Hold for Release Until
Presented by Witness

National Aeronautics and
Space Administration

December 11, 2019

Subcommittee on Government Operations

Committee on Oversight and Reform

U.S. House of Representatives

Statement by:
Reneé Wynn
Chief Information Officer

116th Congress

HOLD FOR RELEASE
UNTIL PRESENTED
BY WITNESS
December 11, 2019

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

before the

Subcommittee on Government Operations
Committee on Oversight and Reform
U.S. House of Representatives

Chairman Connolly, Ranking Member Meadows, and members of the Subcommittee, 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 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 information systems with components geographically dispersed around the globe. In FY 2020, the Agency plans to spend approximately $2.16B on enterprise, mission, and mission support IT products and services.

NASA's IT infrastructure plays a critical role in every aspect of NASA's mission, from controlling spacecraft to processing scientific data. It is a privilege to support spacecraft that are pushing the frontiers of knowledge, probing the atmosphere of the Sun, passing through the depths of interstellar Space and roving over the surface of Mars. Now, we have accepted the challenge to return humans to the Moon. NASA's new Artemis Program, named after Apollo's twin sister, will deliver the first American woman and next American man to the Moon in 2024. We will use a long-term presence on the Moon to test, build and validate new capabilities for human missions to Mars. Artemis will bring together the capabilities and resources of our international and commercial partners and demonstrate to young people around the world the power of a unified purpose, helping to inspire the next generation. NASA is committed to this challenge, and NASA's OCIO team looks forward to playing its part in this great endeavor.

NASA's scores on the FITARA scorecard are improved, but are not where we want them to be. We have work to do as the Agency continues to evolve from a highly decentralized IT environment controlled by the Centers to an enterprise IT environment that is more centrally managed and overseen by the Agency CIO. 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. I am proud of my team and the lean-forward attitude they demonstrate daily in these efforts.

The high-profile nature of NASA's missions means that it, like other Federal agencies, continues to be a major target of attacks from domestic and foreign adversaries. 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. The collective actions of NASA's Office of the Chief Information Officer (OCIO), as well as information sharing with the Department of Homeland Security (DHS) and other Federal agencies involved in cybersecurity, are contributing to an improved IT security posture at NASA.

In order to address the new and unique cyber risks and challenges posed by human spaceflight generally, and in particular by Artemis, OCIO is partnering with the Human Exploration and Operations Mission Directorate (HEOMD) and its Advanced Exploration Systems Division at Headquarters. An OCIO representative will attend vital staff-level and leadership meetings, providing immediate OCIO input on programmatic matters. This partnership will allow the OCIO representative to better understand HEOMD's programs and processes, while helping HEOMD identify and resolve any cyber gaps. The OCIO representative will directly support the Artemis team in evaluating cybersecurity requirements; ensuring an integrated approach to addressing cybersecurity risks; and making certain that cybersecurity considerations are included at the outset of this groundbreaking work.

Protecting and effectively evolving NASA's IT infrastructure is and will remain a top Agency priority. NASA is fully committed to becoming more secure, effective and resilient, and we are actively pursuing this on all levels. My testimony today will summarize our major achievements to date, while also foreshadowing the work yet to be accomplished. FITARA has been and will continue to be an integral part of NASA's efforts to effectively manage and protect its IT resources.

Evolving the Way We Do Business

NASA is fully committed to meeting the requirements of foundational Federal IT laws such as FITARA; the Federal Information Security Modernization Act (FISMA); the Federal Cybersecurity Enhancement Act (FCEA); and more recently, the Modernizing Government Technology (MGT) Act, the Making Electronic Government Accountable by Yielding Efficiencies (MEGABYTE) Act, and the 21st Century Integrated Digital Experience Act (IDEA Act), amongst others. We also are committed to meeting the requirements of IT-related Executive Orders issued by the President, as well as additional security directives issued by the Office of Management and Budget (OMB) and the DHS.

Over the last several years, NASA has established a new governance structure that gives the CIO greater visibility and authority within the Agency. Many of these changes are aligned with requirements in FITARA and other new laws, including:

- 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, while also ensuring that the CIO reports directly to the Administrator;
- Establishing IT acquisition process changes, ensuring that, in partnership with the Office of Procurement, the NASA CIO approves IT acquisition strategies and IT acquisition plans, as well as leverages strategic sourcing; and
- 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.

Additionally, NASA has aligned 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 including 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 throughout the NASA enterprise, including our Centers.

In FY 2018, OCIO developed the NASA IT Strategic Plan for FY 2018-2021. This plan serves as an integrated roadmap that identifies critical activities, milestones, and resources needed to manage IT as a strategic Agency resource that is aligned with Agency priorities and is designed to best meet customer and mission needs. NASA's IT community will accomplish this outcome by sharing NASA's results and partnering on new strategic capabilities to drive discovery while increasing quality, productivity, mission safety, and cost optimization.

To further improve the IT operating model, OCIO is participating in NASA's Mission Support Future Architecture Program known as MAP. MAP is intended to transform all mission support services (to include budget authority and lines of reporting) from their current state to a more efficient enterprise operating model that maintains critical capabilities and meets current and future mission needs. These efforts also include strategically assessing and aligning workforce to support the transformation. OCIO expects to complete its MAP assessment and planning by December 2020.

<u>FITARA at NASA</u>

As Federal CIO Suzette Kent recently testified: "FITARA is more than just a law and a scorecard—it serves as a vehicle for communicating evolving priorities and a method to capture progress. … it is a tool to empower Agency CIOs to drive priorities across their technology landscape." I couldn't agree more. Many elements of NASA's FITARA implementation plan are enabled through the implementation of the Agency's aforementioned IT governance changes and the associated clarified roles and responsibilities of the NASA CIO.

We are seeing the results of these efforts in several key FITARA areas. Since the initial release of the FITARA Scorecard in November 2015, NASA has proactively engaged with the General Accountability Office (GAO) and other key stakeholders to collect and report comprehensive and accurate data while maintaining a commitment to executing the NASA mission. While our scores have improved in several elements of the FITARA scorecard, we know there is more work to be done. For example, in the December 2018 scorecard, NASA met only four out of 10 metrics; however, as of June 2019, NASA has currently met and exceeded seven out of 10 metrics. We'd like to make that 10 out of 10.

Incremental Development of IT Projects: NASA notably has improved our scorecard measurement in the area of Incremental Development of IT Projects. Incremental Development of IT Projects is an effective management practice that delivers capabilities to users more rapidly and increases the likelihood that projects achieve cost, schedule and performance goals. Thanks to the Agency's work and the cooperation of major IT Investment owners, NASA reported a new data set of software development projects and found that 75 percent of these projects followed incremental development practices. Their work in reporting this information significantly contributed to the increase in our FITARA Scorecard released in December 2018.

Data Center Consolidation: Another area where NASA has made great progress is in the consolidation of data centers. In 2010, NASA had 79 data centers at the beginning of the Federal Data Center Consolidation Initiative (FDCCI), which 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 2010, NASA has reduced its number of data centers to 19 or roughly by 75 percent. We have repurposed approximately 80,000 square feet of space and generated a total cost savings of about $36.2M since FY 2012. Additionally, NASA OCIO has 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. NASA's Computing Services Program aims to maintain the efficiencies gained through data center closures and is working to continue to implement virtualization and energy efficiency improvements in NASA's remaining data centers. As a result of the successful management of the computing program, OCIO has seen significant growth in cloud adoption from the science and mission communities within NASA and is working to grow and improve cloud skills and modern development techniques across the NASA workforce.

Portfolio Review: FITARA mandates that CIOs have approval authority over an Agency's entire IT budget. In order to achieve this FITARA-based objective, NASA leadership and the NASA CIO established a new budget review aligned with the Agency's annual budget cycle deliverables. 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 review process is driven by input from all IT stakeholders, including Center CIOs, Center Chief Financial Officers, and Mission Program Managers.

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.

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

- NASA achieved and has maintained an Overall rating of 'Managing Risk' (the highest rating) for the FISMA Risk Management Assessment. This is a significant improvement compared to NASA's Overall rating of 'High Risk' in FY 2017; and
- NASA is meeting or exceeding eight of 10 Cross-Agency Priority FISMA goals in FY 2019, compared with just three of 10 in FY 2017.

NASA has developed a high-availability NASA Security Operations Center (SOC) Continuity of Operations (COOP) for cybersecurity operations. Previously, if cybersecurity operations at NASA's Ames Research Center, where the COOP is located, were disrupted, the Agency would be limited in the ability to identify, detect, and respond to cybersecurity incidents. With new back-up operations and processes in place across multiple Centers, NASA is prepared to maintain operations in the event of an isolated disruption. The development of COOP capabilities is aligned to an increase of overall SOC capabilities as well. NASA has recently on-boarded resources to evolve the SOC from a predominately reactive capability to a pro-active resource the Agency can leverage, including the NASA missions.

A critical part of our success in improving our FISMA ratings was our effort to implement DHS's Continuous Diagnostics and Mitigation (CDM) program, which enables NASA to identify all assets and vulnerabilities for remediation. In 2016, we had just begun the initial operating phase of CDM at our Kennedy Space Center (KSC) in Florida -- 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 KSC. Today, NASA is a leader in the adoption of the CDM program and tools, 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. Deployment of CDM Phase 1, which focuses on identifying what is on NASA's networks, is now complete across our corporate network and NASA is making significant progress on the mission network, with completion scheduled for the first quarter of Fiscal Year 2021

Related to this, NASA has made great strides in Personal Identity Verification (PIV) efforts. NASA requires 100 percent of privileged users to authenticate with PIV, and between FY 2017 and FY 2019, NASA increased the percentage of unprivileged users required to use PIV from 72 percent to 90 percent, thus meeting a FISMA Risk Management Assessment target. NASA has developed PIV solutions for a variety of unique NASA systems and CDM efforts, further solidifying the security of identity management and access on the Agency's network. Our team developed the first-ever native smartcard authentication for Apple's MacOS platform, a solution which NASA has shared with other Federal partners. Additionally, NASA's Identity, Credential and Access Management (ICAM) program was a finalist for the National Security Agency's prestigious Frank B. Rowlett Award, which recognizes outstanding Federal Government excellence in the field of cybersecurity.

In addition to the aforementioned activities, NASA has also implemented notable program changes and updates to mature our cybersecurity management. NASA has:

- Deployed and continues to update and maintain the Risk Information Security Compliance System (RISCS), which allows system owners to manage all aspects of cybersecurity throughout the entire lifecycle of the system. RISCS also delivers customizable risk information to all relevant stakeholders, and centralizes and formalizes the management and acceptance of IT risk, culminating in Authorizing Officials being able to authorize their systems to operate;
- Transformed NASA's SOC by clarifying its mission and increasing its scope. The SOC is taking on initiatives to become more proactive in preventing security incidents; and
- Established an Office of CyberSecurity Services, which standardizes and optimizes cybersecurity service delivery across the entire enterprise. This minimizes duplicative activities occurring

across Centers, increases cost-savings, and ensures that missions are able to have access to necessary cybersecurity services.

It is also important to point out that NASA is extremely proactive in our approach for handling data 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.

Legacy IT

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.

Knowing that many of our IT assets may be operational for decades, we take their origins very seriously. We are proud to be considered a leader within the Federal government in Supply Chain Risk Management (SCRM). In January 2019, NASA became a voting member of the DHS Information and Communications Technology SCRM Task Force and co-chairs one of the four working groups. We have worked diligently to address the findings from the May 2018 NASA Inspector General (OIG) audit related to NASA’s IT supply chain risk management efforts and are scheduled to correct the two remaining findings by the end of FY 2020.

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 OCIO in general, must balance securing its IT resources with data accessibility to further global science and technology collaboration around the world. In particular, NASA OCIO has developed a Web consolidation initiative to inventory NASA’s public-facing websites, consolidate their domains and ensure that domains have been assessed for risk and are authorized to be visible to the public.

Looking Ahead

Effective IT management is not an easy task – costs must be balanced against risks and customer needs, as well as against the quick pace of technology development which never slows.

Like all agencies, NASA is adjusting to new laws and directives designed to improve how the entire Federal Government manages and secures its IT resources. While NASA is proud of the progress we have made, we recognize that more work remains to fully comply with new laws and policy. There is a lot at NASA to be excited about, and as the CIO, I am eager to play a more active partnership role in key decision-making processes within the Agency. Here ae just a few of the exciting opportunities ahead of NASA OCIO:

Cloud Computing: NASA's commercial cloud computing interest and adoption has rapidly escalated as missions planning for launch in FY 2021 / 2022 are aggressively making the transition from traditional Agency-hosted software platforms to reliance on cloud native services and applications. There is also significant interest in delivering observation data from orbiting assets directly to the cloud. This would be accomplished through the use of newer, more sophisticated cloud services such as one cloud provider's "Groundstation-as-a-Service" that offers satellite downlink options in remote locations where NASA potentially doesn't currently have access and also allows NASA to pay for use by the minute as a metered service, eliminating significant capital investment. NASA is presently consuming more than 1.4M computing hours in the commercial cloud every month and has almost 10 petabytes of data stored in the cloud with the majority of data available for unrestricted use by the global science community. The portfolio of data for just one major NASA program will increase this data amount by at least an order of magnitude within the next five years. Mission growth in use of commercial cloud computing services is fully aligned with the Agency's thrust to rely on industry as much as possible for capabilities so that NASA can focus on its key objectives in the areas of science and discovery.

Website Modernization: NASA is also working on a full review of NASA's web footprint and digital presence, resulting in an enhanced cyber posture, improved operating efficiencies, and an improved focus for communicating our messages. This is a priority for NASA's senior leadership, as outlined in a May 15, 2019, memo from NASA Administrator James Bridenstine. To accomplish this review, NASA has created an internal NASA Website Modernization Team, led by NASA Chief Scientist Dr. Jim Green, to provide recommendations to reshape NASA's digital landscape in an optimal state. In doing so, NASA will take into account the statutory requirements included in the IDEA Act.

Cyber workforce: OCIO is appreciative of the new hiring authority that the Office of Personnel Management (OPM) granted NASA in November 2019 in order to meet NASA's urgent staffing requirements resulting from a national priority of returning astronauts to the Moon by 2024. OPM has authorized NASA to hire a total of 3,600 General Schedule (GS) employees for five years under this new authority, including GS-7 through GS-15 information technology specialists. OCIO has a good working relationship with NASA's Office of the Chief Human Capital Officer so we look forward to working with that office regarding this new hiring authority and others that may be applicable to the Federal cyber workforce. NASA is appreciative of Congress, and in particular, this Committee's efforts to ensure that the United States has a knowledgeable, skilled, effective and fully staffed Federal cyber workforce.

Conclusion

Protecting and evolving NASA's IT infrastructure is and will remain a top Agency priority. 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 ensuring that our IT network is secure, effective and resilient. We look forward to working with Congress, the GAO, the NASA OIG and other Federal stakeholders, including OMB and other Federal agency CIOs in effectively implementing FITARA, and other associated laws, to reduce costs and increase the value of our IT acquisitions.

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

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.