HOLD FOR RELEASE
UNTIL PRESENTED
BY WITNESS
Nov. 16, 2016

**Statement of**
**Reneé Wynn**
**Chief Information Officer**
**National Aeronautics and Space Administration**

**before the**

**Subcommittee on Information Technology**
**Committee on Oversight and Government Reform**
**U.S. House of Representatives**

Chairman Hurd, Ranking Member Kelly, and members of the Subcommittee, thank you for the opportunity to testify before you today about NASA's efforts to manage our information technology (IT) resources and protect national assets in an ever-changing threat landscape. The NASA Administrator and all of NASA's leadership considers this to be a very high priority.

As NASA's Chief Information Officer (CIO), my office provides IT products and services including policy and procedure for all of NASA. Currently about 17,100 civil servants and 40,000 contractors work at nine NASA Centers and one Federally Funded Research and Development Center, as well as several smaller satellite facilities. We also collaborate with space agencies around the world and have deep partnerships with researchers, engineers and scientists all over the world. Each day, hundreds of thousands of NASA personnel, contractors, academics and members of the public access some part of NASA's IT infrastructure – a complex array of 418 information systems with over 140,000 components geographically dispersed around the globe. This infrastructure plays a critical role in every aspect of NASA's mission, from controlling spacecraft to processing scientific data.

Last year, for example, the entire world watched as New Horizons sent back the first close-up images of Pluto, and we continued to make new discoveries about Mars that will help inform human missions there. This year, the world watched as American Astronaut Scott Kelly returned home from the International Space Station after 12 months of working off the Earth for the Earth. Recently, our Deep Space Network, which relies on NASA's IT infrastructure, was able to get in contact with STEREO-B which had been out of communication with us for over two years. Additionally, this year in space will pay scientific and medical dividends for years to come, helping pave the way for future astronauts to travel to Mars and beyond. The Orion spacecraft and the Space Launch System rocket that will carry us again to deep space continued to reach new milestones. In cooperation with our industry partners Boeing and SpaceX, we moved closer to commercial launches of astronauts from American soil. We are formulating missions to study dark energy, perform galactic and extragalactic surveys and to explore exoplanets. We learned more about our home planet and our challenging climate as newer Earth science missions began to return their data. Technology continues to drive exploration in space and in aeronautics where we have made advances toward a future in which we make air travel safer, cleaner and more efficient.

In support of NASA's many missions, the Office of the Chief Information Officer (OCIO) works to safeguard NASA's IT systems and their associated components from attack, assess them against Federal and Agency security requirements, and continuously monitor them for compromise and for the effectiveness of currently implemented security measures. Given the evolving threat of attacks, our work is never done.  Internal governance and infrastructure changes at NASA have already improved the Agency's security posture, but admittedly, more work remains, especially as the Agency evolves from a highly decentralized IT environment controlled by the Centers and Agency programs and projects to an enterprise IT environment that is more centrally managed and overseen by the Agency CIO.

Therefore, the remainder of my testimony today will summarize key achievements to date, as well as work that is underway to comply with new laws and Administrative directives to all Federal agencies. But before I address those topics, I believe it is important to look at some of the recent governance changes that NASA has made to further empower the CIO to effectively manage its IT network and thus reduce risk of unauthorized access to NASA's assets and data.

## NASA IT Governance Changes

NASA is fully committed to meeting the requirements of Federal laws such as the Federal Information Security Management Act (FISMA) of 2002, the Federal Information Security Modernization Act (also known as FISMA) of 2014, the Federal Information Technology Acquisition and Reform Act (FITARA) of 2014, and the Federal Cybersecurity Enhancement Act (FCEA) of 2015, along with additional security directives issued by the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS).

Over the last several years, NASA has made significant progress in updating IT security policies, processes, and procedures to support the ongoing enhancement and automation of information system monitoring and reporting.  As a result, Agency IT security staff have obtained more in-depth visibility into NASA systems, enabling improved responsiveness, and further supporting a risk-based security paradigm.  Some of the more recent changes include:

- Initiating a Business Services Assessment (BSA) review of how IT is delivered at the Agency (see enclosure);
- Increasing the responsibility, accountability and authority of the NASA CIO in order to drive efficiencies and cost-savings through the acquisition, deployment and management of IT across NASA;
- Using a tool known as Solutions for Enterprise-wide Procurement to help NASA manage a suite of government-wide IT products to meet the requirements of FITARA; and
- Aligning IT and mission strategy in order to achieve goals and measure performance while ensuring stakeholders are informed including:
    - Strengthening the Agency's ability to align IT resources with Agency missions, goals, programmatic priorities and statutory requirements;
    - Clarifying the scope of the Agency CIO's role with respect to program IT and mission IT decisions, as well as allowing the CIO to participate in major Agency decision making processes for Agency missions;
    - Holding the CIO accountable for Agency IT cost, schedule and performance through a new portfolio review process.  The CIO will also have new authority and greater visibility into the overall budget planning cycle, allowing me to spot IT resource problems at a mission level earlier on;
    - Increasing transparency of IT resources across the entire Agency; and

- Ensuring that the IT security policies and procedures are implemented at NASA Centers. NASA has recently realigned the reporting structure so that I, as the NASA CIO, have direct authority and oversight over the Center CIOs.

In addition, organizational changes within OCIO are contributing to NASA's improved IT security posture. For example, NASA recently hired its first Senior Cybersecurity Advisor who reports directly to me and serves as my senior technical expert on IT security, staying abreast of the threat environment not only at NASA but also threats to other Federal and non-Government networks that may in turn come to threaten NASA networks. Additionally, I have hired a permanent Chief Information Security Officer (CISO) who serves as NASA's Senior Agency Information Security Officer. She works with all our NASA Center CISOs as well as CISOs across the Federal Government on operational IT security and cybersecurity matters. The NASA Inspector General was correct about the need to have this critical position filled and our new Senior Agency Information Security Officer brings impressive experience and in-depth expertise. Both of these new officials are actively engaged with our Federal partners, thus ensuring that best security practices are implemented at NASA, and that NASA remains coordinated on and protected against threats. They will continue to meet with other Federal IT partners to leverage best practices for IT management and cybersecurity operations.

I am also engaging the private sector for support. While the Federal Government has made significant strides, I know that we do not have all the answers. I am leveraging the expertise of the private sector for advisory and technical services to ensure that our security posture at NASA is benefitting from lessons learned and best practices in the private sector.

## NASA IT Threat Environment

Like other Federal agencies, NASA's IT infrastructure is under constant attack from domestic and foreign adversaries. Decades of NASA aeronautics and space technology research and development represents billions of dollars in U.S. Government and aerospace industry investment. The very nature of NASA's mission, and the extremely important technical and intellectual capital produced therein, makes the Agency's information a valuable target for hackers, criminals and foreign enterprises. Many of these threats are well-resourced, highly motivated, and sophisticated. Therefore, there is no perfect, one-size-fits-all tool to predict, counter and mitigate the wide range of attacks across the Federal Government.

The collective actions of NASA's OCIO as well as information sharing with the DHS and other Federal agencies involved in cybersecurity are contributing to an improved security posture. When threats are detected, NASA personnel take immediate action and depending on the level of the threat, NASA alerts other Federal agencies involved with cyber intelligence issues, and partners with them to deter and thwart future attacks. For example, in FY 2015, the NASA Security Operations Center, which is responsible for cyber incident response at NASA, transitioned its incident management process to adhere to the DHS' U.S. Computer Emergency Readiness Team's (US-CERT) new Federal Incident Notification Guidelines[1]. NASA now categorizes all incidents and reports the information at the Federal-level to the US-CERT in near-real-time.

Here are two key metrics that reflect improvements NASA has recently made in its IT security environment:

- NASA has significantly reduced its cybersecurity risk measured by the DHS Cyber Hygiene report. One improved measure of performance, on public facing vulnerabilities, is "time to

[1] OMB Memorandum 15-01, "Updated DHS US-CERT Incident Notification Guidelines", pg. 12-13. October 3, 2014: https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-01.pdf

patch."  We have looked at the aggregate risk, as measured by DHS, and have reduced our vulnerabilities by 25 percent in the last eight months.

- With regard to NASA's FISMA implementation in FY 2016, we deployed a tool to enable identification of phishing attacks thereby reducing the workload on the end user to identify phishing attacks.  For FISMA 2016, we have made inroads on issues such as malware defense and network defense, and we have implemented a secure policy framework on email further reducing the amount of attacks a user would experience.

It is also important to point out that NASA is extremely proactive in our approach for handling breaches caused by human error through awareness and education.  NASA reaches out to every employee to notify them of best practices.  Employees must take mandatory training in order to retain access to our networks.  The Administrator and other senior leaders also have repeatedly stressed to all NASA employees that they will be held accountable for failing to adhere to our established procedures and policies.  Additionally, employees are warned before they take any NASA online training, for example, that any misuse of assigned accounts may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution.

While some Federal agencies, including NASA, have been criticized for our use of legacy IT systems, NASA must sometimes make limited exceptions for the continued use of legacy IT that is critical to the success of long-term Agency missions that were launched, in some cases, decades ago and which are still transmitting data back to NASA.  While some IT can be upgraded throughout the project life cycle, a subset of hardware, software applications and operating system components must remain in the state in which they were originally deployed.  In these instances, NASA actively monitors all aspects of system end-to-end functionality to assure any IT security risks are identified, contained and mitigated.

Another unique challenge that NASA has in terms of IT security is our statutory mandate to engage the public in our missions and much of that engagement is accomplished via our IT portals.  Our Open Data websites, for example, include more than 30,000 publicly-accessible datasets.  Therefore, NASA as a whole, and my office in general, must balance securing its IT resources with data accessibility to further global science and technology collaboration around the world.

## Work in Progress

Like all agencies, NASA is adjusting to new laws and directives designed to improve how the entire Federal Government improves its IT security posture.  While NASA is proud of the progress we have made, we recognize that more work remains to fully comply with new laws and policy.  We are making progress with:

- **Patching:**  Correcting deficiencies in the timeliness, completeness and tracking of the implementation of security patches is a multi-faceted issue with no simple answer.  For mission related software, I, as the CIO, was recently provided additional IT oversight responsibilities within NASA (see enclosure).  Additionally, NASA's deployment of the Continuous Diagnostic and Mitigation (CDM) tools will help the OCIO gain better insight into patching vulnerabilities

- **Einstein3A: (E3A):**  This capability will allow us to detect malicious traffic targeting NASA networks, but also prevent malicious traffic from harming our networks.  As required by DHS, we have worked diligently with DHS and our NASA Centers to deploy E3A.  While we have experienced some challenges around deploying this technology at some Centers, we are working with DHS to resolve technical issues and enable NASA to meet the December 18, 2016 deadline for full deployment.

- **CDM:** As required by DHS, NASA’s implementation of the CDM program has started with the initial operating phase beginning at our Kennedy Space Center in Florida. This is a necessary step to increase awareness, understanding and effectiveness when we roll CDM out across NASA. The NASA OCIO team has conducted our first lessons-learned evaluation on the CDM deployment at the Kennedy Space Center. We are also partnering with other agencies that have deployed CDM to ensure we have a transfer of knowledge and gain lessons learned from those agencies similar to ours that have already implemented CDM.
- **Incident Response Assessments**: NASA’s Incident Response Assessment Program demonstrates our capability to identify, protect from, detect, respond to and recover from issues facing our networks. We conduct assessments once a quarter and identify issues with our NASA-wide enterprise capability as well as those of the individual Centers. We develop process improvements and track those until the issue can be resolved. This is another key check on our processes and systems that assists us as we evolve our security posture.
- **Portfolio Management**: In an effort to strengthen our security posture we are working with the Centers on business cases, for example OMB-300s, to have better insight into their cybersecurity operations. These actions will lead to processes that increase the regular reviews in this area to monitor the risk and progress at an enterprise level. In alignment with FITARA, this increase in accountability will provide more transparency around cybersecurity issues.
- **Authority to Operate (ATO):** We must continuously scrutinize and improve our IT security posture. The security assessment and authorization process is a key element of our overall risk management strategy. To ensure our leadership has the information they need to make truly informed risk decisions, we must provide them a consistent and well understood taxonomy of security requirements, processes, and documentation. In support of this mandatory oversight model, the NASA IT Security Division is deploying a new, modernized toolset (known as RISCS) to more effectively guide processes and capture security assurance artifacts, and to inform NASA senior management on associated cyber security risks. By providing the ATO for a NASA information system, our leadership – myself included – are explicitly accountable to our customers and our missions for ensuring the integrity, confidentiality, and availability of our data. I take this responsibility very seriously. I am working closely with my new Senior Agency Information Security Official to ensure that these expectations are clearly understood, and to make sure that all requisite oversight mechanisms are in place for success.

## Conclusion

Protecting and evolving NASA’s IT infrastructure is and will remain a top Agency priority.
As evidenced by my testimony today, NASA is fully committed to becoming more secure, effective and resilient, and we are actively pursuing this on all levels. We look forward to working with Congress, the Government Accountability Office, the NASA Inspector General and other Federal stakeholders, including OMB and other Federal agency CIOs and CISOs in effectively implementing a restructured NASA security program.

In conclusion, thank you for the opportunity to testify before you today. I would be happy to answer any questions that you may have.

**Enclosure 1**

# National Aeronautics and Space Administration (NASA)
# Business Services Assessment (BSA) Decision Summary
# Information Technology (IT) Pilot Deep Dive

## Background

In 2015, NASA established the Business Services Assessment (BSA) to strategically assess mission support services, evaluate the health of current mission support capabilities, and identify opportunities to further optimize performance. The NASA BSA supports the Agency's objective of establishing a more effective and efficient operating model to meet current and future mission requirements.

## Process

For each BSA activity, NASA establishes a core team, comprised of diverse professionals from across NASA organizations, to evaluate mission support activities. The core teams collect data from across NASA, conduct surveys and interviews with internal stakeholders, review recent audits and regulations, benchmark external organizations, and perform a detailed assessment of existing operations. As part of the BSA process, the Agency employs several feedback mechanisms to collect input from NASA Centers, Mission Directorates, and other key organizations on potential options to enhance the specific mission support activities. Based on the results of the BSA and input collected from across NASA, the Agency makes decisions to strategically re-shape operations in an attempt to optimize mission support services to meet current and future Agency mission needs.

## Topic

The Information Technology (IT) assessment was the pilot activity for the NASA BSA. The IT BSA deep dive included assessments of IT roles and responsibilities, governance, data centers, communications, end-user services and security. The findings and decisions below provide a summary of the IT BSA. The Agency Chief Information Officer (CIO) is responsible for oversight of NASA's IT activities, as well as implementing NASA BSA IT decisions.

## Findings and Decisions

### 1. IT Roles & Responsibilities and Governance

**Finding:** The IT BSA found the existing governance and operating model for IT across the Agency needed to better align with the changing business of IT management and the Federal Information Technology Acquisition Reform Act (FITARA) to ensure compliance with applicable policies, laws and directives as part of the OCIO's responsibility.

**Decisions:** The OCIO will create a multi-tier (level 0 through level 3) management structure and appoint Program Executives for each IT domain; develop a plan to enable IT management improvements; restructure and streamline existing duplicative IT boards; conduct a formal annual capital investment review as part of the budget process; work with procurement and formalize guidance on strategic sourcing for IT contract activities; and conduct functional reviews of all Centers on a 3-year rotating basis.

### 2. Data Centers

**Finding:** The BSA found insufficient strategic direction, consistent coordination and oversight of NASA data center and computing investments.

**Decision:** The OCIO will implement a federated/hybrid data center operational model by developing an integrated, Agency-wide data center architecture to guide future investments and further consolidation, including on-site, outsourced, and cloud-based data center services as well as enabling strategic sourcing/contract optimization.

### 3. Communications

**Findings:** Multiple NASA Centers were found to have outdated communication services for phones, voicemail and Land Mobile Radios (LMR). In addition, the deep dive found that some mission areas were unable to effectively and securely collaborate using existing IT infrastructure.

**Decision:** The Agency will realign NASA Integrated Communications Services (NICS)-provided voice services, network operations and transformation funding from Centers to the Agency OCIO to enable an enterprise funded and managed approach for communications.

### 4. End-User Services (Workstations and Collaboration & Content Management Tools)

**Findings:** The Agency Consolidated End-User Services contract (ACES) was not being used as extensively as intended, which led to less than optimal IT operations. The deep dive also found multiple contracts and methods were being used to procure and administer workstations; and numerous independent platforms and tools were being used across NASA for collaboration.

**Decisions:** The OCIO will consolidate Non-ACES workstations administration and support, where feasible and appropriate. A target was established for each NASA Center to obtain at least 80% of their desktop, laptop, and workstation computing services through ACES. Further, the Agency decided that using non-ACES systems would require waiver approval from the Center CIO. Compliance with these objectives will be evaluated as part of the annual Center functional reviews. Finally, the OCIO will develop a core suite of collaboration tools and standards to meet the majority of NASA requirements.

### 5. IT Security

**Finding:** The absence of an enterprise-wide risk management framework created gaps managing NASA’s cybersecurity risks, implementing the Agency’s cybersecurity program, and effectively managing cybersecurity resources and tools.

**Decisions:** The OCIO will sponsor a zero-based review of IT Security spending and ensure alignment to the NASA IT security strategy. The OCIO will also establish an Agency IT Security risk management framework and IT security architecture that aligns with NASA’s business risks.

## Reneé P. Wynn
## NASA's Chief Information Officer

**Reneé P. Wynn** is the NASA Chief Information Officer. Wynn joined NASA in July 2015 as the Deputy Chief Information Officer. She came to NASA from the Environmental Protection Agency (EPA) where she had served as the Acting Assistant Administrator for the Office of Environmental Information since July 2013. Ms. Wynn has a long career in the Federal government. She was with EPA for more than 25 years, and joined the Office of Environmental Information in April 2011. Beyond the experience she gained since joining the information management and technology arm of the Agency, Ms. Wynn served in EPA's Office of Solid Waste and Emergency Response and the Office of Enforcement and Compliance Assurance.

Ms. Wynn has managed program administration for science, information management, and international programs; regulatory management; budget formulation and execution; contracts, grants and interagency agreements; long term strategic planning and analyses; and environmental and administrative policy.

Ms. Wynn holds a Bachelor of Arts in Economics from DePauw University, Indiana.