

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

before the

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

Chairman Hurd and Chairman Meadows, Ranking Member Kelly and Ranking Member Connolly, and members of the Subcommittees, thank you for the opportunity to testify before you today about NASA's implementation of the Federal Information Technology Acquisition Reform Act (FITARA) and its impact on information technology (IT) acquisition and security at NASA.

As the world leader in space exploration and cutting-edge science missions, NASA's work contributes directly to the economic vitality of our great Nation. In doing so, 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 more than 500 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. 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 the air – and we made advances toward a future in which we make air travel safer, cleaner and more efficient.

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 Center, as well as several smaller satellite facilities.

Every day NASA faces dynamic and continuing challenges defending our IT systems and networks from intrusion originating from individuals and organizations with malicious intent. Therefore, NASA

continues to improve its technical and procedural capabilities employed to: attain situational awareness of our information-security vulnerabilities and threats; and proactively defend the IT assets supporting our enterprise. Recently, NASA hired its first Senior Cybersecurity Advisor who reports directly to me, as the CIO. In this role, Rob Powell serves as my senior technical expert on IT security, staying abreast of the threat environment not only at NASA but at other Federal and non-Government networks. He actively engages with our Federal partners, thus ensuring that best security practices are implemented at NASA, and that NASA remains coordinated on and protected against threats and threat mitigations.

The collective actions of NASA's Office of the Chief Information Officer (OCIO), as well as information sharing with the Department of Homeland Security and other Federal agencies involved in cybersecurity, are contributing to an improved security posture. For example, the Department of Homeland Security's Cyber Hygiene report for NASA currently shows that there are zero critical vulnerabilities older than 30 days. Additionally, NASA did not experience any "major" cybersecurity incidents in FY 2015, as defined by the Office of Management and Budget¹. Additionally 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 Department of Homeland Security's U.S. Computer Emergency Readiness Team's (US-CERT) new Federal Incident Notification Guidelines². This new incident notification process took effect on Oct. 1, 2015. NASA now categorizes all incidents and reports the information at the Federal-level to the US-CERT in near-real-time.

It is also important to point out that NASA is extremely proactive in our approach to handling breaches caused by human error through awareness and education. NASA reaches out to every employee and guest with network accounts to notify them of best practices, both within the industry and within NASA. Employees must take mandatory training in order to retain access to our networks. They are encouraged to engage in discussions with professionals during activities such as webinars, road shows, and IT security technical expos featuring guest speakers, and related activities. 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.

Admittedly, NASA's scores on the FITARA scorecard are unacceptable. We have work to do, and challenges to overcome. But at the same time, I believe it is also important to reflect on the major strides NASA has already taken in improving the management of and protection of the Agency's IT infrastructure. Thus, the remainder of my testimony today will provide a brief summary of our achievements to date, and other work in progress directed at becoming the best stewards of the Agency's IT resources.

NASA's Implementation of FITARA

NASA is fully committed to implementing the FITARA requirements by aligning our IT services and capabilities against those requirements. Following passage of FITARA, NASA immediately began working toward implementing the law's requirements while also building upon internal changes previously made at NASA. In summary, this work has included:

¹ OMB Memorandum 16-03, "Definition of Major Incident", pg. 7-9. October 30, 2015: <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-03.pdf>

² 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>

- Initiating a Business Services Assessment (BSA) review of how IT is delivered at the Agency;
- 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 which will 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 Agency 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 the Centers. NASA has recently realigned the reporting structure so that I, as the NASA CIO, have direct authority and oversight over the Center CIOs.

The BSA for IT

NASA established the BSA evaluation process in 2015 to strategically assess Agency mission support services, evaluate the health of current mission support capabilities, and identify opportunities to further optimize performance. The BSA supports the Agency's objective of establishing a more effective and efficient operating model to meet current and future mission objectives.

For each BSA activity, NASA establishes a core team, comprised of diverse professions from across NASA, 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 about 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.

The 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 and end-user services and security. Many elements of NASA's implementation of FITARA lie within the aforementioned BSA Implementation Plan, specifically, (1) Agency Chief Information Officer Authority Enhancements; (2) Portfolio Review; and (3) Data Center Consolidation.

On March 31, 2016, the BSA IT Implementation Plan, which includes an exhaustive methodology on influencing budget formulation and execution, increasing involvement in IT acquisitions, and building a competent IT workforce while aligning our workforce to execute these strategies and approaches was approved by NASA. Like FITARA, the BSA was designed to ensure that IT is seen as a strategic Agency resource. One of the most important objectives of the BSA process was to establish clear objectives for the NASA CIO to approve the Agency's IT spend plan for non-highly specialized and highly specialized IT.

As the Agency CIO, I am now responsible for implementing the NASA BSA IT decisions outlined in Enclosure 1.

Improving NASA's IT Governance Structure

In November 2011, NASA adopted a phased approach to implement IT governance across all areas of IT. Phase I successfully focused on Enterprise IT services directly managed by the NASA CIO. Phase II was formally initiated in December 2013 and focused on Center IT services.

Currently, the NASA CIO has visibility into and oversight of all NASA IT through IT authority. The CIO also has direct control over CIO managed services through IT program authority. Additionally, to ensure that the IT security policies and procedures are implemented at the Centers, several years ago, NASA realigned the reporting structure so the NASA CIO has direct authority and oversight over the Center CIO. Specifically, the NASA CIO "[d]irects, manages, and provides policy guidance and oversight of the Agency's Center [CIO] activities, and operations, including in concurrence with Center Directors, the approval of the assignment, promotion, discipline, and relief of the principal CIO at each Center, and assesses their performance."

Next, as a result of the lessons learned from Phase II of NASA IT governance implementation, the release of FITARA legislation, and NASA's technical and business optimization efforts, the BSA for IT was initiated. Results from the aforementioned BSA activity highlighted enhancements to IT roles and responsibilities, as well as IT governance, were necessary to clearly distinguish IT authority from IT program authority, even though existing policy provided the NASA CIO clear authority for visibility and oversight of all NASA IT. The plan to execute these related enhancements was approved March 31, 2016.

Many elements of NASA's FITARA implementation plan are enabled through the implementation of the Agency's transformed IT governance structure and clarified roles and responsibilities. NASA is streamlining the Agency's IT governance structure while simultaneously broadening council membership to promote integrated, efficient Agency-wide decision-making.

One of the key findings of the BSA is that the existing governance and operating model for IT across NASA needed to better align with the changing business of IT management and FITARA to ensure compliance with applicable policies, laws and directives as part of the OCIO's responsibility.

The BSA identified key roles, including the position of the CIO, which required more visibility and authority in order to exercise greater influence in optimizing NASA's IT. This new governance structure will be in place for NASA's FY 2018 budget planning cycle, thus allowing the CIO to have visibility into Agency budget decision-making processes across the Agency. This is the first step in improving visibility into decision-making information. The portfolio review will be conducted in partnership with the NASA Chief Financial Officer (CFO), Deputy Center Directors, and key mission leadership and includes a comprehensive review of institutional and mission IT and related acquisition strategies. The

decisions made during this review will include joint recommendations for IT optimization that are carried out under the authority of the NASA CIO. In addition, the budget review will validate the CIO has direct accountability for IT, and increase this new authority in the budget cycle. Moreover, the review is the formal venue for uncovering mission IT details ranging from acquisitions to execution, an area the NASA CIO has previously lacked insight. In addition, by gaining awareness into mission IT acquisitions, the CIO will have more insight into and influence over the security of mission assets.

The good news is that we have already seen positive evidence of the expansion of the CIO's role in monitoring Agency IT program performance through the elimination of duplicative and ineffective IT boards. Additionally, I have made an effort as the Agency's new CIO to more proactively engage the Center CIOs, visiting each Center during my first six months as CIO. I also have reached out to mission stakeholders within the Agency so as to better understand their work and how my job intersects with their mission. I also am engaged with our other Federal partners who share the FITARA responsibility. Additionally, I have engaged with the CIOs of our international partner agencies so as to share best practices with them.

Portfolio Review

In order to achieve FITARA-based objectives, NASA leadership and the NASA CIO established a new budget review aligned with the Agency's annual budget cycle deliverables. This new budget review is part of the Agency's implementation of FITARA, which mandates that NASA's CIO have approval authority over the entire IT budget, and increases the CIO's responsibility. The scope of the review includes IT and program-funded IT and related acquisition strategies. In this model, the NASA CIO is responsible for ensuring that IT investments align with NASA's mission, goals, and programmatic priorities while strengthening accountability for IT cost, schedule, and performance. The budget review enables the NASA CIO to be more directly accountable through increased authority in the budget cycle. The strategy of this inaugural review process is driven by input from all IT stakeholders, including Center CIOs, Center CFOs, and Mission Program Managers.

Data Center Consolidation

In 2010, at the beginning of the Office of Management and Budget's (OMB) Federal Data Center Consolidation Initiative (FDCCI), NASA had 79 data centers. The FDCCI promotes the use of Green IT by reducing the overall energy and real estate footprint of Government data centers, reducing the cost of data center operations, and shifting IT investment to more efficient computing platforms and technologies. Since that time, NASA has closed 50 data centers freeing more than 39,000 square feet of space for re-purposing. The target is to reduce to 22 data centers by the end of FY 2018.

Additionally, NASA OCIO recently embarked on the development of an integrated Agency-wide data center architecture to guide future investments and further consolidation, including on-site, outsourced, and cloud-based data center services.

Conclusion

While NASA has a strong foundation upon which to successfully implement FITARA, we recognize there is still much work to do. As evidenced by my testimony today, NASA is fully committed to implementing FITARA, and we are actively taking steps to complete that implementation as quickly as possible. We look forward to working with Congress, the Government Accountability Office, and other Federal stakeholders, including OMB and other Federal agency CIOs in effectively implementing FITARA to reduce costs and increase the value of our IT acquisitions. In conclusion, thank you for the opportunity to testify before you today, and I would be happy to answer any questions that you may have.

**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.