National Aeronautics and Space Administration
Office of Inspector General
Washington, DC 20546-0001

APR 28 2008

TO: Associate Administrator for Institutions and Management
Chief Information Officer

FROM: Assistant Inspector General for Investigations

SUBJECT: Lost and Stolen Laptop Computers

The purpose of this memorandum is to recommend management action regarding recent reports of lost and stolen laptops and other computer equipment.

During the past calendar year, we have received nine reports of lost and stolen computer equipment, the most recent being a NASA employee who, while on travel, left her laptop computer unattended on a chair in a common area of a restroom – while she used the facilities. Other reports of stolen laptops included ones that have been taken from NASA employees in a variety of other circumstances, to include thefts from unsecured vehicles, the workplace, or from home. While the amount of physical losses is small compared to NASA's overall laptop inventory, the loss of one laptop (depending on the data therein) could have a profound impact on Agency operations – to include risks to employee privacy. Fortunately, these cases don't appear to raise these issues, although more work needs to be done.

This office recognizes the difficulty of stopping a determined thief from perpetrating a planned theft requiring access to unauthorized or protected areas like a home, a locked car, or the work place. But unfortunately, most of the reports we've received point toward a NASA employee's negligence as being a contributing factor to the loss. This is troubling, because according to NASA regulations, NASA employees have duties and obligations regarding the protection of NASA's data and equipment. For example, NPR 2810.1A, Security of Information Technology, requires employees to comply with policies and procedures to *protect* unclassified NASA information; and NPD 4200.1B, Equipment Management, requires employees to *safeguard* and prudently operate assets issued to them. Other regulations set forth employee requirements pertaining to protection of sensitive but unclassified information[1] – which often is found on NASA laptops.

[1] NPR 1600.1, NASA Security Program Procedural Requirements, defines Sensitive But Unclassified (SBU) Controlled Information/Material as unclassified information or material determined to have special protection requirements to preclude unauthorized disclosure to avoid compromises, risks to facilities, projects or programs, threat to the security and/or safety of the source of information, or to meet access restrictions established by laws, directives, or regulations. This information includes ITAR, Privacy Act, Proprietary and other types of information that the Agency has determined to be sensitive; NASA employees are obligated to safeguard and protect this information. NASA employees are also required to protect Personally Identifiable Information, as defined by NPR 1382.1, NASA Privacy Procedural Requirements.

We also recognize the inherent challenges associated with protecting laptops and other small, transportable data items (like memory sticks) that are highly susceptible to loss and theft. But we also believe that the recent amounts of loss and their attendant circumstances suggest that NASA can do better in protecting our equipment *and information* – possibly through increased situational awareness and training. We all know that systemic, passive, and reasonable common sense measures taken by our employee workforce are the best steps to protect our equipment and information from physical and virtual theft.

Please be assured that this office, in coordination with the Federal Bureau of Investigation and NASA's Office of Security and Program Protection, remains committed to doing everything we can to ensure that those who commit these NASA-related crimes are held accountable. This year, we apprehended, indicted, convicted, and imprisoned a Johnson Space Center security guard and his fence who were stealing and selling laptops (and other electronic equipment) belonging to the Johnson Space Center. And in recent years, we've also had successful prosecutions involving laptops at Marshall Space Flight Center and Glenn Research Center. Other NASA laptop-related cases are still under investigation, and we stand ready to assist the Agency should you bring other such cases to our attention.

In the meantime, however, we recommend that the Agency review its present policies[2] on this subject matter, with a view toward taking steps to raise or renew the awareness of the above-mentioned regulations and safeguarding assigned computers and peripherals, while in the office, at home, and on travel. On a related topic, a June 2007 report by the Government Accountability Office was critical of NASA's lack of accountability and weak internal controls pertaining to equipment losses, theft and misuse -- which we also commend for your review in this context.[3]

We respectfully request a response to this memorandum within 30 days. I am available for questions regarding this matter at (202) 358-2580 or you can contact the Deputy Assistant Inspector General for Investigations, Matt Kochanski at (202) 358-2576.

K. H. Winters

Kevin H. Winters

cc:
Chief of Staff/Mr. Morrell
General Counsel/Mr. Wholley

---

[2] This includes the Deputy Administrator's October 2, 2007, memorandum, "Safeguarding Sensitive but Unclassified Information."

[3] *See*, GAO-07-432, Property Management, Lack of Accountability and Weak Internal Controls Leave NASA Equipment Vulnerable to Loss, Theft and Misuse, June 2007.