National Aeronautics and
Space Administration

Office of Inspector General
Washington, DC 20546-0001

February 4, 2010

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-10-007)

Dear Madame Chairman:

This letter responds to Public Law 106-391, "National Aeronautics and Space Administration Authorization Act of 2000," that directs the NASA Inspector General to 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) and 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.

During the past year, the NASA Office of Inspector General (OIG) continued to work closely with NASA's Office of the Chief Information Officer (OCIO), Office of Protective Services (OPS), Office of the 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 NASA's 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 the individuals found responsible are held accountable. We also continue to work with OCIO and OPS to address related counter-intelligence and counter-terrorism issues.

During the past year, the OIG has conducted a series of audits, investigations, and reviews to meet its requirements in this area. This letter provides summary information about our work. We will continue to provide you copies of each OIG product and will be pleased to discuss any of these reports with you or your staff.

OIG Assessment of NASA's IT Security Program

For fiscal years (FY) 2006 and 2007, NASA has reported IT security as a material weakness in the Administrator's annual Statement of Assurance. During this period, NASA implemented various solutions in an attempt to improve its IT security. These solutions have resulted in continued incremental improvements across NASA's IT infrastructure; however, several significant challenges remain. Specifically, not all solutions have been fully implemented and continued breaches of NASA computer systems have resulted in the theft of sensitive data related to Agency programs, which adversely affected NASA's mission and resulted in millions of dollars in losses.

The Agency reported in FYs 2008 and 2009 that it had taken steps to prevent future breaches of its computer systems by making progress on two key IT security initiatives. First, the Cyber Threat Analysis Program proactively detects intrusions into NASA's cyber assets. The program includes threat analysis, identification, and reporting as well as advanced data forensics. Second, the Security Operations Center (SOC) project consolidates Agency security operations and incident response capabilities for NASA computer networks and systems. When fully operational in April 2010, NASA expects the SOC to provide end-to-end visibility and real-time monitoring of its computer networks and systems.

In addition, the Agency reported making significant progress in implementing corrective actions related to IT security weaknesses identified by the OCIO's comprehensive IT security assessment as well as meeting its annual requirements under the Federal Information Security Management Act (FISMA). The requirements include providing an overall view of the Agency's security and privacy program to the Office of Management and Budget.

Based on the Agency's reported progress in improving IT security, the OCIO concluded in 2008 that IT security no longer needed to be reported as a material weakness in the Administrator's annual Statement of Assurance, provided certain conditions were met. These conditions included substantiated progress in implementing corrective actions related to IT security weaknesses, full implementation of the SOC, and favorable results from regular security compliance reviews.

The OIG performed a limited review in 2008 to independently assess NASA's actions to improve IT security. We found that NASA had closed 91 percent of the OIG recommendations to improve IT security in FYs 2005 through 2007, established the Cyber Threat Analysis Program, completed planning for the SOC, and improved compliance with FISMA requirements for its systems to be certified and accredited.

Based on our limited review, we agreed with the OCIO's conclusion that IT security need no longer be reported as a material weakness. However, the threat to NASA's computer networks and systems is tangible and evolving, both in scope and sophistication. Therefore, we included IT security in our November 2009 report identifying "NASA's Most Serious

Management and Performance Challenges" to ensure that the necessary attention and resources are directed toward fully implementing a reliable IT security program.

On January 5, 2009, the Office of External Relations announced its annual audit of the NASA Export Control Program (ECP) to be conducted at each Center. The purpose of this audit "is to ensure adequacy of the overall NASA ECP; to verify, via sampling, that required screening and licensing procedures are regularly followed; and to confirm that required documents are maintained in compliance with the requirements of the EAR [Export Administration Regulations] and the ITAR [International Traffic in Arms Regulations]." The ECP audits, which were completed between January and March 2009, found overall compliance with NASA's ECP and export control regulations. While common weaknesses were identified in the area of training and specific instances of failure to adhere to established procedures, none of these weaknesses appear to have resulted in reportable violations of ITAR or EAR.

OIG Products Issued in FYs 2008 and 2009

Since our previous letter to you in July 2008, we issued five products that directly or indirectly related to assessing 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 that could place NASA's export-controlled technologies and data at risk of being stolen or compromised.

"Federal Information Security Management Act: Fiscal Year 2008 Report from the Office of Inspector General" (Report No. IG-08-031, September 30, 2008) *Sensitive But Unclassified – Not for Public Release*

FISMA requires agencies to report annually on the effectiveness of their IT security and privacy programs and requires Inspectors General to perform independent evaluations of these agency programs. We reviewed system security certification and accreditation (C&A) documentation for a representative sample of NASA's non-national security systems. We found that all 39 Agency systems in our sample met FISMA requirements for system C&A. However, only 3 of the 6 external (contractor) systems in our sample complied with system C&A requirements. We also found that NASA could improve its processes for remediating identified IT security weaknesses. For example, plans of action and milestones (POA&Ms) were not always created to address known IT security weaknesses. In addition, when POA&Ms were developed, the Agency did not have an effective process for monitoring progress on POA&M activities. Our review found that NASA needed to improve its POA&M process and strengthen oversight of external systems in accordance with FISMA.

"NASA's Processes for Providing Personal Identity Verification (PIV) Cards Were Not Completely Effective in Meeting Federal Requirements" (Report No. IG-09-015, April 27, 2009) *Available on the Internet*

We evaluated the adequacy of processes put in place by NASA to prevent unauthorized access to Agency facilities, computer systems, and data. Specifically, we examined whether

NASA's process for issuing employee and contractor personal identity verification (PIV) cards complied with Homeland Security Presidential Directive 12, "Policy for a Common Identification Standard for Federal Employees and Contractors." We found that NASA issued more than 70,000 PIV cards to staff and contractors from a non-accredited PIV card issuer. We also found that NASA did not ensure that staff with PIV card responsibilities received the training needed to competently perform their duties. Although these conditions increased the likelihood of issuing PIV cards to unauthorized individuals, we did not identify any instances of this occurring. We recommended that NASA take steps to ensure that PIV cards are issued only from accredited card issuers; individuals receive training appropriate to their PIV card role; and NASA computer systems that support the PIV card process be developed in accordance with Agency guidance. Management concurred with our recommendations and their proposed actions were responsive.

"Improvements Needed in NASA's Oversight and Monitoring of Small Business Contractor Transfers of Export-Controlled Technologies" (Report No. IG-09-018, July 14, 2009) *Available on the Internet*

To determine whether NASA maintained effective oversight and monitoring of contractor transfers of critical technologies and technical information to foreign nationals and countries of concern, we reviewed 13 contracts from 10 contractors: 4 large corporations, 2 universities, and 4 small companies with either Small Business Innovation Research (SBIR) or Small Business Technology Transfer (STTR) contracts. We found that NASA could improve its oversight and monitoring of small business contractor transfers of critical technology and technical information. Although the large corporations and universities we reviewed generally had adequate procedures to protect export-controlled technology from illegal transfer, the procedures at the small business contractors did not adequately protect export-controlled technology. Specifically, we found a lack of awareness of export control regulations among small business contractors and small business procurement personnel. As a result, small business contractors are at increased risk of improperly releasing critical technology and technical information. We recommended that NASA monitor policy as implemented at other Federal agencies and amend its policy to incorporate the best practices; require contracting officers to monitor and oversee contractors' compliance with export control regulations; and expand its export control outreach efforts to include personnel involved in administration of SBIR/STTR contracts and small business contractors. Management's planned corrective actions were responsive to our recommendations.

"Final Memorandum on the Audit of the Reporting of NASA's National Security Systems" (Report No. IG-09-024, August 28, 2009) *Sensitive But Unclassified – Not for Public Release*

We evaluated the adequacy of NASA's process for certifying and accrediting its national security (classified) IT systems and determined that the process generally provided adequate information security protection. However, we found some systems lacked appropriate C&A documentation, which NASA subsequently has addressed. All of the report recommendations are resolved or closed.

"Federal Information Security Management Act: Fiscal Year 2009 Report from the Office of Inspector General" (Report No. IG-10-001; November 10, 2009) *Sensitive But Unclassified – Not for Public Release*

We conducted our annual review of the Agency's compliance with FISMA and Agency privacy management requirements and provided the results to the Office of Management and Budget in November 2009. This review examined systems from all 10 NASA Centers, NASA Headquarters, and the NASA Shared Services Center to evaluate NASA's compliance with FISMA and Agency privacy management requirements. Overall, we found the Agency complied with privacy management requirements, although we identified internal control weaknesses related to the Plan of Action and Milestones process, operating system configuration management, security controls testing, and contingency plan testing. In addition, we found that oversight for external systems could be improved.

Incident Reports and Referrals

The synopses below concern incidents either investigated by us or issues brought to our attention that involved the loss, theft, or inappropriate release of sensitive data that resulted in the filing of police reports, inter/intra-agency notifications, or formal referrals to NASA management for action.

Loss of NASA Laptop that Contained Sensitive Information (August 2008)

A NASA employee lost a laptop containing sensitive data on the Avionics System for the Atlas V. The employee filed a report with NASA detailing the circumstances under which the laptop was lost and also filed a report with the local police department.

Release of an Unmarked Export-Controlled Document to the Internet (September 2008)

A NASA contract employee doing routine research on the Internet found an unmarked export-controlled document that contained SBU information on the Upper Stage Program of Ares I. The contractor notified the appropriate Center's export control office of the document discovery. In addition, the contractor conducted an internal investigation to determine the extent and scope of this violation and concluded that the unauthorized release of this document was not the result of any action on its part and that the release of this document had no impact on national security.

Computer Compromises and Theft of Export Restricted Data from the Jet Propulsion Laboratory (January 2009)

The OIG notified the Agency of systemic IT deficiencies discovered during the course of an investigation into unlawful computer intrusions at the Jet Propulsion Laboratory (JPL). The OIG determined that the intrusion resulted in the theft of approximately 22 gigabytes of program data, which was illegally transferred to an Internet Protocol (IP) address in China;

that the stolen data included information protected under ITAR and EAR; and that a significant contributing factor to the loss was inadequate security settings at JPL, which allowed the intruder access to a wide range of sensitive data. In a memorandum summarizing our findings, we recommended that NASA immediately assess JPL's IT security to ensure that JPL's systems comply with IT security standards. We also recommended that the Agency ensure that all reporting requirements regarding the loss of ITAR and EAR data were met in connection with this incident, and recommended the Agency take this incident into account when assessing contract performance. NASA Headquarters officials responded that they had discussed the matter at length with JPL and approved a corrective action plan to address our findings and recommendations.

Stolen NASA Laptop that Contained Sensitive and Export-Controlled Information (June 2009)

In June 2009, a NASA laptop was stolen from an employee's locked rental car in San Francisco, California. The laptop contained SBU and ITAR data pertaining to the Ares I. A police report was filed and specifics about the stolen laptop were entered in the National Crime Information Center and the National Stolen Computer registry. The applicable Center's Protective Services Office is conducting a damage assessment relative to the loss and possible compromise of the SBU and ITAR information on the laptop.

Stolen NASA Employee's Suitcase Contained ITAR Material (June 2009)

In June 2009, the Office of External Relations reported to the Department of State that a NASA employee had a suitcase stolen at the Seattle, Washington, Sea-Tac Airport that contained ITAR material. The suitcase contained a hardcopy set of detailed drawings (more than 700 pages) of a model of the Orion Launch Abort Vehicle and two disk drives with a variety of files containing detailed information about the Orion Crew Exploration Vehicle. The files on the disk drives were encrypted. A police report was filed and authorities were tracking the use of a credit card also contained in the suitcase.

Assignments in Progress

The OIG is conducting several computer intrusion investigations involving NASA systems containing technical data covered by ITAR or EAR. This work includes multi-Agency investigations involving hackers in Italy, Portugal, Sweden, Russia, and China. We are also conducting other investigations involving the potentially unlawful disclosure of sensitive information covered by ITAR or EAR. In all of these investigations, we continue to work with law enforcement agencies and NASA officials to identify and remedy systemic weaknesses that allow for network intrusions by outsiders and unauthorized disclosures by NASA civilian and contract employees.

Additionally, the OIG is currently conducting an audit related to the transfer, control, and protection of critical technology and sensitive data. The results of this audit should assist NASA in determining the extent to which it is in compliance with Federal export control laws and other reporting requirements. In addition, the OIG is examining the effectiveness

of NASA's management, operational, and technical controls for ensuring the confidentiality, integrity, and availability of data from NASA's Enterprise Document Management System.

Planned OIG Projects

For FY 2010, the OIG is planning an audit examining NASA's compliance with export control laws and regulations and the protection of scientific and technical information from illegal transfer. Specifically, this audit will include an assessment of the identification and disposition of export-controlled property associated with the Space Shuttle Program. As NASA winds down the Space Shuttle Program, the protection of sensitive technologies will become even more critical to national security and the safety of NASA missions. As the Space Shuttle Program draws to a conclusion, we plan to not only focus on the disposition of Space Shuttle Program assets but also ensure that controls are in place to provide adequate assurance that sensitive technologies of next-generation efforts are protected from loss or theft.

If you or your staff would like to meet with us to discuss any of the issues addressed in this letter, please contact Debra Pettitt, Acting Assistant Inspector General for Auditing, at (202) 358-3725.

Sincerely,

signed

Paul K. Martin
Inspector General

cc: Charles F. Bolden, Jr.
NASA Administrator

William B. Waits
Deputy Assistant Administrator, Office of Security and Program Protection

Jerry Davis
Deputy Chief Information Officer for Information Technology Security

John F. Hall 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 Science and Space
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable David Vitter
Ranking Member
Subcommittee on Science and Space
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 Frank R. Wolf
Ranking Member
Subcommittee on Commerce, Justice, Science, and Related Agencies
Committee on Appropriations
House of Representatives

The Honorable Edolphus Towns
Chairman
Committee on Oversight and Government Reform
House of Representatives

The Honorable Darrell Issa
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

The Honorable Gabrielle Giffords
Chairman
Subcommittee on Space and Aeronautics
Committee on Science and Technology
House of Representatives

The Honorable Pete Olson
Ranking Member
Subcommittee on Space and Aeronautics
Committee on Science and Technology
House of Representatives