National Aeronautics and
Space Administration
**Office of the Administrator**
Washington, DC 20546-0001

August 19, 2002

The Honorable Andrew H. Card, Jr.
Assistant to the President
and Chief of Staff
Executive Office of the President
Washington, DC 20500

Dear ~~Mr. Card:~~ Mr. Secretary

This letter is in response to your request dated March 19, 2002, that agencies review their records management procedures to ensure that information related to weapons of mass destruction and other information that could be used to harm the Nation's security is appropriately safeguarded.

In light of the terrorist attacks of September 11, 2001, and the possibility for further terrorist activity in their aftermath, NASA recognized the need to safeguard unclassified but sensitive information related to homeland security. The Agency took several significant actions to ensure that its approach to the electronic dissemination of any such information was appropriate. On November 16, 2001, the NASA Chief Information Officer (CIO) and the Associate Administrators for Management Systems and for Security Management and Safeguards jointly issued NASA's Web Site Registration and Internet Publishing Content Guidelines. The guidelines instructed that, effective immediately, access to public Web sites from the Internet was blocked for all unapproved sites residing on NASA networks. Until a site was registered, reviewed, and approved, access to unregistered and unapproved sites was limited to the NASA network domain (nasa.gov) only. Additionally, the guidelines noted that some links on the public NASA Home page might become unavailable to the public until approved. NASA Centers were made accountable for establishing a process implementing the guidelines and for monitoring the process to ensure ongoing appropriate and thorough Web site reviews.

In January 2002, NASA established an Operational Security program to further educate and orient employees and contractors to security considerations related to protecting any information that could potentially be useful to an adversary. The program includes identification of critical information, threat, and vulnerability analyses, risk assessment, and countermeasures. This program will increase each NASA employee's awareness of the importance of protecting sensitive information.

In response to the October 12, 2001, policy memorandum from Attorney General Ashcroft to the Heads of all Departments and Agencies related to disclosure policy under the Freedom of Information Act (FOIA), NASA Headquarters instructed all of its Center FOIA offices to carefully review all requests for information and to report any security-related requests as well as any others that appear to be unusual or questionable to the Agency FOIA Officer for appropriate coordination with the Agency's Office of Security Management and Safeguards. Your March 19, 2002, memo and its enclosures were also distributed to all Center FOIA offices and were discussed at the Agency's Annual FOIA Conference in June 2002. Richard Huff, the Co-Director of the Office of Information and Privacy at the Department of Justice, who we understand collaborated in the drafting of both of the memoranda, conducted a session to specifically provide an update and clarification of the new policies. Since November 1995, NASA has had an Agencywide Export Control Program, to ensure that transfers of export-controlled technologies, software, and commodities in NASA's international programs are consistent with U.S. export-control laws, regulations, and policies.

We have sent a memorandum to all of our Centers reminding them of their obligation to thoroughly review and screen all material deemed sensitive. We continue to review current and historical Agency records for the purpose of reclassifying, declassifying and downgrading records containing weapons of mass destruction information and other sensitive records related to homeland security. We are revising NASA policy directives regarding records management and security policy guidelines to further ensure that NASA personnel identify and safeguard homeland security information.

We continue to examine our Agency information practices to assure the safeguarding of all homeland security information, particularly that which relates to weapons of mass destruction.

Cordially,

Sean

Sean O'Keefe
Administrator

cc:
Office of Homeland Security

Our timely response is as a consequence of a thorough process — I think we've met your direction!