

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



June 4, 2008

Reply to Attn of:

Office of Internal Controls and Management

TO: Assistant Inspector General for Investigations
FROM: Assistant Administrator for Internal Controls and Management Systems
SUBJECT: Agency Efforts to Mitigate Lost and Stolen Laptop Computers

This memorandum articulates NASA's actions taken in response to your memorandum on the subject of lost and stolen laptop computers dated April 28, 2008.

In your memorandum, you recommended that NASA raise/renew employee awareness of prevailing Agency guidance with respect to the safeguarding of laptop computers, peripheral equipment, and electronic data stored on those devices.

As you are well aware, NASA management has developed a robust framework of policies and procedural requirements which foster an environment in which employees exercise due care in the use, handling, and transport of laptops, peripherals, and stored data. Given the prevalence of sensitive data handled by NASA employees (i.e., SBU, PII, etc.), it is particularly important to ensure that all employees are aware of their responsibilities in this area.

In an effort to foster renewed awareness of employee responsibilities regarding laptops, peripherals, and stored data, the Office of Internal Controls and Management Systems (OICMS) discussed the contents of your April 28th memo with NASA management officials at the May 6, 2008 Weekly Senior Staff Meeting¹. Additionally, OICMS asked that each OIC in attendance disseminate to their employees the need to exercise due diligence and commonsense while transporting laptops and peripherals especially when sensitive data could be at risk.

In addition to the verbal briefing OICMS provided to senior management on May 6th, a NASA Inc. notification on the topic of safeguarding laptops, peripherals, and stored data was disseminated to all NASA employees on May 19, 2008. The notification included a memorandum dated May 14, 2008 addressed to all NASA employees highlighting the importance of exercising due diligence consistent with NASA policy and procedural requirements in the use, handling, and transport of laptops, peripherals, and stored data.

¹ This meeting, chaired by the Chief of Staff and generally attended by Associate/Assistant Administrator level management or their deputies, is often used to communicate emerging Agency issues in real-time.

The May 14th memorandum was prepared in conjunction with the Office of the Chief Information Officer and the Office of Infrastructure and Administration, Logistics Management Division, NASA principal policy-setting organizations in this specific subject area. Both the May 14th memorandum and the May 19th NASA Inc. notification are enclosed with this response.

We believe that the actions taken by NASA management as described above substantially satisfy the letter and spirit of the recommendation that you communicated in your memorandum dated April 28, 2008. Consequently, we request that you close the recommendation based on those actions.

NASA management recognizes and fully appreciates the efforts of the Office of Inspector General and other federal law enforcement entities to ensure that those who commit property related crimes are held accountable.

If you have any questions, or require additional information regarding this response, please don't hesitate to call either myself on 358-4593 or Paul Roberts on 358-2260.



Lou Becker

Enclosures (2)

cc:

Chief of Staff/ Mr. Morrell

General Counsel/ Mr. Wholley

Associate Administrator for Institutions and Management/Mr. Luedtke

Office of the Chief Information Officer/Mr. Davis

Office of the Chief Information Officer/Mr. Kit

Logistics Management Division/Ms. Kinney

Logistics Management Division/Mr. Staefe

From: headquarters-govt-only-bounces@lists.hq.nasa.gov on behalf of NASA INC [hq-nasa-inc@nasa.gov]
Sent: Monday, May 19, 2008 4:27 PM
To: headquarters-govt-only@lists.hq.nasa.gov
Subject: Lost and Stolen Laptop Computers

This message is being distributed to NASA civil service employees.
Point of Contact: Lou Becker, Assistant Administrator for Internal Controls and Management Systems, 202-358-4593

Lost and Stolen Laptop Computers

The purpose of this notice is to highlight employee responsibilities with respect to safeguarding laptop computers, removable storage devices, and electronic information stored on these devices.

Recent findings by both the NASA Office of Inspector General (OIG) and the Government Accountability Office (GAO) indicate that employee negligence is a significant contributing factor in the loss or theft of laptop computers and removable storage devices. As a result, employees are reminded that reasonable care and vigilance over laptop computers, removable storage devices, and electronic information contained on these devices should be exercised, particularly while on travel status or while in-transit.

All NASA employees have a personal responsibility for safeguarding Government property issued to them. An employee may be held financially liable for the loss, damage, or destruction of Government property when the loss, damage, or destruction is due to the employee's negligence, dishonesty, misconduct, or misuse of such property.

If you are unsure as to your responsibilities relating to the safeguarding of Government property and/or electronic information, contact your respective Property Custodians or IT Security Managers, or refer to:

- * NPD 4200.1B, Equipment Management;
- * NPR 2810.1A, Security of Information Technology;
- * NPR 1600.1, Classified National Security and Sensitive but Unclassified (SBU) Information Management; and
- * NPR 1382.1, NASA Privacy Procedural Requirements

Note:

The memorandum, "Lost and Stolen Laptop Computers," was signed by Lou Becker, Assistant Administrator for Internal Controls and Management Systems, on May 14, 2008. The original document in PDF format is posted online at: http://oim.hq.nasa.gov/oicms/docs/Safeguarding_Laptops_Memo.pdf

This notice is being transmitted by NASA INC in the Office of Public Affairs. For more information on NASA INC products and services, mailto:NASA_INC@hq.nasa.gov or visit the NASA INC Web page at http://insidenasa.nasa.gov/nasa_nas/ops/NASA_INC/index.html

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



May 14, 2008

Reply to Attn of: Office of Internal Controls and Management Systems

TO: All NASA Employees
FROM: Assistant Administrator for Internal Controls and Management Systems
SUBJECT: Lost and Stolen Laptop Computers

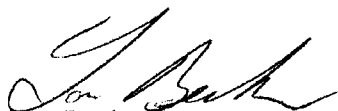
The purpose of this memorandum is to highlight employee responsibilities with respect to safeguarding laptop computers, removable storage devices, and electronic information stored on these devices.

Recent findings by both the NASA Office of Inspector General (OIG) and the Government Accountability Office (GAO) indicate that employee negligence is a significant contributing factor in the loss or theft of laptop computers and removable storage devices. As a result, employees are reminded that reasonable care and vigilance over laptop computers, removable storage devices, and electronic information contained on these devices should be exercised, particularly while on travel status or while in-transit.

All NASA employees have a personal responsibility for safeguarding Government property issued to them. An employee may be held financially liable for the loss, damage, or destruction of Government property when the loss, damage, or destruction is due to the employee's negligence, dishonesty, misconduct, or misuse of such property.

If you are unsure as to your responsibilities relating to the safeguarding of Government property and/or electronic information, contact your respective Property Custodians or IT Security Managers, or refer to:

- NPD 4200.1B, *Equipment Management*;
- NPR 2810.1A, *Security of Information Technology*;
- NPR 1600.1, *Classified National Security and Sensitive but Unclassified (SBU) Information Management*; and
- NPR 1382.1, *NASA Privacy Procedural Requirements*


Lou Becker

ENCLOSURE 2