National Aeronautics and
Space Administration

Office of Inspector General
Washington, DC 20546-0001

July 22, 2008

The Honorable Barbara A. Mikulski
Chairman
Subcommittee on Commerce, Justice, Science, and Related Agencies
Committee on Appropriations
United States Senate
Washington, D.C. 20510

Subject: NASA's Compliance with Federal Export Control Laws and Risks Associated with the Illegal Transfer or Theft of Sensitive Technologies
(Report No. IG-08-022)

Dear Chairman:

This letter is sent in compliance with Public Law 106-391, "National Aeronautics and Space Administration Authorization Act of 2000." That law requires that the Inspector General of NASA conduct an annual audit of NASA policies and procedures with respect to the export of technologies and the transfer of scientific and technical information (STI) to assess the extent to which NASA is carrying out its activities in compliance with Federal export control laws and other reporting requirements. In addition, Conference Report 108-401, which accompanied H.R. 2673, the "Consolidated Appropriations Act, 2004," directed that NASA and the NASA Inspector General work together and report annually on the risks associated with the illegal transfer or theft of sensitive technologies from NASA.

The NASA Office of Inspector General (OIG) continues to work closely with NASA's Office of the Chief Information Officer (OCIO), Office of Security and Program Protection (OSPP), Office of General Counsel, and Office of External Relations to identify and reduce the risks associated with the illegal transfer or theft of sensitive technologies and ensure compliance with Federal export control laws. We remain committed to ensuring that incidents of stolen or compromised sensitive data and technology receive immediate action and that those responsible are held accountable. The Office of External Relations is continuing its initiative to reach out to NASA authors to ensure that NASA's STI is properly approved for public release before it is presented at conferences, in scientific journals, or otherwise disseminated. The initiative was launched, in part, as a result of our audit report IG-08-017, "Actions Needed to Ensure Scientific and Technical Information Is Adequately Reviewed at Goddard Space Flight

Center, Johnson Space Center, Langley Research Center, and Marshall Space Flight Center," June 2, 2008. We also continue to work with OCIO and OSPP to address counter-intelligence and counter-terrorism issues (the results of which cannot be addressed in this document).

To comply with the Public Law and the Conference Report requirement, NASA OIG conducted, is conducting, or plans to conduct the audits, investigations, and reviews reported herein. This letter does not provide detailed information about our findings; however, we will provide to you copies of each product, some of which are marked sensitive but unclassified (SBU), and will discuss any of these products with you or your staff at your request.

Status of the Agency IT Security Program and OIG Assessment

The strength of NASA's information technology (IT) security program is crucial to protecting the Agency against the illegal transfer or theft of sensitive technologies. In our annual report to the Administrator, "NASA's Most Serious Management and Performance Challenges" (last issued November 13, 2007), we continued to report findings on management, operational, and technical control weaknesses that impact the Agency's IT Security Program and threaten the confidentiality, integrity, and availability of NASA information and its systems. The threat is tangible in that the Agency continues to be a target for criminal computer intrusions. For example, we investigated a series of unlawful computer intrusions into NASA's Earth Observation System networks. The operational impact these intrusions have had on the Agency's mission—such as the temporary suspension of automated processes—has been significant. In one case during fiscal year (FY) 2007, an unlawful intrusion resulted in approximately $1 million in Agency losses.

NASA has also recognized IT security as a material weakness in its system of internal controls. Demonstrating its commitment to improving its security posture, NASA has reported making enterprise infrastructure improvements and progress against its IT security corrective action plan, as well as adequately meeting the requirements of the Federal Information Systems Management Act (FISMA). On the basis of these reported improvements, the OIG is currently evaluating NASA's actions taken to improve IT security so that we may provide the Agency with an independent assessment of its progress.

OIG Products Issued in FY 2007 and FY 2008

Since our last letter to Congress issued in July 2007, we have issued six products that directly or indirectly related to identifying and reporting on risks associated with the illegal transfer or theft of sensitive technologies. These products identified systemic issues related to a lack of consistent application of, or noncompliance with, established policies and regulations. The inconsistent application of, and noncompliance with, policies and regulations could place NASA's export-controlled technologies and data at risk of being stolen or compromised.

"NASA's Reporting of Performance Measure Data for the Federal Information Security Management Act (FISMA) Needed Improvement at Four Centers and NASA Headquarters" (Report No. IG-07-023, September 6, 2007)
Sensitive But Unclassified – Not for Public Release

We reviewed selected IT systems at four NASA Centers and Headquarters to determine whether NASA had satisfied FISMA performance measure reporting requirements. We found that those Centers and Headquarters had not fully complied with the standards and guidance established by the National Institute of Standards and Technology (NIST), as required by FISMA. Of the 18 systems we reviewed, 15 systems lacked a NIST-compliant certification and accreditation (C&A), 13 systems had not undergone a security control review in the past year, and 6 systems lacked a tested contingency plan. Additionally, we found that NASA's databases contained inaccurate data on the systems we reviewed, and when we compared data from the databases with NASA's FISMA report for the second quarter of FY 2006, we found discrepancies. As a result, we concluded that NASA's FISMA performance measure data were unreliable indicators of the overall status of the Agency's IT security program. We recommended that NASA ensure compliance with NIST requirements and that NASA validate the performance measure data reported in the FISMA quarterly reports and retain documentary support for the reported data. Management's planned and completed corrective actions were responsive to our recommendations.

"Assessment of NASA's Certification and Accreditation Process"
(Report No. IG-07-035, September 26, 2007)
Sensitive But Unclassified – Not for Public Release

Office of Management and Budget (OMB) and NASA's OCIO requested that we provide, as a part of the FY 2007 FISMA compliance review, an early assessment of NASA's C&A process for unclassified systems categorized as moderate and high-risk impact. Overall, we found that OCIO's policies and procedures for the C&A process for unclassified systems were in compliance with FISMA requirements; however, the quality assurance function of the process could be improved. Specifically, we found inaccuracies and inconsistencies in C&A documentation for 11 of 13 security assessment reports we reviewed. Inaccurate and inconsistent information in the security assessment report reduces the assurance that authorizing officials have the information they need to make a credible, risk-based decision about system accreditation—e.g., whether to authorize operation of an information system. OCIO immediately began taking corrective actions to address our concerns. We recommended that OCIO provide formal notice to the contractor and the contracting officer of our findings and take them into consideration with regard to the contract performance metric; increase oversight of deliverables provided by contractors; and formally remind system personnel of the importance of reviewing and verifying the accuracy of security assessment reports. NASA management concurred with the recommendations and is taking appropriate action.

"Federal Information Security Management Act: Fiscal Year 2007 Report from the Office of Inspector General" (Report No. IG-07-034, September 28, 2007)
Sensitive But Unclassified – Not for Public Release

FISMA requires agencies to report annually on the effectiveness of the agency's IT security program and requires Inspectors General to perform independent evaluations of their agency's information security programs and practices. We performed an annual independent assessment of NASA's IT security posture and provided the results to OMB. In a memorandum, we notified the Administrator of our plan to identify IT security as a management and performance challenge in NASA's *Fiscal Year 2007 Performance and Accountability Report*. We also noted that NASA had identified its IT security program as a material weakness, reportable in accordance with the Federal Managers' Financial Integrity Act, and that the IT security program should continue to be reported as a material weakness until all security weaknesses previously identified have been mitigated.

"Actions Needed to Ensure Scientific and Technical Information Is Adequately Reviewed at Goddard Space Flight Center, Johnson Space Center, Langley Research Center, and Marshall Space Flight Center" (Report No. IG-08-017, June 2, 2008)
Available on the Internet

We conducted this audit to evaluate and test NASA's guidance for the review, approval, and release of STI. We found that although the roles and responsibilities for reviewing and approving STI were adequately defined and documented in NASA guidance, the guidance was not adequately implemented at the four Centers we reviewed. Specifically, we identified 413 STI items that had been publicly released at those Centers during FYs 2005 and 2006 without the required reviews. We recommended that

- the four Center Directors implement a plan to increase awareness of STI review requirements contained in NASA guidance;
- NASA revise its STI guidance to require Center STI managers to timely notify STI authors whether their STI was approved for release and prohibit STI authors from publicly releasing STI before approval is received; and
- NASA revise its STI guidance to include "effectiveness of the STI review process" as one of the annual performance measures used to determine whether NASA is achieving compliance with internal guidance.

Management concurred with the recommendations and their proposed actions were responsive.

Intra-Agency Memorandums

Sale of Export-Controlled Items (March 2008)

In March 2008, we provided the NASA Office of General Counsel three referrals identifying individuals involved in the potential sale of items controlled under

International Traffic in Arms Regulations (ITAR). We recommended that cautionary letters be issued to those individuals explaining their obligations under ITAR and emphasizing the uncertainty inherent in selling defense articles and shuttle tiles in cyberspace. In one case, we also recommended that the Agency consider revising, updating, and strengthening its protocol for excessing property by working more closely with the NASA Export Control Office to devise procedures to prevent ITAR-controlled property entering the stream of commerce.

Lost and Stolen Laptop Computers (April 28, 2008)

We recommended that Agency management take action regarding recent reports of lost and stolen laptops and other computer equipment. Most of the reports pointed toward employee negligence as a contributing factor. NASA regulations require employees to protect and safeguard unclassified NASA information from unauthorized disclosure including protecting SBU information (e.g., information related to ITAR), which is often found on NASA laptops. We recommended that the Agency review its current policies on safeguarding SBU information with a view toward taking steps to raise or renew awareness of Agency regulations and safeguarding NASA assets from loss, theft, and misuse. On May 19, 2008, NASA issued a message to all NASA civil service employees highlighting employee responsibilities with respect to safeguarding equipment and electronic information and referencing applicable NASA regulations related to the safeguarding of Government property and electronic information.

Assignments in Progress

Our Office of Investigations is conducting several computer intrusion investigations involving NASA systems containing technical data covered by ITAR or Export Administration Regulations that are potentially at risk of unlawful access. For example, this work includes a multi-Agency investigation involving Romanian computer hackers. One of these hackers is being prosecuted by Romanian authorities; he has also been charged with conspiracy and nine counts of computer intrusion by the U.S. Attorney's Office of the Central District of California. We are also conducting other investigations involving the potentially unlawful disclosure of sensitive information covered by ITAR or Export Administration Regulations. In all of these investigations, this office continues to work with Agency senior leadership to rectify system weaknesses that allow for network intrusions by outsiders and unauthorized disclosures by NASA civilian and contract employees.

Our Office of Audits is currently conducting three assignments related to the transfer, control, and protection of critical technology and sensitive data. The results of these assignments should assist the Agency and the OIG in determining the extent to which NASA is carrying out its activities in compliance with Federal export control laws and other reporting requirements.

"Federal Information Security Management Act: Fiscal Year 2008 Report from the Office of Inspector General" (Assignment No. A-08-006-00; projected issue date, September 2008)
Sensitive But Unclassified – Not for Public Release

In accordance with FISMA, Title III of the E-Government Act, we are conducting our annual review of the Agency's information security and privacy program and will report the results to OMB at the end of the fiscal year. We are conducting our work at all NASA Centers and NASA Headquarters.

"Foreign National Access to NASA's Export-Controlled Technology" (Assignment No. A-08-005-00; projected issue date, December 2008)
Sensitive But Unclassified – Not for Public Release

The objective of this audit is to determine whether NASA has effectively controlled contractors' and grantees' transfers of critical technologies and technical information to foreign nationals and countries of concern. We plan to conduct our audit work at contractor locations.

"Audit of NASA Personal Identity Verification (PIV) Processes" (Assignment No. A-08-009-00; projected issue date, December 2008)
Will be available on the Internet

The audit objective is to evaluate the adequacy of NASA's personal identity verification (PIV) processes to ensure that required safeguards are in place to prevent unauthorized access to Agency facilities, systems, and data. Specifically, we will evaluate the adequacy of NASA's plans for managing the transition to PIV cards that are compliant with Homeland Security Presidential Directive/HSPD-12, "Policy for a Common Identification Standard for Federal Employees and Contractors."

Office of Audits Planned Projects

For FY 2009, our Office of Audits is planning two assignments related to addressing NASA's compliance with export control laws and regulations and the protection of scientific and technical information from illegal transfer. In addition to our annual FISMA reporting requirements, we also plan to conduct an audit concerning the identification and disposition of Space Shuttle Program export controlled property.

As NASA continues its transition from the Space Shuttle Program to the Constellation Systems Program, safeguarding sensitive technologies will become even more critical to the safety of NASA missions and national security. As the transition unfolds, we plan to direct our focus to include not only the disposition of Space Shuttle Program assets but also the development of new technology, ensuring that key controls are in place to provide adequate assurance that sensitive technologies of next-generation efforts are protected.

If you or your staff would like to meet with us to further discuss any of the issues addressed in this letter, please contact Ms. Evelyn Klemstine, Assistant Inspector General for Auditing, at 202-358-2572.

Sincerely,

signed

Thomas J. Howard
Deputy Inspector General

cc:
NASA Administrator
Deputy Assistant Administrator, Office of Security and Program Protection
Deputy Chief Information Officer for Information Technology Security
Director, Export Control and Interagency Liaison Division

Identical letter to:
The Honorable Richard Shelby
Ranking Member
Subcommittee on Commerce, Justice, Science, and Related Agencies
Committee on Appropriations
United States Senate

The Honorable Bill Nelson
Chairman
Subcommittee on Space, Aeronautics, and Related Sciences
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable David Vitter
Ranking Member
Subcommittee on Space, Aeronautics, and Related Sciences
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Joseph I. Lieberman
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Susan M. Collins
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Alan B. Mollohan
Chairman
Subcommittee on Commerce, Justice, Science, and Related Agencies
Committee on Appropriations
House of Representatives

The Honorable Rodney P. Frelinghuysen
Ranking Member
Subcommittee on Commerce, Justice, Science, and Related Agencies
Committee on Appropriations
House of Representatives

The Honorable Henry A. Waxman
Chairman
Committee on Oversight and Government Reform
House of Representatives

The Honorable Thomas M. Davis III
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

The Honorable Mark Udall
Chairman
Subcommittee on Space and Aeronautics
Committee on Science and Technology
House of Representatives

The Honorable Tom Feeney
Ranking Member
Subcommittee on Space and Aeronautics
Committee on Science and Technology
House of Representatives