National Aeronautics and
Space Administration

Office of Inspector General
Washington, DC 20546-0001

December 17, 2012

TO: Charles F. Bolden, Jr.
Administrator

FROM: Paul K. Martin
Inspector General

SUBJECT: NASA's Efforts to Encrypt its Laptop Computers

On October 31, 2012, a NASA-issued laptop was stolen from the vehicle of a NASA Headquarters employee. The laptop contained hundreds of files and e-mails with the Social Security numbers and other forms of personally identifiable information (PII) for more than 10,000 current and former NASA employees and contractors. Although the laptop was password protected, neither the laptop itself nor the individual files were encrypted.[1] As a result of this loss, NASA contracted with a company to provide credit monitoring services to the affected individuals. NASA estimates that these services will cost between $500,000 and $700,000.

This was not the first time NASA experienced a significant loss of PII or other sensitive but unclassified (SBU) data as a result of the theft of an unencrypted Agency laptop. For example, in March 2012 a bag containing a government-issued laptop, NASA access badge, and a token used to enable remote-access to a NASA network was stolen from a car parked in the driveway of a Kennedy Space Center employee. A review by information technology (IT) security officials revealed that the stolen computer contained the names, Social Security numbers, and other PII information for 2,400 NASA civil servants, as well as two files containing sensitive information related to a NASA program. As a result of the theft, NASA incurred credit monitoring expenses of approximately $200,000. Other significant losses occurred in November 2011 with the theft of an unencrypted laptop containing sensitive IT security information from the car of an employee of the Ames Research Center, and the March 2011 theft of an unencrypted laptop containing export-controlled data, including sensitive information relating to the International Space Station, from the car of a Johnson Space Center employee.

[1] Encryption protects data from unauthorized access by converting it into unreadable code that cannot be deciphered easily. Data encryption on computers generally uses a mathematical algorithm to scramble the information to make it unreadable without a key to "unlock" or convert the information to a readable form.

Following the October 31 theft, you accelerated NASA's effort to encrypt the hard drives of the Agency's laptop computers, directing that all laptops be encrypted by December 21, 2012.[2] You further directed that after that date, employees would not be permitted to remove from NASA facilities any laptop that has not been encrypted.[3]

In light of the significance of the recent laptop thefts and our prior work in this area, the Office of Inspector General (OIG) initiated an expedited review to examine NASA's ongoing efforts to encrypt Agency laptops and whether the December 21 target completion date will be met. This memorandum contains the results of our review.[4]

Background

NASA has issued tens of thousands of portable electronic devices to its employees and contractors, including a large number of laptop computers. Many of these laptops process and store SBU data, including PII such as Social Security numbers and sensitive data related to NASA programs and operations.

NASA has a variety of options available to help prevent unauthorized access to data stored on its laptop computers. These include password protecting the computer, encrypting individual files, or encrypting the computer's hard drive, which is commonly referred to as full-disk or whole-disk encryption. Password protecting a computer using the machine's operating system is the least effective way to prevent unauthorized access given the relative ease by which hackers can bypass a computer's logon/password screen and gain full access to stored data. Encrypting individual computer files prevents unauthorized access to those files, but requires ongoing awareness and a proactive effort by the user to identify and encrypt specific files. Full-disk encryption initially encrypts all data and programs on the computer and automatically encrypts new data and programs as they are added. Because of this, full-disk encryption is the most effective way to ensure that sensitive data is not compromised if a laptop is lost or stolen.

[2] This directive was communicated via an Agency-wide e-mail on November 13, 2012. The e-mail also instructed employees "effective immediately" not to remove laptop computers containing sensitive information from NASA facilities unless whole-disk encryption software is enabled or the sensitive files are individually encrypted, to purge from laptops sensitive files no longer needed "for immediate work purposes," and to refrain from storing sensitive data on smart phones or other mobile devices. Ten days later, the Ames Center Director imposed even greater restrictions on Ames employees by forbidding them from taking any laptop from the Ames campus that did not have whole-disk encryption enabled and instructing employees to return any unencrypted laptops that were offsite. The Ames Director said he was taking this action because two Ames laptops, both unencrypted, had been stolen since your November 13 directive.

[3] Users can apply for a waiver from this requirement, but any laptop that receives a waiver must remain on NASA premises. Laptops related to life safety systems, mission critical systems, and multi-user systems that do not store or contain sensitive date, PII, SBU, or ITAR [International Traffic in Arms Control] information are eligible for a waiver. Waivers are valid for 1 year and must be renewed annually.

[4] In this review, we examined the status of encryption efforts for Agency laptops only. We are examining the security of other mobile devices used at NASA such as iPhones, iPads, and Blackberries in a separate audit initiated earlier this year.

NASA owns or leases upwards of 60,000 desktop and laptop computers. As of December 2012, approximately 47,000 of these machines are managed by HP Enterprise Services (HP) through the NASA Consolidated End User Services known as the ACES contract.[5] The remainder were acquired by NASA Centers and Mission Directorates through other means and are managed by NASA directly. As discussed in more detail below, NASA officials cannot identify with any certainty the exact numbers of ACES and non-ACES laptops in the Agency's possession. However, as of December 7, NASA was tracking the encryption status of more than 20,000 ACES-managed and more than 14,000 NASA-managed laptops.

In past reviews of NASA IT security issues, we found that responsibility for NASA IT equipment generally resides with one of three entities:

NASA's Office of Chief Information Officer (OCIO) – based at NASA Headquarters, the OCIO controls the Agency's "institutional" systems and networks used to support administrative functions such as budgeting and human resources. The institutional systems support the day-to-day work of NASA scientists, engineers, and mission support personnel and include networks, data centers, Web services, desktop computers, and other end-user tools such as e-mail and calendaring.

Center Chief Information Officers – While the Agency CIO is responsible for developing IT security policies and implementing an Agency-wide IT security program, each Center has a CIO in charge of Center IT operations. The Center CIOs have the responsibility to ensure that Center IT investments, support, services, policies, and practices align with Federal and Agency requirements, and ensure Center compliance with the Agency's IT and information management policies.

Mission Directorates – IT assets on NASA's mission computer networks are funded by one of the Agency's three Mission Directorates, which are responsible for ensuring IT security on their systems and equipment, including laptops. The Mission Directorates each employ a CIO and IT staff responsible for implementing security controls on their IT assets, and these individuals report to their respective Mission Directorates rather than the OCIO.

Prior OIG reviews have concluded that this decentralized governance model has resulted in inconsistent implementation of NASA IT security policy.

NASA reported the loss or theft of 45 laptops in 2011 and 62 laptops in 2012. Recognizing that such losses are inevitable, the Agency has taken steps to protect data stored on its laptops. For example, NASA policy requires that employees encrypt sensitive data on laptops using approved encryption software and reminds employees of this responsibility as part of mandatory annual IT security awareness training. In addition, since at least 2007 NASA has been working toward full-disk encryption of its laptops. However, this effort – referred to by NASA as the Data-At-

[5] HP Enterprise Services is a division of Hewlett Packard and provides global business and technology services.

Rest or DAR initiative – has been extremely slow and the Agency has repeatedly extended the deadline for completion of the project.[6]

As of October 26, 2012 – less than a week before the theft of the laptop from the NASA Headquarters employee – HP reported 8,376 ACES-managed laptop computers had been encrypted, with the remainder scheduled to be completed by March 2013. Prior to the October 31 theft, no effort was made to centrally track the encryption status of non-ACES machines.

NASA's Whole-Disk Encryption Effort Has Suffered Repeated Delays

In December 2010, NASA signed the ACES contract with HP to obtain a wide range of IT services for the Agency and its employees, including laptop and desktop computers and related support. The ACES contract replaced NASA's previous IT contract with Lockheed Martin Corporation (Lockheed) known as the Outsourcing Desktop Initiative (ODIN).

Under the ACES contract, HP was to assume responsibility from Lockheed in three waves, with specific "phase-in" and "implementation" dates assigned to each wave. During Wave 1, HP would begin phase-in at Dryden Flight Research Center, Goddard Space Flight Center, Kennedy Space Center, and Headquarters beginning on January 3, 2011, with a completion date of July 1, 2011. Wave 2 included the NASA Shared Services Center (NSSC), Stennis Space Center, Glenn Research Center, Marshall Space Flight Center, and the Jet Propulsion Laboratory with initiation and completion dates of March 1 and September 1, 2011, respectively. Wave 3 was scheduled to cover Johnson Space Center, Langley Research Center, and Ames Research Center beginning on May 1 and completing on November 1, 2011. According to the contract, HP was to "assume full responsibility" for a range of specified IT services on the implementation date at each location.

One of the services HP was contractually required to provide was full-disk encryption. Specifically, HP was to "provide DAR Services that encrypt all data on each Agency desktop and laptop" computer. The contract did not specify a particular DAR solution, but stated that the solution should meet a number of requirements including "provid[ing] full disk encryption for internal hard drives." It also stated that NASA's current DAR solution, "McAfee Endpoint Encryption," was "in the process of being implemented" and that HP would be responsible for supporting the Agency's "current DAR infrastructure . . . until [HP]'s proposed solution is in place and accepted by [NASA]." Finally, the contract provided that "[f]or any remaining systems to which the DAR solution has not been applied and for which the application . . . has not been waived by the Government, the DAR solution shall be applied on the next system refresh" and that if HP brought in new equipment "the DAR solution shall be applied at that time."[7] With regard to non-ACES computers, HP was required to provide DAR software licenses but NASA was responsible for installing the software on the Agency-managed equipment. According to the NASA Project Executive for the ODIN contract, when that contract

[6] In February 2012, NASA's Chief Information Officer and I testified at a House of Representatives oversight hearing that examined the Agency's IT security. At the hearing. I noted that at that time only 1 percent of NASA portable devices (including laptops) were fully encrypted compared to a Government-wide encryption rate for these devices of 54 percent.

[7] A "system refresh" generally refers to replacement of an older piece of IT hardware by a newer model. Budgets permitting, most end-user IT hardware is refreshed every 3 years.

expired on November 1, 2011, a small percentage of the computers managed by ODIN were equipped with McAfee Endpoint Encryption software (McAfee Endpoint).

NASA and HP officials told us that under the ACES base contract, HP initially planned to replace all existing ODIN equipment with HP equipment in three waves and that the new equipment was to include a preloaded DAR solution. Accordingly, under the original schedule DAR would have been implemented on all ACES-managed laptops by November 1, 2011. In addition, HP was to deliver, but was not responsible for installing, a DAR solution for the NASA-managed computers.

However, for a variety of reasons, the transition from ODIN to ACES was troubled from the start and events did not unfold as planned. First, Lockheed protested the contract award to HP and this protest was not resolved until April 2011. As a result, HP began the phase-in process 3 months later than originally planned and did not actually assume full responsibility from Lockheed at all NASA Centers until November 1, 2011.

Once the bid protest was resolved, HP took several additional weeks to fully staff up and did not begin to replace ODIN equipment with new machines until June 2011, leaving only 5 months to complete the process for all NASA Centers by the November 1 deadline specified in the base contract. According to witnesses we interviewed, NASA officials did not believe it was feasible for HP to replace approximately 47,000 computers Agency-wide in this shortened timeframe. Accordingly, at NASA's urging HP agreed to purchase from Lockheed thousands of ODIN computers still in use at NASA when the ODIN contract expired. As noted above, the vast majority of these computers were not equipped with a DAR solution. Consequently, acquiring the ODIN computers presented HP with the challenge of having two sets of computers on which to implement a DAR solution: the new ACES-configured machines and the older ODIN computers.

Another issue that contributed to the whole-disk encryption delay was selecting a DAR solution that was compatible with the different computer platforms and operating systems in use at NASA. As noted above, NASA's DAR solution at the time the ACES contract was signed was McAfee Endpoint, and this software had been installed on a small percentage of ODIN computers. However, this software was incompatible with Macintosh (Mac) computers and with computers running Linux-based operating systems. According to the Project Executive for the ODIN contract, approximately one-third of the laptop computers in use at the Agency were Macs or Linux-based.

HP and NASA did not select a replacement DAR solution until August 2011 – 4 months after the bid protest was resolved – and then spent several additional months evaluating that solution for compatibility with the various types of computers in use at the Agency. Accordingly, the new DAR solution was first implemented for a pilot group of users at the end of March 2012. Although HP had begun replacing ODIN laptops before this date in accordance with a revised refresh schedule, the new laptops did not have whole-disk encryption. Indeed, we found that even after HP and NASA had settled on the current DAR solution, not all new laptop computers provided to NASA employees were delivered with the solution installed.

Finally, HP ran into a series of obstacles when installing the DAR solution, particularly on the older ODIN equipment. HP's approach for installing the encryption software is to "push" the DAR solution to laptops using a remote tool. However, not all ODIN machines were compatible with the software program HP uses for this installation process. For these computers, HP had to manually install the DAR software, a time-consuming and costly effort. Other ODIN computers were simply too old, did not have sufficient hard drive space, or were otherwise unable to support the encryption software. Other computers lacked current backups, a requirement for the software to be installed.[8]

Moreover, the encryption process cannot be finalized without affirmative action by the computer user. Users receive an on-screen prompt explaining that the software is ready to be installed on their machine along with the estimated time to complete the encryption process, which can be anywhere from 2 hours to nearly a full day.[9] The user must then take several steps to initiate the encryption process. NASA officials said that many users failed to respond to the prompt, choosing to delay the encryption process due to the length of time required to complete it or their hesitancy to accept the software download. This user reluctance caused further slippage to the implementation schedule.

Given these problems and the resulting delays, NASA and HP agreed to revise the deadline for completing the DAR process on all ACES machines to March 2013. In addition, HP agreed to credit NASA $15 million over the first 2 years of the contract as a result of various performance issues, including the refresh and DAR delays.[10]

NASA Adjusts DAR Plan in Response to Loss of Ames Laptop

As noted above, in November 2011 an unencrypted laptop computer containing sensitive IT security information was stolen from the car of an Ames employee. This theft caused NASA to alter its DAR rollout plan and undertake an effort to ensure that the laptops of "critical users" would be the first to be fully encrypted. On November 15, NASA's Deputy CIO for IT security sent an e-mail to Center and Mission Directorate CIOs requesting that they "ensure that all staff who house PII or SBU data on their laptop encrypt their laptop hard drive, especially . . . technical staff and high profile users." The e-mail did not provide further guidance on the process Center CIOs should use to identify such users, nor did it establish a deadline for completing laptop encryption for these users. Moreover, because the Agency and HP had not yet completed their evaluation of the new DAR software, the e-mail did not inform the CIOs which DAR solution they should use.

Approximately 6 weeks later, on January 31, 2012, the NASA CIO issued informal guidance to assist Center CIOs in identifying critical users. This communication defined a critical user as anyone whose computer contained sensitive data, including International Traffic in Arms

[8] The encryption process is unsuccessful in a small percentage of the cases, and this can result in loss of data stored on the machine. A backup prior to encryption ensures that data can be recovered. An unsuccessful backup can occur for a number of reasons, including a prolonged period during which the laptop is not connected to a NASA network or issues that affect the computer's ability to connect to the backup servers.

[9] Users may continue to use their computers during the encryption process.

[10] NASA estimates it will spend more than $194 million on the first 2 years of the contract.

Regulations (ITAR), Export Administration Regulation , PII, SBU, procurement sensitive or financial data. The Center CIOs were instructed to provide their critical user lists to the OCIO by February 15, 2012. However, the OCIO did not receive lists from all Centers until March 31, and the number of critical users Center CIOs identified varied widely from a high of 279 at Langley to 31 at Stennis.[11] Surprisingly, Headquarters identified only 34 critical users apart from the OIG. In total, the lists identified 1,631 critical users Agency-wide. According to the former ACES Project Executive, all of these machines were fully encrypted by June 2012.

An OCIO official told us that NASA chose a Center-based rather than an Agency-wide approach for identifying critical users in order to give each Center the flexibility to match the Center's business and IT environments with user needs.

We spoke to the Center CIOs for Headquarters, Johnson, Goddard, and Marshall regarding the actions they took in response to the request to identify critical users and found that the process varied from Center to Center. The Johnson CIO told us that developing his Center's list was a process that evolved over several months. He said that the list Johnson provided the OCIO included members of the Center's IT Security team, IT Information Resources Directorate, and NASA OIG personnel. Later, Johnson expanded the group of critical users by canvassing Center mangers, although the Center did not update the list it provided to the OCIO.

At Goddard, CIO officials identified critical users using data the Center had previously collected regarding the categories of personnel that typically handle sensitive information. Using this method, Goddard identified 157 critical users, 20 of whom were OIG employees.

The Marshall CIO said that the Center's critical users were identified through a collaborative process with computer security officials in each Center organization. Ultimately, Marshall identified 242 critical users.

Headquarters CIO officials told us that in response to the Deputy CIO for IT Security's November 2011 e-mail, they identified as critical users IT Security personnel and several other individuals from the OCIO. However, they did not reach out to the IT points of contact (POCs) in any other Headquarters offices to request that they identify critical users in their organizations. Although these officials told us they intended to request this information from the POCs before the summer of 2012, they did not follow through on this task. In fact, the Headquarters POCs were not asked to identify critical users in their organizations until November 16, 2012 – more than 2 weeks after the laptop theft that triggered the Administrator's December 21 encryption deadline. For this reason, the Headquarters employee whose computer was stolen on October 31 was not identified as a critical user and her laptop was not encrypted as part of the DAR rollout to critical users.[12]

[11] The OIG's more than 200 laptop computers were among the first machines encrypted by ACES. This was in response to a specific request to NASA IT security officials from the OIG.

[12] According to an OCIO official, this employee had an older computer that was scheduled to be replaced in a few months with a new model with DAR software preloaded.

NASA Unlikely to Meet December 21 Encryption Deadline

As a result of the October 31 laptop theft, NASA accelerated the deadline by which all ACES-managed laptop computers were to be equipped with a DAR solution from March 2013 to December 21, 2012. The Agency estimates that this expedited encryption effort will cost at least $259,000, not including the time civil servants have devoted the project. The Agency also established the same deadline for encrypting non-ACES machines.

In our judgment, it is extremely unlikely that the Agency will meet its December goal primarily because the Agency does not have a full account of the number of ACES and non-ACES laptops in its possession. Without knowing the full universe of laptops that require encryption, the Agency cannot be sure that all of its laptops are protected with whole-disk encryption software.

Following establishment of the December 21 deadline, Headquarters and Center officials began making weekly reports to the Administrator's Office related to the progress of the DAR initiative. We reviewed the first four of these reports, which purport to show the number of laptops on which DAR is required, the number for which the DAR process has been completed, and the percent complete as of November 15, 21, and 30 and December 7. The first report reflects only ACES laptops while the three later reports include figures for non-ACES machines as well.

According to the December 7 report, DAR encryption software has been installed on 84.4 percent of ACES and non-ACES laptops. However, this figure is inherently unreliable because, as is clear from the examples below, the Agency has little certainty as to the total number of laptops in use at NASA.

- We found that the number of ACES laptops being reported to the Administrator's Office differed from the number HP is tracking on its internal reports. For example, the December 7 report to the Administrator identified 20,595 ACES laptops requiring DAR installation. In contrast, on December 7 internal HP documents listed 25,414 ACES laptops requiring DAR installation – a discrepancy of 4,819 laptops.

- The number of laptops reported to the Administrator has fluctuated widely from week to week. For example, in just 2 weeks the reported population of ACES computers at Ames increased by 75 percent. The November 15 report indicated that Ames had 554 ACES laptops, of which 498 had been encrypted, for a completion rate of 89.9 percent. However, the November 21 report indicated that Ames had 627 ACES laptops, of which 445 had been encrypted, for a 71 percent completion rate.[13] The numbers changed again on the November 30 report when Ames reported 968 ACES laptops requiring encryption, with 864 complete for an 89.3 percent completion rate.

- While NASA's inability to identify the size of its ACES laptop computer inventory is disconcerting, it appears that there is even less centralized control over and accountability for non-ACES equipment. With respect to the ongoing DAR encryption effort, the number of

[13] While the number of Ames laptops identified as requiring encryption increased on this second report, the number of laptops purportedly encrypted decreased from the previous week's report by 53.

non-ACES laptops requiring encryption has increased by 32 percent over the course of 3 weeks.[14] For example, according to the November 21 report Dryden had 1,019 non-ACES laptops, of which 859 had been encrypted for a completion rate of 84.3 percent. However, on the November 30 report the number of non-ACES laptops plummeted to 217, of which only 15 had been encrypted for a completion rate of 6.9 percent. The December 7 report showed Dryden's non-ACES laptops decreasing again to 181, of which 41 were reportedly encrypted for a completion rate of 22.7 percent. Such wide fluctuations in the number of laptops requiring a whole-disk encryption solution raises concerns about the accuracy of NASA's Center- and mission-based controls over their IT equipment.

Our conversations with the Center CIOs confirmed our concerns about the accuracy of the Agency's numbers regarding both the number of ACES and non-ACES laptops in use and the percentage of all laptops that have whole-disk encryption installed. For example, the Johnson CIO told us his Center was reporting 60 percent of its computers had completed the DAR process by November 30, including 81.4 percent of ACES computers and 38.2 percent of non-ACES computers. However, he also said he was not confident that all computers at the Center had been identified, noting that he had no authoritative database of active laptops at Johnson. Other Center CIOs expressed similar doubt that they will be able to accurately identify all non-ACES computers that require DAR and several said they are not confident that HP can accurately account for the full inventory of ACES computers.

In addition to the uncertainty regarding the number of ACES and non-ACES computers, NASA and HP have not fully addressed the technical challenges that have hindered the DAR installation process from the outset. Moreover, because HP is not responsible for installing DAR software on the tens of thousands of NASA-managed machines, NASA personnel need to be trained to complete the installation process.

Conclusion and Recommendations

This review examined a persistently troubling issue – the Agency's diffuse and decentralized control of its laptops and other computer equipment and, by extension, its lack of centralized oversight for the security of the data on these NASA-managed machines. Specifically, we found that NASA's full-disk encryption effort has been repeatedly delayed due to slow implementation of the ACES contract, the highly decentralized nature of IT management at the Agency, and a lack of sufficient internal controls. Moreover, the Agency does not have a reliable accounting of the number of ACES and non-ACES laptops in its possession and therefore will not likely be able to ensure that DAR software is installed on 100 percent of required machines by December 21, 2012.

While we have focused on laptop security in this review, we reiterate our findings from past audits that NASA needs to improve its Agency-wide oversight of the full range of its IT assets.[15]

[14] The November 21, 2012, report to the Administrator's Office identified 10,892 computers requiring DAR installation. That figure increased to 14,372 in the December 7 report.

[15] In several previous reports, the OIG recommended that the NASA CIO implement an Agency-wide inventory/tracking system for all IT components. See "NASA's Implementation of Patch Management Software Is Incomplete" (IG-06-007, March 17, 2006) and "Audit of NASA's Efforts to Continuously Monitor Critical

Moreover, although Federal law and NASA policy designate the Headquarters-based CIO as the official responsible for developing IT security policies and implementing an Agency-wide IT security program, we continue to find that the CIO has limited ability to direct NASA's Mission Directorates to fully implement CIO-recommended or CIO-mandated IT security programs.[16]

Based on the results of this expedited review, the OIG recommends that NASA take the following actions:

1. Ensure that the Administrator's prohibition on removing from NASA facilities any laptop that has not been fully encrypted (unless it has received a waiver from this requirement) is strictly enforced, including assigning a senior level official to coordinate with senior managers and IT officials at each NASA Center to monitor adherence to the directive.

2. Appoint a senior-level official to lead an expedited effort to develop accurate accounting for ACES and non-ACES laptops and for other mobile computing devices. This official should work closely with HP executives and NASA IT officials at Headquarters and the Centers to improve internal controls over the inventory of such machines and their DAR status.

3. Consider whether reducing the number of non-ACES devices would improve accountability for laptop computers.

4. Work with HP to develop procedures to ensure that all new or "refreshed" laptops provided to NASA employees and contractors have the appropriate DAR software pre-installed.

5. In light of the poor coordination and decentralized nature of the laptop encryption process, re-examine the role of Agency IT officials for safeguarding the security of NASA laptop computers and other mobile computing devices, and ensure that NASA managers at Headquarters, in the field Centers, and in the Mission Directorates understand their individual responsibilities for protecting the integrity of NASA information and data.

cc: Lori B. Garver
Deputy Administrator

Robert Lightfoot
Associate Administrator

Information Technology Security Controls," (IG-10-019, September 14, 2010). Although the OCIO agreed with these recommendations and established the IT Security – Enterprise Data Warehouse (ITSEC-EDW) as an inventory control mechanism, it does not appear that ITSEC-EDW is comprehensively or consistently capturing IT component information.

[16] An ongoing OIG audit examining NASA's IT governance structure will offer findings and recommendations for improving accountability across the full range of acquisition, management, and security of the Agency's IT assets.

David Radzanowski
Chief of Staff

Linda Cureton
Chief Information Officer

Janet Petro
Acting Director for Office of Evaluation

Richard Keegan
Associate Deputy Administrator

Rebecca Keiser
Associate Deputy Administrator for Strategy and Policy

Arthur Maples
Acting Assistant Associate Administrator

Michael French
Deputy Chief of Staff

Jonathan A. Herczeg
White House Liaison

Elizabeth Robinson
Chief Financial Officer

Michael Ryschkewitsch
Chief Engineer

Richard Williams
Chief Health and Medical Officer

Terrence W. Wilcutt
Chief Safety and Mission Assurance

Waleed Abdalati
Chief Scientist

Mason Peck
Chief Technologist

Michael Wholley
General Counsel

David Weaver
Associate Administrator for Communications

Brenda Manuel
Associate Administrator for Diversity and Equal Opportunity

Leland Melvin
Associate Administrator for Education

Michael F. O'Brien
Associate Administrator for International and Interagency Relations

L. Seth Statler
Associate Administrator for Legislative and Intergovernmental Affairs

Glenn Delgado
Associate Administrator for Small Business Programs

Jaiwon Shin
Associate Administrator for Aeronautics Research Mission Directorate

William Gerstenmaier
Associate Administrator for Human Exploration and Operations Mission Directorate

John Grunsfeld
Associate Administrator for Science Mission Directorate

Woodrow Whitlow, Jr.
Associate Administrator for Mission Support Directorate

Jeri Buchholz
Assistant Administrator for Human Capital Management

Bill McNally
Assistant Administrator for Procurement

Joseph S. Mahaley
Assistant Administrator for Protective Services

Olga Dominguez
Assistant Administrator for Strategic Infrastructure

Nancy A. Baugher
Director, Internal Controls and Management Systems

Eugene H. Trinh
Director, NASA Management Office

Jay M. Henn
Executive Director, Headquarters Operations

Michael Smith
Executive Director, NSSC

Simon P. Worden
Director, Ames Research Center

David D. McBride
Director, Dryden Flight Research Center

Ray Lugo
Director, Glenn Research Center

Christopher J. Scolese
Director, Goddard Space Flight Center

Charles Elachi
Director, Jet Propulsion Laboratory

Michael L. Coats
Director, Johnson Space Center

Robert Cabana
Director, Kennedy Space Center

Lesa B. Roe
Director, Langley Research Center

Patrick Scheuermann
Director, Marshall Space Flight Center

Richard J. Gilbrech
Director, Stennis Space Center