National Aeronautics and Space Administration

IT Talk

Oct - Dec 2023 Volume 13 • Issue 4

NASA's Pathway to Zero Trust

IT Talk

Oct - Dec 2023 Volume 13 • Issue 4

Office of the CIO
NASA Headquarters
Mary W. Jackson Building
300 E Street SW
Washington, D.C. 20546

Chief Information Officer
Jeff Seaton

Editor & Publication Manager
Eldora Valentine

Graphic & Web Designer
Michael Porterfield

Copy Editor
Meredith Isaacs
Mia Roundtree

IT Talk is an official publication of the Office of the Chief Information Officer of the National Aeronautics and Space Administration, Headquarters, Washington, D.C. It is published by the OCIO office for all NASA employees and external audiences.

For distribution questions or to suggest a story idea, email:
eldora.valentine-1@nasa.gov

To read *IT Talk* online visit:
www.nasa.gov/offices/it-talk

For more info on the OCIO:
- *www.nasa.gov/ocio*
- *nasa.sharepoint.com/sites/cio/*
  (Internal NASA network only)

www.facebook.com/NASAcio

In this Issue

Message from the NASA CIO

None of us are immune to cyber threats. We all need to do our part to ensure that our online personal and work lives are kept safe and secure. This fall, we mark the 20th annual Cybersecurity Awareness Month. It's the perfect opportunity to highlight some of the ways NASA is increasing its resiliency to prevent and address cyber incidents.

In this issue, we'll share how we continue to work diligently to improve the agency's cybersecurity and to more effectively manage the IT systems that make NASA missions possible.

We'll explore how NASA's Pathway to a Zero Trust architecture is providing tremendous benefits to the agency. Zero Trust principles can securely enable the "anywhere, anytime, any device" in a hybrid workforce.

We'll take a closer look at how NASA is addressing a Federal mandate known as HTTPS - Everywhere for Government. HTTPS is a key protection for websites and web users. It offers security and privacy when connecting to the web and provides Federal agencies with the assurance that what they publish is what is delivered to users.

And we'll recognize some of our team members for the exceptional work they are doing to modernize and broaden NASA's records management capabilities.

We have a great lineup this issue, so I hope you enjoy reading our most recent and ongoing activities.

With gratitude,

Jeff Seaton

NASA Chief Information Officer

Workplace and Collaboration Services (WCS) News and Updates

Check out the latest news from WCS (all links are internal to NASA):

- *Stay up to Date on the Rollout of Follow Me Print*
- *Maintaining Security Compliance on Your Mobile Device*
- *Permission Levels for Managing Your Computer*
- *Cloud Recording Now Available for Webex Hosts*
- *Microsoft Edge Browser is Becoming Edge for Business*
- *New Teams Features: Add Pronouns to Your Profile, Zoom Controls for Screenshared Content, Files App, Chat Settings, Spatial Audio, and Speaker View*
- *See What's New with ICAM*

Jet Propulsion Laboratory Named a 2023 CIO 100 Honoree

By Whitney Haggins, IT Communication Strategist, Jet Propulsion Laboratory, California Institute of Technology

The Jet Propulsion Laboratory (JPL) was honored by Foundry's CIO as a 2023 CIO 100 Honoree at the CIO 100 Symposium & Awards in August. The CIO 100 awards program, now in its 36th year, celebrated 100 organizations that apply innovative methods to IT and drive business value. The honor is considered by many to be a mark of enterprise excellence, and this is JPL's 12th consecutive selection to the prestigious list.

Chris Mattmann, JPL Chief Technology and Innovation Officer, accepted the award at the August 16 award ceremony. Mattmann had this to say about the honor: "The JPL team is so proud to receive this award in an area of prime technological importance in today's threat environment: cybersecurity and protecting our NASA assets. IT has a prime role to play in ensuring that the hardware is robust, and our winning CIO 100 submission promises to help secure NASA hardware using an innovative blockchain-based approach. Meeting Ken Jennings, the co-host of Jeopardy, to receive the award was icing on the cake!"

The complete honoree list is available at https://events.foundryco.com/event-series/cio100-symposium-and-awards/awards/cio-awards-august-2023/.

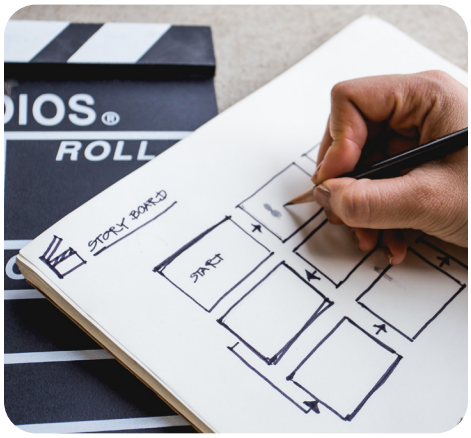
From Newsletters to Videos: How HQ/GSFC OCIO Uses Video to Catch Employees' Attention

By Hilary Jackson Gambale, Strategic Communications Specialist, Code 702, Goddard Space Flight Center (GSFC)

Gone are the days when employee newsletters maintain the same readership levels they once did. With texting, Teams chats, and short videos on social media, people are used to receiving information in quick short spurts. The dramatic decline in the number of readers of the Headquarters (HQ) and Goddard Space Flight Center (GSFC) Office of Chief Information Officer (OCIO) newsletter, The Nexus, demonstrates this trend. Jamie Dulaney, a member of the HQ/GSFC Communications Team, came up with a way to solve this problem. Why not replace the lengthy newsletter, produced quarterly, with a short monthly video? Whereas the quarterly Nexus took weeks to produce and covered events as far back as 3 months, a video could be produced quickly with more current events. In addition, unlike newsletters, videos can convey emotions, expressions, and personalities, which is greatly needed in our remote work environment. The Nexus was formal, time-consuming, and impersonal, whereas a narrated video can portray a friendly voice and presence. Unanimously, the communications team decided to sunset The Nexus as a newsletter and replace it with a new video format.

The Nexus had gone through a transition over the years. It began as a PDF newsletter in 2013, shared with employees via e-mail, then moved to the intranet as a website newsletter in 2019; now, after declining readership, the newsletter is being retired and replaced with a new video series that Dulaney named What's Up HQ/GSFC OCIO? At first, creating the video was time-consuming since Dulaney had never professionally produced videos and was lacking a video-editing tool, but she learned quickly how to use Camtasia and is now able to produce videos in a matter of hours. Not only did she cut production time by 90 percent since she no longer had to produce a lengthy newsletter, but viewership improved by over 200 percent, even with a reduced staff post-realignment. The videos were more personal, showcasing employee engagement events, in-person directorate meetings, special employee events, and colleague accomplishments.

If you decide to use videos in place of print, you should first determine who your audience is and how best they like to consume information. Videos offer many advantages over newsletters. They are easier and faster to create and consume. They allow employees to showcase their skills, talents, and passions in a more engaging way. And they enable employees to see and hear each other, creating a sense of closeness and trust. Videos are also great for telling stories and conveying narratives and can be an effective way to provide instruction or training. Overall, videos are an incredibly versatile medium that can be used to convey a wide range of information in a highly engaging and powerful way. Our What's Up HQ/GSFC OCIO? videos proved this to be true. The team now wonders what will replace videos, probably something AI-related, but are prepared to embrace the next new communication medium when it comes their way.



Engineering for Tomorrow Focuses on Data-Centric Approach

By Alex H. Wagner, Digital Transformation Communications Specialist, NASA Headquarters

In December 2022, 50 years after the launch of the last human mission to the Moon, the Artemis I Orion spacecraft safely landed back on Earth. It was the beginning of a new era of space exploration, one that is powered in part by the innovations harnessed through NASA's Digital Transformation (DT).

DT's Engineering for Tomorrow project utilized Model-Based Systems Engineering (MBSE) methodologies and tools to create a "digital twin" of the electrical system on board the Orion spacecraft. Relying on data modeling to understand competing and interdependent requirements in the vast documentation of the spacecraft's design, the team could provide as-flown engineering design insights in a fraction of the time required by traditional document-centric approaches. Such developments embolden DT's guiding principles of transcending the document-centric approaches of the past to data and model-centric approaches for today and the future.

"How do we transform engineering beyond what it is today? We've had simulation capabilities for decades, we have math models, and 3D CAD models which we use for mechanical and electrical design. Everything's 'digital,'" says Terry Hill, NASA's Digital Engineering Transformation Lead and Office of Chef Engineer's Digital Engineering Program Executive. "The difference is really looking at every aspect of engineering from a data-centric standpoint. And not just hard-core engineering processes, but the business side of engineering as well."

While NASA's journey harnessing MBSE for engineering transformation began nearly a decade ago, the creation of the MBSE Leadership Team (MLT) in 2020 solidified the agency's efforts. The initial goal: develop a new implementation strategy for systems engineering, which would rely on interoperable tools and common federated sources of truth to streamline and accelerate the agency's capabilities.

"It's about understanding the flow of information like you would understand the flow of electricity, or the flow of water in your designs," says Hill.

The MLT published an MBSE handbook, NASA Systems Modeling Handbook for Systems Engineering (NASA-HBK-1009), and partnered with the Academy of Program/Project and Engineering Leadership (APPEL) to embed MBSE principles into NASA training. As MBSE approaches are adopted, this will drive transformation systems engineering from documents to models, helping to accelerate the design process, manage increasing mission complexity, and reduce design error rate.

In 2022, in partnership with NASA's Office of Chief Engineer, the Engineering for Tomorrow project broadened their focus and proposed an implementation plan for scaling Digital Engineering across the agency. The team's activities and accomplishments to date include the following:

- Clearly defining what digital Engineering is for the NASA Engineering domain by applying standard systems engineering approach of defining DE Need, Goals, & Objectives which are mapped to functional capabilities.
- Approving a Digital Engineering transformation approach at the November 2022 Engineering Management Board by the Engineering Directors from across the agency
- Initiating a multi-center, cloud-based product life-cycle management (PLM) pilot to demonstrate a secure approach to project integration, collaboration, and exchange of information between centers
- Completing a benchmarking survey to understand the current state of integrated toolchain capabilities and identify interoperability requirements
- Exploring opportunities for managing unique NASA standards in a structured format, which will facilitate tailoring and assistance via AI/ML technologies
- Developing MBSE training content requirements for the agency's APPEL office
- Modeling agency policy and process documents (NPR 7132, 7120.5/.8, and 8705) in integrated SysML models to identify potential changes when performing engineering, safety, and mission assurance from a data-centric approach
- Generating the "digital twin" for the electrical system of Artemis I's Orion capsule, launched on November 16, 2022

By identifying and leveraging common federated sources of truth through this data-centric approach, the amount of errors can be dramatically reduced and addressed much earlier in the engineering process, meaning greater workplace efficiency, quicker project turnaround, and potential cost savings.

This will be crucial as the aeronautical and space sectors continue to mature, Hill says, in areas where NASA "used to be the only people that could do it."

Currently, according to Hill, the team has been busy with an agencywide 5-year digital engineering roadmap.

With further exploration into our solar system and greater challenges on Earth expected in the future, this new way of doing engineering is not just an ideal, but a necessity.

"The new missions that we need to embark [on] here on Earth and out in the solar system are going to be bolder and more complex than ever before," says Hill, "and to manage that complexity and risk, we must approach the business of engineering differently: different models, different tools, different approaches to managing and leveraging our data and corporate knowledge. This is the next step of how NASA leads in engineering."

The NASA Pathway to Zero Trust

By Mark Stanley, CIP Cybersecurity Architect, Langley Research Center (LaRC), and Rachel Campbell, CIP Communications Lead, NASA Headquarters

Zero Trust Architecture (ZTA), a common IT buzzword, sounds a bit unfriendly. Trust is a good thing, right? Actually, not when it comes to cybersecurity. According to a 2020 Stanford University/Tessian Research study, "Psychology of Human Error," 88 percent of cybersecurity breaches are caused by human error. Users are the major target for cyberattacks in which the attacker searches for and targets the system's users instead of directly attacking the system itself. Indeed, this kind of cyberattack gives the attackers an easier way to get access to the targeted systems or sensitive assets such as databases, sensitive files, or even control processes in industrial enterprises.

In a user-oriented attack, the attacker searches for and extracts sensitive information about the user, such as their e-mail or personal address or social network profiles, or even information on their closest and most vulnerable friends, to build an efficient attack. Once the user is compromised, the attacker takes full control of their machine so that the attacker can use their access to the system to spread malware within the corporate network and retrieve sensitive data.

As a result, NASA OCIO is working to consolidate and transform our IT architectures with a data-centric "zero trust" cybersecurity model.

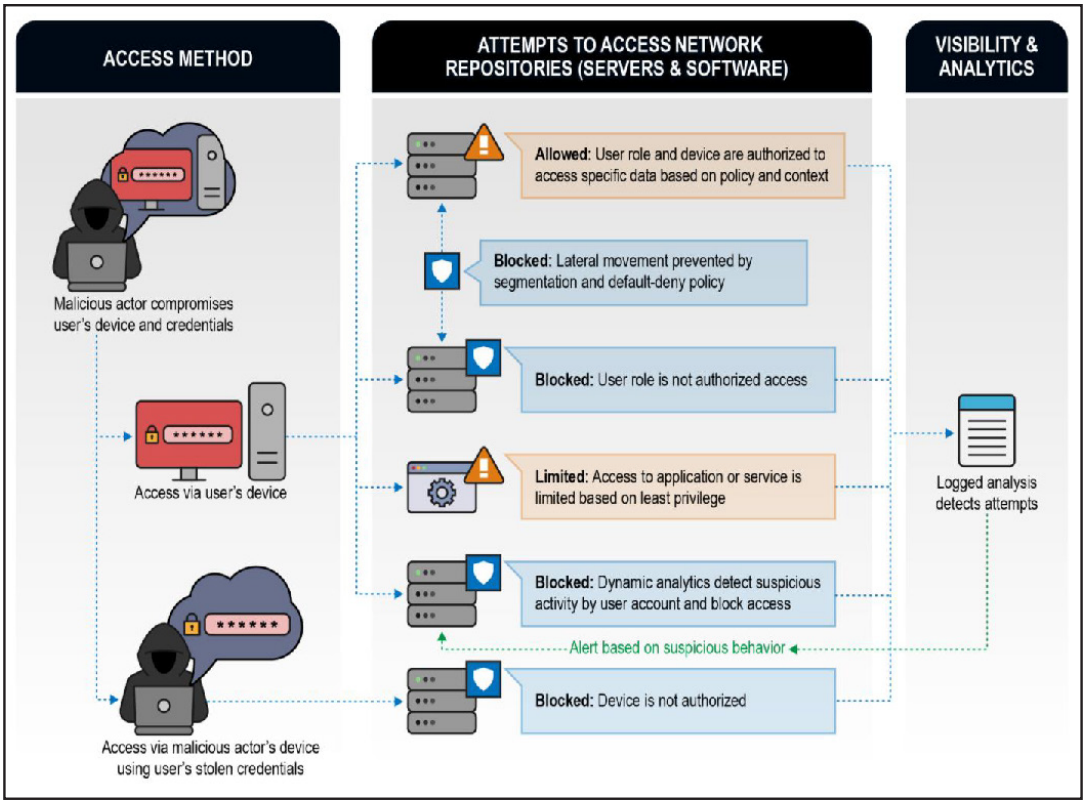
What Is Zero Trust?

The GAO Science & Tech Spotlight describes ZTA as "a cybersecurity approach that authenticates and authorizes every interaction between a network and a user or device—in contrast to traditional cybersecurity models that allow users or devices to move freely within the network once they are granted access. ZTA works on the 'never trust, always verify' principle and assumes that attacks will come from within and outside of the network."

Zero Trust Tenets

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture.

In a Zero Trust network, the compromised user's credentials and the



NSA Example of Zero Trust remote exploitation scenarios where most attempts would have been successful in non–Zero Trust environments.

device are already assumed to be malicious until proven otherwise, and the network is segmented, limiting both enumeration and lateral movement opportunities. While the malicious actor can authenticate as both the user and the device, access to data will be limited based on security policy, user role, and the user and device attributes. In a mature Zero Trust environment, data encryption and digital rights management may offer additional protections by limiting which data can be accessed and the actions that can be taken with the sensitive data even if access is allowed. Further, analytic capabilities continuously monitor for anomalous activity in accounts, devices, network activity, and data access. While a level of compromise occurs in this scenario, damage is limited, and the time for defensive systems to detect and initiate appropriate mitigating responses is greatly reduced.

What Are the Benefits of Zero Trust?

According to Gartner in their *September 2022 version of "Quick Answer: How to Explain Zero Trust to Technology Executives"*:

- Zero Trust principles can securely enable the "anywhere, anytime, any device" hybrid workforce (Future of Work).
- Well-implemented Zero Trust architectures streamline cybersecurity and provide the same security controls and user experience regardless of location.
- Zero Trust forms a guiding principle for security architectures that improve security posture and increase cyber-resiliency.
- Zero Trust architectures both reduce the risk of malware infections and minimize the potential spread of an attack.
- Zero Trust principles enable more secure use of cloud computing via identity-based adaptive controls.
- Partial Zero Trust deployments still result in dramatic security improvements—do not let perfect be the enemy of good.

So How Is NASA Working Toward Zero Trust?

OMB Memorandum M-22-09, issued in late January 2022, calls for a collaborative effort to allow teams within and across agencies to regulate access based not only on who or what is accessing data, but also on the sensitivity of the data being requested.

One key component of NASA's response to this mandate is the OCIO's *Cybersecurity Improvement Portfolio (CIP)* (link internal to NASA). Managing projects and initiatives as a portfolio realizes greater benefits, efficiencies, and points of integration than working on each effort individually. The CIP focuses exclusively on projects and initiatives that mitigate cybersecurity risks, achieve compliance with Federal mandates, and deliver a Zero Trust Architecture.

Zero Trust is a marathon, not a sprint. It will take years to achieve Zero Trust (target level) and years to achieve the optimized state (advanced). We realize that this is a tectonic shift in how we create, use, and protect resources (DAAS—Data, Assets, Applications, Services).

Preloading @ NASA

By Karim Said, Goddard Chief Information Security Officer (CISO)

In 2020, the Federal Chief Information Office (CIO) announced its *"intent to preload"* all .gov and .mil domain names. Preloading will force the "green lock" in folks' browsers when they connect to Federal Government websites, which ensures the security, privacy, and trustworthiness of those connections.

Agencies are responsible for preloading their own longstanding domains. That includes NASA and the domains we manage across *www.nasa.gov*, as well as other program-specific ones like globe.gov, usgeo.gov, and scijinks.gov. In support of this effort, NASA announced its own intention to preload all agency domains by September 2024, a major milestone in our nearly decade-long push to implement the *"HTTPS-Everywhere"* standard.

Now, NASA is one of the oldest residents of the internet and manages nearly 1,800 public-facing websites, which collectively influence how the global community views and interacts with our agency. We also manage tens of thousands of websites that are accessible only on our private internal networks, upon which we rely to do all of our day-to-day work. Along with that history and complexity, we carry the weight of thousands of technical choices made by thousands of systems administrators. Some of those choices weren't always made through the lens of modern cybersecurity, so orchestrating the preloading of our domains is no simple task!

So why bother? One view might just call the whole thing a bureaucratic "compliance" activity. From this perspective, preloading is just another in a long line of arbitrary requirements foisted upon our helpless agency.

I don't agree with that view. For me, cybersecurity has never and will never be about "compliance," and I bristle every time I hear the term applied to what are fundamentally sound engineering principles. Cybersecurity exists to support our mission, and a big part of that mission is rooted in our agency's good name. People trust in and rely on NASA. Integrity is core to our work, and preloading is the most effective tool we have for safeguarding that integrity across our websites.

Sure, we have work ahead. A lot of work. Tough work! But it's all in service of our mission and the public that believes in it.

AEGIS Enables Cybersecurity Enhancements for NASA

By Sylvester Placid, AEGIS Communications Team Lead, Marshall Space Flight Center

The Advanced Enterprise Global IT Solutions (AEGIS) team recently implemented several cybersecurity enhancements for NASA:

- AEGIS received concurrence from NASA Senior Agency Information Security Officials (SAISOs) and approval from Authorizing Officials (AOs) for enterprise Wide Area Network (WAN) and Local Area Network (LAN) System Security Plans (SSPs). AEGIS conducts annual authorizations from AOs to assess the health of SSPs, analyze vulnerability management performance, and review risk items. NASA commended the AEGIS team for the high quality of a recent review and our continuous monitoring program.
- A new credential set for Simple Network Management Protocol (SNMP) version 3 has been implemented on all NASA center LAN devices. This will enable the AEGIS-managed Cisco Identity Services Engine (ISE) to take over Hardware Asset Management (HWAM) requirements from the Cybersecurity Services service line within the Office of the Chief Information Officer (OCIO) and replace the existing Forescout infrastructure managed by the Cybersecurity Infrastructure (CSI) team. ISE is a next-generation Network Access Control (NAC) solution used to manage endpoint, user, and device access to network resources within a zero-trust architecture. It has been proven to increase coverage in identifying devices and provide more accurate profiling capabilities. AEGIS is powering the ISE solution for NASA to meet the ever-growing cybersecurity needs of the agency.
- AEGIS developed a Pulse Secure Virtual Private Network (VPN) dashboard requested by a senior agency information security official to provide monitoring of NASA external partner access to internal resources and improve collaboration.

AEGIS continues to migrate NASA's enterprise networks to software-defined access (SDA), an innovative approach to network security and automation being deployed across the agency.

Shaping Cybersecurity Policy for Space

By Katherine Herrick, Communications Officer, Johnson Space Center

In August, the White House's Office of the National Cyber Director (ONCD) visited NASA's Johnson Space Center (JSC) to conduct an industry workshop on Space Systems Cybersecurity. Representatives from JSC and many of NASA's commercial partners gathered to discuss the state of cybersecurity policies as they apply (or do not apply) to the space industry today. The ONCD is working to update cybersecurity policy to help translate terrestrial cybersecurity practices into space cybersecurity practices. The aim is to establish best practices that can be applied across small, medium, and large organizations, covering both Federal and commercial realms. The workshop's discussions focused heavily on the theme "Cybersecurity by Design," as well as on how companies of varying sizes handle mitigations for cyber risks.

The major takeaway? With growing dependency on space systems, growing security integration across different sectors, and growing cybersecurity threats, there is an increasing need to determine the most resilient protections for our systems and data. We must understand how all the organizational and technical pieces fit into the full industry/Government ecosystem to make these policies effective, as information and its security are at the nexus of everything we do as a nation. From a NASA perspective, proactively securing our systems is imperative to ensure crew safety and mission success.

Records Management Recognized for Innovative Management Services Tool

By Patti Stockman, NASA Records Officer, Information, Data, & Analytics Services, NASA Headquarters

A development team at Ames Research Center, spearheaded by Records Manager Steven Hunt, was recognized last year with a NASA Group Achievement Award that commends the team for its "vision, dedication, digital-savvy, and user focus in developing NASA's Organizational Records Inventory (ORI) application."

The application will provide every NASA organization, program, and project with the ability to maintain an efficient, accurate, and comprehensive records inventory. All NASA records managers will be able to conduct real-time records analysis, granting full situational awareness of NASA records within their scope. The ORI also holds some promise of usefulness for Controlled Unclassified Information (CUI) and Contingency Operations management.

With NASA quickly transforming many mission support functions from center-managed to enterprise-managed models, a primary goal in developing the ORI tool was to reduce the number of center-unique records management services and achieve greater efficiency and improved service delivery.

Hunt expressed to colleagues that he feels the award extends beyond the Ames team to everyone who contributed many hours refining functional requirements for ORI, testing, and suggesting improvements. This effort to modernize and broaden NASA's records management capabilities is a success story for the entire agency's information and data management community.

NASA employees can work with their organization's Records Liaison Officer to ensure that their records are represented in ORI.

Steven Hunt displays the NASA Group Achievement Award at Ames Research Center

Records Officer Patti Stockman points out a prime example of why managing records is so important. She is holding a replica of the Apollo Lunar Rover wheel created through reverse engineering, from a test article, by a GRC Constellation Program team because the original wheel design records were not preserved. Proper disposition of records preserves NASA's legacy and serves the agency itself.

Future Horizons in Records Management

By Patti Stockman, NASA Records Officer, Information, Data, & Analytics Services, NASA Headquarters

NASA has long pushed the technology envelope, employing new technologies throughout the years to enhance the way we conduct business, accomplish our mission programs and projects, and keep the agency running. These new technologies introduce opportunities and challenges in records management for NASA and all Federal agencies.

One challenge is ensuring proper management and disposition of electronic records created through use of new technologies. Memoranda issued by the Office of Management and Budget mandate that all Federal agencies create and manage records exclusively in electronic formats by June 30, 2024.

Transitioning Federal agencies to an electronic—or "paperless"—environment is a priority to enable and increase the ability of the public to engage with Government in new and more efficient and effective ways.

Newly selected NASA Records Management Team Lead Christi Yapching will help orchestrate several initiatives that are underway toward NASA accomplishment of the mandate's intent:

- The development of the Organizational Records Inventory (ORI) – an enterprise tool conceived by Steven Hunt, Records Manager at Ames Research Center, for the oversight of records agencywide. As the ORI is populated by NASA organizations, records managers will be able to identify the locations of all physical (e.g., paper) records, allowing them to work with organizations to produce only electronic records.
- The revision and consolidation of NASA records retention schedules is another enterprise initiative, led by Anne Mills at Glenn Research Center, that aims to reduce the number of retention schedule items. Records Managers are also exploring means for an automated, user-friendly way to identify schedule items that prescribe how long their records must be maintained.
- Cloud capabilities, including SharePoint Online, OneDrive for Business, and Exchange, will also be leveraged. The broader team supporting agency records management is spearheading the deployment of a new capability for managing records in the MS Cloud.
- As part of the agency web modernization, a team of archivists developed criteria for assessing NASA web content that is historically, culturally, scientifically, or technologically significant. Future application of these criteria could enable identification and capture of this valuable digital content for eventual transfer to the National Archives.

With the opportunities and challenges presented by new technologies and the transition away from physical to electronic records, it is essential for NASA organizations to leverage the expertise and responsiveness of our records management professionals. Records management services within Information, Data, & Analytics Services of the Office of the Chief Information Officer enable targeted assistance to functional and mission organizations and are available as a resource to all of NASA.

Internal records management resources are available on the *records management site*.

The NASA records management community met at Ames Research Center in March 2023 to collaborate on ways to move NASA forward to better manage records.

AR/VR and STEM

By Phil Posey, Mission Program Enabling Applications Service Element Chief, Application & Platform Services, Marshall Space Flight Center

In July, The Application & Platform Services (APS) AR/VR team represented NASA, alongside Astronaut Anne McClain, at the Learn Fresh STEM event at the MLB All-Star game in Seattle, WA. Launched in partnership with the MLB Players Trust, MLB Players STEM League is a baseball-inspired program for middle-school-age youth. The program brings to life the energy of the sport through a board game and curriculum that cultivates students' math and social-emotional skills. The event featured students across the United States and Latin America. *Learn more about the event at their website*.

At the event, the APS AR/VR team led students through an interactive STEM activation that allowed them to experience the AR/VR technologies developed by the team. This event was a huge success and students expressed great excitement with the AR/VR activities.

The APS AR/VR team's public outreach goals include engaging with the general public to provide a positive image of NASA's efforts in science for all mankind, whether it is at a large tradeshow such as CES, SXSW, MegaCon, or at smaller local exhibitions such as Orlando's Science Center Otronicon and NASA's Dreamflight night event. *Learn more about the APS AR/VR team here* (link internal to NASA).

Coming Soon: The NASA IT Strategic Plan for Fiscal Years 2022–26

By Jonathan Walsh, IT Strategic Planner, Strategy & Architecture Office, NASA Headquarters

The new NASA IT Strategic Plan outlines our vision for the strategic use of information and technology at NASA through fiscal year (FY) 2026. This plan provides a unified direction for mission alignment, roadmaps, investments, and accountability for NASA's IT community to help achieve NASA's Strategic Plan. Once published in the October timeframe, the plan will be available on OCIO's public website.

The agency's IT strategy focuses on achieving outcomes—the impacts and change NASA's missions need to be successful. We engaged NASA's mission directorates, mission support offices, and centers during formulation, as well as external stakeholders. Execution of this plan will maximize the value of our IT contribution to NASA's missions and partners, as well as the public.

The NASA IT Strategic Plan identifies five strategic goals and underlying strategic objectives and performance objectives for IT. Our goals are to deliver great customer experiences; achieve consistent operational excellence; transform NASA through information and technology; and ensure proactive, resilient cybersecurity—all delivered by an exceptional team.

These goals provide a focus for roadmap and investment priorities that will continuously guide the allocation of IT resources to help accomplish NASA's missions. We are excited about the journey ahead, and we are ready to make this vision our reality with our mission partners.

IT Talk

National Aeronautics and Space Administration

Office of the Chief Information Officer
Mary W. Jackson Headquarters
300 E Street SW
Washington, DC 20546

www.nasa.gov