team” with participants from key Center organizations and major contractors involved in the IT disposition process to review and improve the sanitization and disposition processes.

The Kennedy contracting officer’s technical representative for the Abacus contract said her staff will work with Center Operations and IT Security personnel to document the number of computers processed by the property disposal facility, which will allow Kennedy to determine how many of those computers need to undergo sanitization testing to meet a 20 percent minimum validation requirement.

Conclusion

NASA’s information systems capture, process, and store significant amounts of data including sensitive information. Without proper sanitization of those systems, the Agency is at risk of releasing sensitive information that could inhibit NASA’s ability to accomplish its mission as well as violate privacy and export control laws. For these reasons, strong controls over the disposition and sanitization processes are required to mitigate the risk of unauthorized disclosure. As Space Shuttle Program transition and retirement activities increase, significantly more IT equipment will enter the disposal pipeline and it is imperative that NASA revise its policies and procedures to protect its data from unauthorized release. Therefore, we believe that immediate Agency-wide attention to the proper disposition of IT equipment is required.

Recommendations, Management’s Response, and Evaluation of Management’s Response

We acknowledge the actions taken at Kennedy in response to the issues we raised during our audit. However, as discussed in this report we also found weaknesses in the sanitization and disposition processes for IT equipment at the three other Centers we visited. Consequently, we recommended that NASA’s Chief Information Officer (CIO) take the following actions:

Recommendation 1. Increase oversight efforts by initiating a review of sanitization procedures across all NASA Centers to identify deficiencies, share best practices, and take corrective action.

Management’s Response. The CIO stated that a review of NASA’s media sanitization policy and procedures would be initiated and used to update NPR 2810.1 and develop a

new IT Security handbook to replace NASA's Standard Operating Procedure (ITS-SOP-0035). The CIO also stated that the Office of Strategic Infrastructure could use this policy to take corrective action by amending existing contracts to compel contractor compliance and include the new requirements in all new contracts with vendors who conduct media sanitization for NASA. She indicated that NASA expected to complete the proposed action in the third quarter of fiscal year (FY) 2011.

Evaluation of Management's Response. In our judgment, the CIO's comments lack the urgency required to address the serious weaknesses identified in our report. We do not believe that it is either prudent or responsible for the Agency to wait for the conclusion of a lengthy document review process before addressing these issues. Instead, the Agency should develop a plan that includes an expedited physical review of the sanitization procedures at all Centers and a course of action to quickly implement necessary corrective action. Accordingly, we consider this recommendation to be unresolved.

Recommendation 2. Coordinate with the Assistant Administrator for Strategic Infrastructure to ensure Center Property Disposal Officers have the knowledge necessary to ensure that dispositioned IT equipment has been adequately sanitized prior to release to the public.

Management's Response. The CIO stated that NASA policy will be updated to reflect mandatory and exclusive use of approved software and tools for media sanitization. Additionally, the CIO stated that the Office for Strategic Infrastructure can use the updated policy to amend existing contracts to compel contractor compliance. She indicated that NASA expects to complete the proposed action in the third quarter of FY 2011. The Office of Strategic Infrastructure nonconcurred with our recommendation, stating that Property Disposal Officers do not have the technical expertise, training, or knowledge to ensure adequate sanitization of IT equipment and are only responsible for obtaining documentation that someone else has certified that each computer entering the disposal process has been adequately sanitized.

Evaluation of Management's Response. Neither the CIO nor the Office of Strategic Infrastructure adequately addressed the concerns that prompted our recommendation. Revising policy and relying on another office to interpret that policy and implement appropriate corrective action does not equate to coordination. In our view, the CIO should work closely with the Office of Strategic Infrastructure to determine the best course of action to improve the control weaknesses we identified. Similarly, although we agree that Property Disposal Officers are not personally responsible for sanitizing equipment, they are the last line of defense in preventing the unauthorized release of NASA data. NIST Special Publication 800-88 provides that "Organizations should ensure that property management officials are included in documenting the media sanitization process in order to establish proper accountability of equipment and inventory control." Accordingly, we believe that the Agency should ensure that property disposal personnel are adequately trained to ensure, for example, that IT equipment

marked “fail” is not released to the public. In light of management’s response, we consider this recommendation to be unresolved.

Recommendation 3. Develop a sampling methodology for verification testing that meets or exceeds the minimum requirements established by best practices, to include

- a. identifying NASA’s acceptable risk level for excess IT equipment;
- b. specifying the percentage of equipment to be tested and the frequency of testing needed to satisfy NASA’s risk determination; and
- c. requiring each Center to document its sampling methodology, identify in writing responsible officials, and maintain records of testing results.

In response to management’s comments, we revised the language of this recommendation slightly to make clear that the sampling methodology should be based on best practices rather than NIST and NISPOM requirements.²⁵

Management’s Response. The CIO partially concurred with our original recommendation, stating that because NIST and NISPOM do not mandate Federal agencies to develop a sampling methodology or conduct verification testing NASA would not sample or conduct testing in accordance with those entities’ standards. The CIO further stated that the Agency could develop a sampling methodology that aligns with the International Standard’s Organizations 2859 standard, but indicated that doing so would be too burdensome in terms of costs and paperwork. The CIO expressed the view that rather than adopting this burdensome standard, the Agency would be better off requiring that all electronic storage media be destroyed. The CIO stated that the new IT Security handbook will include NASA’s acceptable risk level for excess IT equipment, articulate a less burdensome verification policy, and designate responsible officials to ensure that NASA policy is followed. Management expects to complete the proposed action in the third quarter of FY 2011.

Evaluation of Management’s Response. We concede that NIST policy and NISPOM do not explicitly establish minimum requirements for sampling methodology in regard to verification testing; therefore, we revised the recommendation to cite “best practices” instead. Nevertheless, NISPOM does require the security authority to issue instructions on sanitization and DOD has implemented this requirement by requiring that 20 percent of sanitized hard drives be examined. In addition, personnel in NIST’s IT Security office informed us that a minimum sample size for sanitization verification should be 20 percent of total excess IT equipment and stated that NIST is considering revising its policy to specify a 20 percent minimum sample size.

²⁵ DOD “National Industrial Security Program Operating Manual” (NISPOM), 5220.22-M, February 28, 2006.

The CIO's contention that developing and implementing a sampling methodology would be onerous is based upon the guidance provided in International Standard's Organizations 2859 standard. We agree this guidance appears to be more burdensome than simply establishing a minimum sample size of 20 percent. However, in light of our finding that the minimal verification testing performed by the Agency failed to prevent the disposal of IT equipment containing sensitive information, we continue to believe that NASA should develop a sampling methodology for verification testing that meets or exceeds the requirements and best practices established by DOD and NIST. Accordingly, we consider this recommendation to be unresolved.

Recommendation 4. Update NPR 2810.1A and ITS-SOP-0035 to include the sampling methodologies developed in response to Recommendation 3 and from other appropriate references.

Management's Response. The CIO partially concurred with the recommendation and stated that the updated NPR and new IT Security handbook are being drafted. However, the CIO also stated that the new policy will not address a sampling methodology because such a requirement would produce an onerous burden in terms of cost and bureaucratic paperwork. Management expects to complete the proposed action in the third quarter of FY 2011.

Evaluation of Management's Response. As previously stated, in our judgment a sampling methodology is prudent and should be included in NASA's new policies. Accordingly, we consider this recommendation to be unresolved.

Scope and Methodology

We performed this audit from October 2009 through October 2010 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We interviewed the Kennedy IT Security Manager, Information Systems Division and Communications Infrastructure Services Division Chiefs, contracting officer's technical representatives, IT project managers and specialists, and the Kennedy Transition and Retirement Manager to obtain an understanding of the procedures in place at NASA for the sanitization of IT storage media and for safeguarding against the release of sensitive data to the public through the sale of excess IT equipment. We also interviewed USA IT managers and specialists, Abacus IT managers and analysts, and property disposal personnel at Kennedy's property disposal facility to determine their additional policies and procedures for sanitization, testing, reviews and audits, and disposal of excess IT equipment.

At Johnson, we interviewed Implemetrics Incorporated's President and Information Technology Specialist to obtain an understanding of the processes the contractor uses to sanitize excess IT equipment for the Center. To obtain an understanding of USA's sanitization processes at its Houston, Texas, office, we interviewed the contractor's IT Security Manager as well as Logistics and Property personnel. To obtain an understanding of Lockheed Martin's sanitization process under its ODIN contract with Johnson, we interviewed Johnson's contracting officer, the contracting officer's technical representative, and the contractor's Project Manager. We also observed Johnson's and USA's sanitization areas and equipment.

To obtain an understanding of the IT sanitization process at Ames, we interviewed personnel in Center Operations, including the Property Disposal Officer, Computer Security Official, Deputy Chief of Protective Services, a security specialist, and a system administrator. In addition, we interviewed the IT Security Manager for the Information Technology Directorate. To obtain an understanding of the ODIN contract, we interviewed the contractor's Deputy Program Manager and IT technician. In addition to the interviews, we observed examples of sanitized IT equipment in the property disposal area as well as the ODIN contractor's sanitization area.

At Langley, we interviewed the ODIN Deputy Program Manager and Langley's Deputy Manager of IT Security, Property Disposal Officer, and personnel from Logistics Management Division and Center Operations to obtain an understanding of the processes and procedures for sanitizing IT equipment for disposal. We also interviewed Tessada contract personnel to determine their processes for removal and destruction of hardware (specifically, hard drives) sent to the Langley warehouse. We toured the Langley warehouse, the Steam Plant (where the hard drives are destroyed), and the off-site ODIN warehouse, where the hard drives are wiped before they are processed for donation.

We identified and reviewed the following as applicable to the proper disposition of IT equipment:

- NASA Policy Directive (NPD) 2810.1D, "NASA Information Security Policy," May 9, 2009
- NPR 2810.1A, "Security of Information Technology," May 16, 2006
- NPD 4300.1B, "NASA Personal Property Disposal Policy," February 19, 1999
- NPR 4300.1A, "NASA Personal Property Disposal Procedural Requirements," July 19, 1999
- NASA ITS-SOP-0035, "Digital Media Sanitization," September 15, 2008
- "2010 NASA Headquarters Security Awareness Training," Course HQ-0050-10, Revision October 28, 2010
- NASA Federal Acquisition Regulation Supplement, Sections 1804 and 1852
- Ames Procedural Requirements 2815.2, "Information Technology (IT) Policies and Requirements," February 1, 2007
- Ames Procedural Requirement 2815.1, "Excessing Government Owned Computer," July 26, 2010
- Johnson Space Center Work Instruction 4300.1, "JSC Instructions for Excess and Disposal of Government Property," September 28, 2009
- Kennedy (NASA-KSC) "Personal Property Transfer/Excess Process," KDP-KSC-P-3716, October 13, 2010
- Langley Procedural Directive 2810.1, "Security of Information Technology," April 11, 2005

- ODIN/Langley Research Center, “Quality Management Work Instruction 006,” January 12, 2010
- NIST Special Publication 800-88, “Guidelines for Media Sanitization,” September 2006
- NIST Special Publication 800-53, Revision 3, “Information Security,” August 2009
- DOD “National Industrial Security Program Operating Manual,” 5220.22-M, February 28, 2006
- Multiple DOD memorandums related to sanitization
- ITAR (Code of Federal Regulations Title 22, “Foreign Relations,” Chapter 1, Subchapter M, Parts 120-130)
- Multiple USA policies and procedures related to sanitization
- Multiple Abacus policies and procedures related to sanitization and audits
- L&M Technologies Procedure 6004, “Reutilization and Disposal,” July 27, 2009
- Tessada Procedure 4.5.2-1, “Processing Computer Equipment for Donation,” March 16, 2009

We conducted numerous meetings with NASA program office personnel involved in IT media security and the Space Shuttle Program transition efforts to understand their roles and determine responsibilities. We performed testing at Kennedy to determine whether Agency data remained in the hard drives of previously sanitized IT equipment. Although Kennedy was the only Center that we visited with procedures in place to test previously sanitized IT equipment, we determined that those procedures did not adequately ensure that the equipment was properly sanitized before disposal.

Use of Computer-Processed Data. We did not use computer-processed data to perform this audit.

Review of Internal Controls. We reviewed internal controls for NASA’s IT equipment disposition and sanitization processes. The control weaknesses we identified are discussed in this report. Our recommendations, if implemented, will correct the identified control weaknesses.

Prior Coverage

During the last 5 years, the Government Accountability Office (GAO) has issued two reports of particular relevance to the subject of this report. Unrestricted reports can be accessed over the Internet at <http://www.gao.gov> (GAO).

“NASA: Agency Faces Challenges Defining Scope and Costs of Space Shuttle Transition and Retirement” (GAO-08-1096, September 2008)

“Property Management: Lack of Accountability and Weak Internal Controls Leave NASA Equipment Vulnerable to Loss, Theft, and Misuse” (GAO-07-432, June 2007)

NASA POLICIES AND BEST PRACTICE GUIDANCE

NPR 2810.1A, “Security of Information Technology,” May 16, 2006. This policy establishes the procedures and requirements of the NASA Information Technology Security Program and provides direction designed to ensure that safeguards for the protection of the confidentiality, integrity, and availability of unclassified IT resources are integrated into and support NASA's missions, functional lines of business, and infrastructure based on risk-managed, cost-effective IT security and information security principles and practices. It applies to all NASA employees, NASA support service contractors, NASA IT resources, and in NASA contracts and requires that any IT resource in or behind the NASA assigned Internet Protocol address space to follow NASA and Center policies and requirements

NPR 4300.1A, “NASA Personal Property Disposal Procedural Requirements (Revalidated 2/17/06 with Change 1),” July 19, 1999. This policy offers procedural guidance to NASA Centers for the utilization and disposal management of NASA-owned excess, surplus, and exchange/sale personal property. The policy applies to NASA Headquarters and NASA Centers and other NASA contractors to the extent specified in contracts and to NASA-owned personal property wherever located.

NASA Standard Operating Procedure, ITS-SOP-0035, “Digital Media Sanitization,” September 15, 2008. The purpose of this Standard Operating Procedure is to protect NASA information and to ensure that there is no accidental leakage and institutes a procedure for sanitizing electronic storage devices. Any electronic storage device that has ever contained NASA information, even for a brief period, must be sanitized before it can be reassigned, transferred, or discarded. This Procedure applies to all information system owners, who are required to follow these procedures from the creation to the disposal of all information that is stored on information technology systems under their control.

NIST Special Publication 800-88, “Guidelines for Media Sanitization,” September 2006. This guide assists organizations and system owners in making practical sanitization decisions based on the level of confidentiality of their information. It describes sanitization decision processes that can be applied universally. The objective of this special publication is to assist with decision making when media require disposal, reuse, or will be leaving the effective control of an organization. Organizations should develop and use local policies and procedures in conjunction with this guide to make effective, risk-based decisions on the ultimate sanitization and/or disposition of media and information.

DOD NISPOM, 5220.22-M, February 28, 2006. It provides baseline standards for the protection of classified information released or disclosed to industry. It prescribes the

requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information. The Manual controls the authorized disclosure of classified information released by U.S. Government Executive Branch departments and agencies to their contractors.

DOD Memorandum, “Disposition of Unclassified DoD Computer Hard Drives,” June 4, 2001. It specifies methods and procedures for sanitization and guidance on disposition of hard drives and states that 20 percent of hard drives will be examined via sampling.

MANAGEMENT COMMENTS

National Aeronautics and Space Administration
Headquarters
Washington, DC 20546-0001



Reply to Attn of: Office of the Chief Information Officer

NOV 29 2010

TO: Assistant Inspector General for Audits

FROM: Chief Information Officer

SUBJECT: Draft Audit Report, "Preparing for the Space Shuttle Program's Retirement: A Review of NASA's Procedures for the Disposition of Information Technology Equipment" (Assignment No. A-09-018-01)

The Office of the Chief Information Officer (OCIO) appreciates the Office of Inspector General's (OIG) review of the Agency's procedures for the disposition of Information Technology equipment. Below are OCIO responses to the recommendations made by the OIG. OCIO developed these responses with assistance of the Office of Strategic Infrastructure (OSI), Headquarters' Logistics Management Division (LMD), where appropriate, as the jurisdictions for this audit crossed both organizations.

Recommendation 1:

Increase oversight efforts by initiating a review of sanitization procedures across all NASA Centers to identify deficiencies, share best practices, and take corrective action.

NASA Management Response to Recommendation 1:

OCIO and OSI: Concur.

From a policy perspective, OCIO will be updating NPR 2810.1B, and developing a new IT Security handbook to replace ITS-SOP-0035, thereby initiating a review of NASA's media sanitization policy and procedures. Additionally, the process for the drafting of a handbook to replace ITS-SOP-0035, in conjunction with the findings of this audit, will allow OCIO to identify deficiencies. OCIO believes that OSI can then use this new policy to take corrective action by amending existing contracts to compel contractor compliance with new NASA policy, and to include these requirements in all new contractual relationships with vendors who will be conducting Media Sanitization on the Agency's behalf.

Management Corrective Action Dates:

NPR 2810.1B and a new IT Security handbook to replace ITS-SOP-0035 will be finalized in the third quarter of Fiscal Year 2011.

Recommendation 2:

Coordinate with the Assistant Administrator for Strategic Infrastructure to ensure Center Property Disposal Officers have the knowledge necessary to ensure that dispositioned IT equipment has been adequately sanitized prior to release to the public.

NASA Management Response to Recommendation 2:

OCIO: Partially Concur.

OCIO will update the NASA policy to reflect mandatory and exclusive use of the software and/or tools approved by NASA for Media Sanitization. OCIO believes that OSI can then use this policy to amend existing contracts to compel contractor compliance with new NASA policy, and to include these requirements in all new contractual relationships with vendors who are conducting Media Sanitization on the Agency's behalf.

OSI: Non-Concur.

The responsibility for "adequate sanitization" of the computer hard drives is not the responsibility of the Centers Property Disposal Officers (PDOs). PDOs do not have the technical expertise, training, or knowledge to ensure that a computer has been adequately sanitized. PDOs are responsible for obtaining the documentation that someone (e.g., Center OCIO, disposal warehouse IT person, the contractor, etc.) has certified that each computer entering the disposal warehouse has been adequately sanitized before its final disposition. The method in which each Center does the sanitization differs: some Center OCIOs directly sanitize all computers during disposal; or at some Centers, each computer is sanitized within the disposal warehouse; or at some Centers only documentation/proof of sanitization is required upon receipt; or all hard drives are removed and destroyed; or some combination of the above. Also, the software used by contractors is a matter of the terms and conditions of the contract and the PDO has no control of the type of software tool used in those cases.

Management Corrective Action Dates:

NPR 2810.1B, and a new IT Security handbook to replace ITS-SOP-0035, will be finalized in the third quarter of Fiscal Year 2011.

Recommendation 3:

Develop a sampling methodology for verification testing that meets or exceeds the minimum requirements established by NIST and NISPOM, to include:

- a. identifying NASA's acceptable risk level for excess IT equipment;
- b. specifying the percentage of equipment to be tested and the frequency of testing needed to satisfy NASA's risk determination; and
- c. requiring each Center to document its sampling methodology, identify in writing responsible officials, and maintain records of testing results.

2

Revised.

NASA Management Response to Recommendation 3:

OCIO and OSI: Partially Concur.

OCIO has studied NIST and NISPOM, and does not see any mandate upon Federal Agencies to develop a sampling methodology, nor conduct verification testing related to media sanitization. NIST SP 800-88 currently does not discuss sample size or the frequency of media sanitization testing. Additionally an investigation of the current version of NISPOM (DoD 5220.22-M, February 28, 2006) reveals advice and specifics on certain technical aspects of cleaning and media sanitization. However, NISPOM *Section 3 Common Requirements, 8-301 Clearing and Sanitization* does not outline a specific random sampling methodology or verification procedure with respect to media sanitization, as called for in the audit recommendation.

Therefore, OCIO does not agree that developing “a sampling methodology for verification testing that meets or exceeds the minimum requirements established by NIST and NISPOM” is possible, nor is it a requirement of a Federal Agency following NIST and NISPOM guidance.

OCIO could potentially develop a policy for a sampling methodology that could align to the recommendations of the non-governmental International Standards Organization’s (ISO) 2859 standard. However, the resulting operational activities from such a policy requirement would produce an onerous burden upon the agency, in terms of a monetary cost to conduct the sampling work, and the storage or warehousing costs associated with rejecting and correcting lots or batches of computers. Additionally, the paperwork associated with adherence to said policy would produce a bureaucratic operation with obedience to forms and paperwork, rather than proper protection of the media. This burden would far outweigh any benefits, value, or recouped dollars that NASA would hope to obtain via reutilization, transfer, donation, or federal sale of the sanitized computers. In fact, the Agency would be better off by simply requiring that all media be destroyed by shredding, or by incineration, than to develop a sampling methodology for verification testing that meets or exceeds the minimum requirements of an industry or government standard.

If the Agency is to continue with the practice of reutilization, transfer, donation, or federal sale of some Agency sanitized computers, OCIO agrees that media sanitization is an important activity that needs a degree of verification. As such OCIO will be updating NPR 2810.1B, and developing a new IT Security handbook to replace ITS-SOP-0035. This new handbook will identify NASA’s acceptable risk level for excess IT equipment, will develop a less burdensome verification policy, and will identify the responsible officials to ensure that NASA policy is followed.

Management Corrective Action Dates:

NPR 2810.1B, and a new IT Security handbook to replace ITS-SOP-0035, will be finalized in the third quarter of Fiscal Year 2011.

Removed reference to NISPOM containing information on random sampling from footnote 14.

Recommendation 4:

Update NPR 2810.1A and ITS-SOP-0035 to include the sampling methodologies developed in response to Recommendation 3 and from other appropriate references.

NASA Management Response to Recommendation 4:

OCIO and OSI: Partially Concur.

NPR 2810.1B, and a new IT Security handbook to replace ITS-SOP-0035, are currently being drafted. They will address media sanitization and will direct readers to the appropriate Federal guidance references from NIST, NISPOM, and the National Security Agency, where appropriate. However, NPR 2810.1B, and the new IT Security handbook will not address a sampling methodology as outlined in Recommendation 3 due to a burden upon the Agency (see response to NASA Management Response to Recommendation 3).

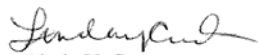
Management Corrective Action Dates:

NPR 2810.1B, and a new IT Security handbook to replace ITS-SOP-0035, will be finalized in the third quarter of Fiscal Year 2011.

At the OIG's request, the OCIO has evaluated the report to identify any information that it believes should not be publicly released. The OCIO has determined that this report does not contain any specific sensitive but unclassified information.

We appreciate the courtesies extended to the OCIO by the OIG in providing the opportunity to submit a revised response to the subject audit. Please direct any questions to Ms. Marion Meissner at (202) 358-0585 or Mr. Dana M. Mellerio at (202) 358-0271.

Respectfully,



Linda Y. Cureton
NASA CIO

REPORT DISTRIBUTION

National Aeronautics and Space Administration

Administrator
Deputy Administrator
Chief of Staff
Chief Information Officer
Assistant Administrator for Strategic Infrastructure
Director, Logistics Division
Director, Ames Research Center
Director, Dryden Flight Research Center
Director, Glenn Research Center
Director, Goddard Space Flight Center
Director, Jet Propulsion Laboratory
Director, Johnson Space Center
Director, Kennedy Space Center
Director, Langley Research Center
Director, Marshall Space Flight Center
Director, Stennis Space Center

Non-NASA Organizations and Individuals

Office of Management and Budget
Deputy Associate Director, Energy and Science Division
Branch Chief, Science and Space Programs Branch
Government Accountability Office
Director, NASA Financial Management, Office of Financial Management and Assurance
Director, NASA Issues, Office of Acquisition and Sourcing Management

Congressional Committees and Subcommittees, Chairman and Ranking Member

Senate Committee on Appropriations
Subcommittee on Commerce, Justice, Science, and Related Agencies
Senate Committee on Commerce, Science, and Transportation
Subcommittee on Science and Space
Senate Committee on Homeland Security and Governmental Affairs

Congressional Committees and Subcommittees, Chairman and Ranking Member (continued)

House Committee on Appropriations

 Subcommittee on Commerce, Justice, Science, and Related Agencies

House Committee on Oversight and Government Reform

 Subcommittee on Government Management, Organization, and Procurement

House Committee on Science and Technology

 Subcommittee on Investigations and Oversight

 Subcommittee on Space and Aeronautics

Major Contributors to the Report:

Raymond Tolomeo, Science and Aeronautics Research Director

Loretta Atkinson, Project Manager

G. Paul Johnson, Project Manager

Julia Eggert, Lead Auditor

Doug Orton, Lead Auditor

Eugene Bauer, Auditor

Nicole Frish, Auditor

Jim Griggs, Auditor

Jason Hensley, Auditor

Barbara Moody, Auditor

James Richards, Auditor

Linda Hargrove, IT Specialist



OFFICE OF AUDITS

OFFICE OF INSPECTOR GENERAL

ADDITIONAL COPIES

Visit <http://oig.nasa.gov/audits/reports/FY11/> to obtain additional copies of this report, or contact the Assistant Inspector General for Audits at 202-358-1232.

COMMENTS ON THIS REPORT

In order to help us improve the quality of our products, if you wish to comment on the quality or usefulness of this report, please send your comments to Mr. Laurence Hawkins, Audit Operations and Quality Assurance Director, at Laurence.B.Hawkins@nasa.gov or call 202-358-1543.

SUGGESTIONS FOR FUTURE AUDITS

To suggest ideas for or to request future audits, contact the Assistant Inspector General for Audits. Ideas and requests can also be mailed to:

Assistant Inspector General for Audits
NASA Headquarters
Washington, DC 20546-0001

NASA HOTLINE

To report fraud, waste, abuse, or mismanagement, contact the NASA OIG Hotline at 800-424-9183 or 800-535-8134 (TDD). You may also write to the NASA Inspector General, P.O. Box 23089, L'Enfant Plaza Station, Washington, DC 20026, or use <http://oig.nasa.gov/hotline.html#form>. The identity of each writer and caller can be kept confidential, upon request, to the extent permitted by law.