National Aeronautics and Space Administration

IT Talk

Oct - Dec 2024 Volume 14 • Issue 4

Cybersecurity Dashboards and the Importance in Safeguarding NASA's IT

IT Talk

Oct - Dec 2024 Volume 14 • 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
Michelle Kim

Cover Design
Kelley May

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/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

Cybersecurity awareness can be a challenging topic for many of us here at NASA. And in an era of increasingly sophisticated cyberattacks, we can feel inclined to keep it at arm's length.

That is why, during October's Cybersecurity Awareness Month, NASA's theme is **"Fall in Love with Cybersecurity."** Our goal this year is to foster agencywide readiness for embracing cybersecurity practices, with a focus on zero-trust principles.

In this issue, we will spotlight our Information System Owner (ISO) and Information System Security Officer (ISSO) SharePoint site that provides ISOs/ISSOs with the valuable resources to protect our data integrity and maintain a secure system. We will learn how the platform's toolkit, including data-driven dashboards and helpful hyperlinks, helps safeguard our information technology while achieving Federal compliance.

We will also share details on the Cybersecurity & Privacy Division's (CSPD) new open-source handbook, offering a look into how our IT communities collaborate to create a resource for teams to peer-review their code using a centralized guide to cybersecurity best practices.

Nurturing a cybersecure culture cannot be complete without the efforts of our employees. From managing Government devices to understanding Zero Trust Architecture, it is vital to stay educated through the latest training in cybersecurity safety awareness from our IT Security Awareness and Training Center (ITSAC) team.

Lastly, we wanted to find a way to congratulate the remarkable work that our team has done. We are sharing the OCIO team members who received Agency Honor Awards this past year to express our sincere gratitude to the OCIO team for always bringing their A-game!

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):

- *Thank You for Making Intune Migrations a Success!*
- *Follow Me Print Now Available at All Centers*
- *Windows 11 Availability*
- *SpaceBar Launches at Glenn Research Center*
- *Approval Required Before Installing Beta Operating Systems on Managed Mobile Devices*
- *Best Practices for Secure Meetings on Webex and Teams*
- *Ordering Software and Support for GFE Computers*
- *Order a Computer for Testing Purposes - Free of Charge!*
- *Teams Enhancements: Meet the Updated Planner App; "New" Label Removed from the New Teams Icon; Turn Off Notifications for Posts in Your Teams Channels; Collaborative Notes; Move the Sharing Toolbar; and More*
- *See What's New with ICAM*

Inspiring Future Engineers and Cybersecurity Experts at the University of South Carolina

By Bonita Oliver, Chief Information Security Officer (CISO), Stennis Space Center

The Office of the Chief Information Officer (OCIO) Cybersecurity & Privacy Division (CSPD) was invited by Kennedy Space Center (KSC) Exploration Ground Systems (EGS) to join the University of South Carolina in participating in the Partners for Minorities in Engineering and Computer Science (PMECS) workshops held on campus on June 13 and 27. PMECS is a partnership between educators and businesses aimed at providing gifted minority students with academic enrichment in the career areas of engineering and computer science. The workshops are designed for rising 9th- through 12th-graders, who attend one of two weeklong sessions.

Yves Lamothe, KSC EGS Senior Systems Engineer, and Bonita Oliver, SSC CISO, introducing students to the importance of cryptology at the University of South Carolina.

Bonita Oliver and Tamiko Fletcher, Chief Information Security Officers (CISOs) at Stennis Space Center (SSC) and KSC respectively, attended the event with EGS Senior Systems Engineer Yves Lamothe. With the assistance of Karim Said, CISO at Goddard Space Flight Center (GSFC), they developed activities to introduce students to cryptography and explore careers in computer engineering and cybersecurity. Cryptography, a method of protecting information and communications using codes, is crucial for modern-day encryption and secure messaging.

Bonita Oliver, SSC CISO, working with students to answer questions about cryptography activity.

Students enjoyed learning about cryptography and encryption, and the camp counselors were equally engaged in deciphering the cryptic codes. The activities emphasized teamwork, communication, and the assignment of roles and responsibilities to achieve goals. Students asked questions about cyber degree programs, the difference between those and engineering degree programs, and even inquired about NASA "secrets."

It was a wonderful experience to collaborate with our fellow NASA colleagues in KSC EGS and within CSPD to support PMECS. We hope this annual effort continues, as it is a great opportunity to inspire the next generation of explorers and cybersecurity professionals.

Tamiko Fletcher, KSC CISO, working one-on-one with a student hoping to inspire the next generation of cybersecurity professionals.

NASA's HERA Project: Cybersecurity Expert Tiffany Snyder Joins the Mission

By Tiffany Snyder, IT Cybersecurity Specialist, Cybersecurity & Privacy Division, Kennedy Space Center

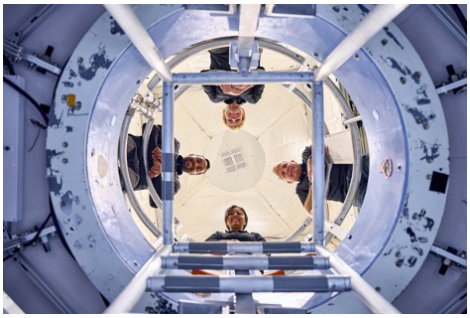
In 2022, NASA employees were invited to participate as volunteers to support human space flight by applying to be a part of the Human Exploration Research Analog *(HERA) project*. Volunteer researchers will test various hazards (isolation, light and dark cycles, and distance from Earth) in a 650-square-foot habitat for approximately 45 days. The HERA habitat is at Johnson Space Center in Houston and is an analog for the isolated and confined living environment of a long-duration space flight mission.

We are happy to announce that one of OCIO's own, Tiffany Snyder in the Cybersecurity & Privacy Division, was selected to participate in the upcoming Campaign 7 Mission 4 (C7M4) crew. C7M4 will run from mid-October until the end of December.

As one of four crewmembers, Tiffany will perform science experiments, extravehicular activity simulations, habitat systems maintenance and housekeeping, and research data and biological sample collections.

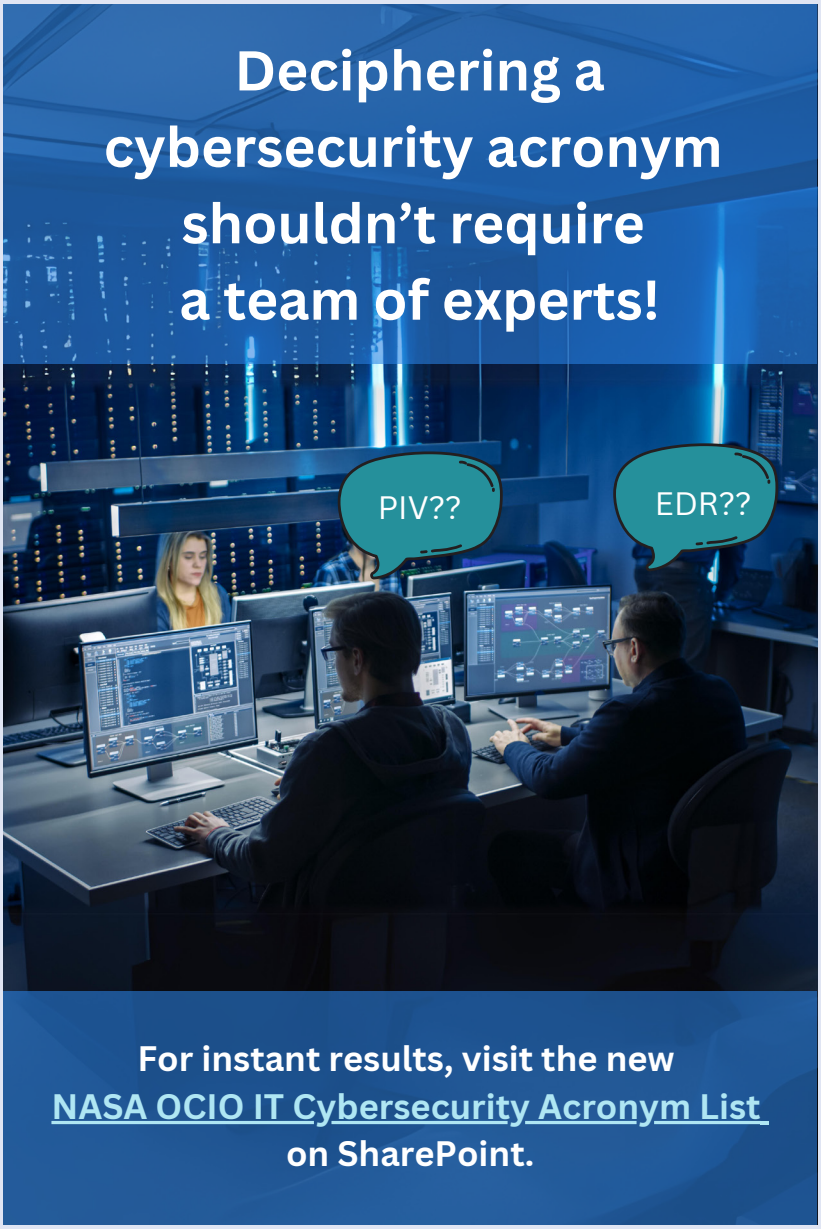
Tiffany is looking forward to working with her fellow crewmembers and hopes that her experience with information technology and cybersecurity will be invaluable as she completes this mission. As a HERA crew member, Tiffany will continue to bridge understanding and partnership between OCIO and NASA missions, representing our OCIO brand and bringing back valuable knowledge.

NASA OCIO Cybersecurity Expert Tiffany Snyder



Human Exploration Research Analog (HERA) Project

NASA's HERA habitat at Johnson Space Center



Cybersecurity Dashboards and the Importance in Safeguarding NASA's IT

By Nick Stavrakis and Janice Haas, Cybersecurity Services (CyS) Communication Team and Shawn Postich, CyS Service Management Service Area Manager, Glenn Research Center

NASA's mission of advancing science, technology, and space exploration relies heavily on the ability to protect data and maintain secure systems. In today's digital age, cyber threats and vulnerabilities have become a primary concern for organizations managing critical and sensitive data. In recognition of these challenges, the Cybersecurity & Privacy Division (CSPD), in collaboration with the Cybersecurity Service Line, has developed a *SharePoint Information System Owner/Information Systems Security Officer (ISO/ISSO) Resource website* (link internal to NASA).

The site features an extensive collection of cyber dashboards and hyperlinks to pertinent cyber resources that help ISOs/ISSOs monitor, assess, and manage the security of information systems. The site is a valuable tool for individuals tasked with safeguarding NASA's resources, supporting mission success, and fostering innovation while maintaining operational integrity.

Streamlined Security Monitoring and Management

The site provides visitors with streamlined access to a vast array of cyber tools, services, and monitoring and management processes offered by CSPD. As NASA operates numerous and complex systems, from spacecraft to ground control systems and scientific databases, each of these systems requires a tailored approach to cybersecurity. The site offers ISOs/ISSOs a "cyber tool bag," complete with hyperlinks to quickly locate and access training, cyber dashboards, and related cyber services.

By aggregating cyber resources into a centralized compendium, individuals in the role of ISO/ISSO are better positioned to identify and manage cyber threats and vulnerabilities. This collection of resources supports timely and informed decision-making and incident response, critical in an environment where a single breach could have significant repercussions for ongoing space missions or scientific research. The scope of cyber resources available on the site facilitates enhanced visibility for ISOs/ISSOs across systems and fosters engagement and coordination among diverse cyber skillsets.

Enhanced Risk Management and Compliance

NASA, like all Government agencies, must adhere to regulations and standards for cybersecurity and risk management. The ISO/ISSO Resource website provides a valuable framework for individuals tasked with cyber compliance requirements, including adherence to guidelines set forth by the National Institute of Standards and Technology (NIST) and other Federal agencies.

This is especially important for NASA as it manages sensitive data related to national security, international partnerships, and proprietary research. The ability to proactively address potential compliance issues helps NASA better manage risk, disruption, delays, and other potential operational impacts.

Improved Decision-Making Through Data-Driven Insights

The ISO/ISSO Resource website promotes data-driven insights that enable NASA's cybersecurity teams to make informed decisions about system security and risk management. The site aggregates various cyber resources—including security incident reports, system

audits, and vulnerability scans—into a single, easy-to-navigate interface.

Supporting the People Who Support NASA Cybersecurity

The ISO/ISSO Resource website is intended to normalize and create a baseline of institutional cyber knowledge for all ISOs/ISSOs regardless of years of experience. Individuals new to the role are introduced to valuable resources to better position them and their work for success. The site is also in a continual state of evolution, with new content being incorporated regularly, and offers visitors an opportunity to recommend additional content to the site. Cyber is a team effort that works best with readily available and ever-increasing knowledge, which is why the site is available NASA-wide.

The Bottom Line

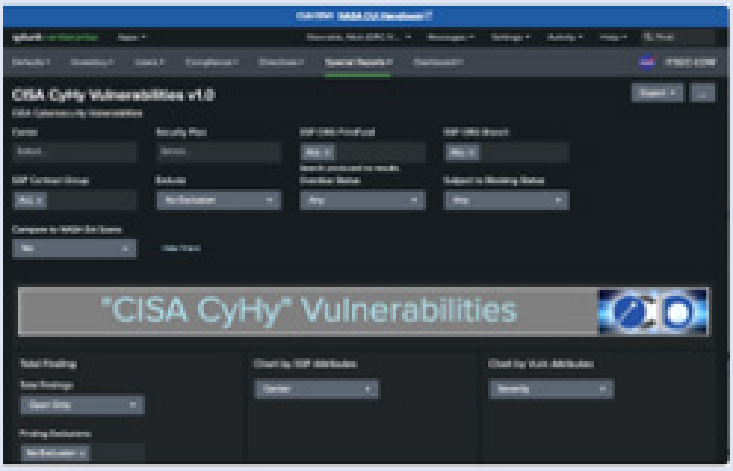
The goal of the ISO/ISSO Resource website is to aid in keeping NASA at the forefront of cybersecurity, enabling the agency to focus on safeguarding NASA's information technology, resources, and missions, including Artemis II and the NASA 2040 Project. In an era when cyber threats are constantly evolving, the site is a powerful tool that plays a critical role in protecting NASA's information systems, ensuring compliance, and supporting risk management efforts. As we continue to evolve and enhance the site to better serve its intended audiences, the Cybersecurity Service Line welcomes and encourages feedback and recommendations.

Learn more (links internal to NASA):

- *ISO/ISSO Resource Website*
- *ISSO as a Service Website*

Dashboard Images:

Examples of ISO/ISSO SharePoint Resource Dashboards



Eight Ways AEGIS Enhanced NASA Cybersecurity This Year

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

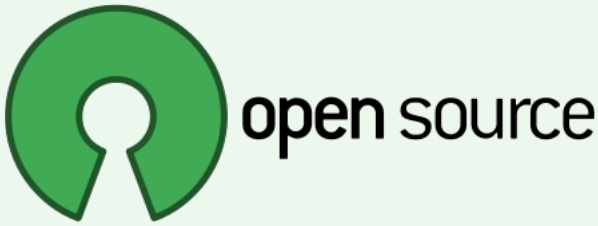
This year, the Advanced Enterprise Global IT Solutions (AEGIS) team completed cybersecurity enhancements to the NASA environment in support of Cloud and Computing Services (CCS), Cybersecurity Services (CyS), Network and Telecommunications Services (NaTS), and Workplace and Collaboration Services (WCS):

1. Working in close coordination with the NaTS Enterprise Network Operations Center (ENOC), the AEGIS team completed a redesign of the Virtual Private Network (VPN) at all Trusted Internet Connection (TIC) sites (Ames Research Center [ARC], Goddard Space Flight Center [GSFC], Johnson Space Center [JSC], and Marshall Space Flight Center [MSFC]). This effort moved the untrusted interfaces for VPN from peering routers to Demilitarized Zone (DMZ) routers, which strengthens the agency's security posture and enables security policy implementation for inbound and outbound VPN traffic at the TIC sites. This enhances security for the agency VPN by leveraging existing equipment at no cost to NASA.
2. AEGIS designed and implemented the Pop-Up Network (PUN) project, which minimizes risk to NASA from unintentional "data spillage." Throughout the NASA network, encryptors help protect against espionage or manipulation of data from unauthorized sources. In the unlikely event that an encryptor device is configured incorrectly or fails in an "open" position instead of securely closed, the encrypted network traffic may "spill" into the untrusted side of the device, leaving the data vulnerable. PUN provides a secure enclave for encrypted traffic from encrypted devices across the NASA network, with logical separation using virtual local area networks and virtual route forwarding tables to isolate encrypted traffic from the rest of the NASA network. The PUN project enables deployment of future encryptors to leverage the secure enclave.
3. AEGIS enhanced NASA Amazon Web Services (AWS) monitoring for CyS by integrating AWS Guard Duty reporting with enterprise cybersecurity logging. The new capability automates the previous manual notification process that required a NASA Security Operations Center (SOC) ticket to be entered when a finding is identified. The new process improves security monitoring in the NASA AWS environment by presenting alerts directly in the SOC dashboard, reducing response time for incidents.
4. AEGIS obtained Authority to Operate (ATO) for the Lockheed Martin partner network and change board approval from CyS for a VPN extension to the Lockheed Martin facility supporting the X-59 Quesst supersonic aircraft, a revolutionary plane designed to help NASA reduce sonic booms for the Low-Boom Flight Demonstrator project. Both accomplishments are critical for supersonic flight testing to begin this year.
5. The Secure Network Analytics Manager (SNAM) is now operational at all NASA centers following a rapid, five-month implementation. SNAM aligns with Software Defined Access (SDA) deployment as a network flow monitoring and analysis solution. It supports end-to-end and Zero Trust Architecture across NASA as part of the overall agency response to the Presidential Executive Order on Improving the Nation's Cybersecurity and protect Federal Government networks. SNAM captures network flow analytics within NASA corporate local area networks and provides real-time network analysis and cybersecurity threat intelligence integrated with Cisco Digital Network Architecture, Identity Services Engine, and SDA.
6. The AEGIS team at JSC supporting CCS replaced the DigiCert

certificate on JSC's Hitachi Content Platform (HCP) system with a NASA Internal Certificate Authority (NICA) certificate. The activity required updating undocumented Java keystores in a vendor-provided solution with trusted NICA root certificates. Transitioning to a NICA certificate resulted in cost savings for the agency and resolved data-in-transit vulnerabilities in HCP associated with using DigiCert.

7. When vulnerabilities were identified in the global Ivanti VPN service used by NASA, the Department of Homeland Security mandated swift action by Federal agencies to remediate the threat. The AEGIS team coordinated a maintenance activity in support of the agency's response to Ivanti to complete password changes to the enterprise infrastructure for wired, wireless, and VPN connections at every NASA center during an 8-hour period, with no issues. More than 700 AEGIS-managed service accounts spanning CCS, NaTS, and WCS were password-reset at least twice over a 48-hour period, with no significant disruption to service.
8. AEGIS introduced additional improvements to enhance NASA's cybersecurity posture during the last year. Two-factor authentication was implemented for Voice over Internet Protocol (VoIP) server infrastructure, bringing enhanced security to critical infrastructure. AEGIS teams supporting NASA Communications (NASCOM) mission infrastructure at GSFC introduced enhanced intrusion-detection scripting and monitoring with new automations, eliminating manual steps and improving data quality while providing NASCOM with surge resourcing for specialized cybersecurity scripting support. The AEGIS team at KSC developed a new process to more easily identify and validate decommissioned devices, ensuring that they can no longer access the NASA network.

The AEGIS team continually works to enhance agency cybersecurity, helping to keep NASA missions safe.



Open-Source Principles And Cybersecurity

By Karim Said, Cyber Information Security Officer (CISO), Headquarters/Goddard Space Flight Center

In my current role, I provide cybersecurity reviews for NASA-developed software. Sometimes this code is working its way through our *public open-source software release process*; sometimes the developers are targeting operational deployments in one of our private computing environments; and other times folks are just looking to share what they have written with their colleagues. This software spans the various classes defined by *NPR 7150* and supports everything from complex, highly specialized scientific computation to garden-variety office automation. In all cases, though, the software developers have a noble aim to solve common problems and help others do the same.

Why Does This Matter?

Well, while I consider this work a privilege and an appetizing challenge, I recognize that, as an individual, I cannot provide the sorts of meaningful cybersecurity reviews necessary across such a huge and diverse corpus of code as we have at our agency. Daunting resource constraints aside, I simply do not have the technical expertise to review code for all the various languages, frameworks, dependencies in use, and unique requirements the code might address. Being such a bottleneck also conflicts with my longstanding admiration of the open-source software community and the prioritization of transparency, flexibility, and community collaboration. These principles drive much of how I take on my day-to-day work, and without them I am just getting in the way.

It is for these reasons that the Cybersecurity & Privacy Division (CSPD) of OCIO is developing a handbook that enables software developer teams around the agency to self- and peer-assess their own code through a cybersecurity lens and in alignment with the National Institute of Standards and Technology (NIST) frameworks relied upon by our agency's cybersecurity stakeholders. The handbook will prioritize rigorous version control, modern software engineering workflows, transparency of documentation, and a collaborative spirit.

Most importantly, though, the handbook will recognize that no single author can solve the agency's sticky software cybersecurity problems. Communities are stronger than individuals, so we will open-source the content. Over the next several months, early drafts of the handbook to various interested communities will be circulated in preparation for publication to our agency's primary instance of *GitHub Enterprise* (link internal to NASA), where we will hopefully be able to engage with, and benefit from, the rich expertise and insights of the broader NASA community.

Exciting News: Power App Premium Licenses Are Here!

By Chris Blakeley, Enterprise Automation Services Product Manager, Application and Platform Services, Kennedy Space Center

The NASA Enterprise Automation Service (NEAS) office is thrilled to announce that Microsoft Power App Premium licenses are now available across the agency! This upgrade brings enhanced tools and features that will take our app-building capabilities to the next level. Whether you're already using Power Apps or new to the platform, the Premium license opens up exciting possibilities for creating more powerful and efficient applications.

So what does this mean for you? With Power App Premium, you now have access to advanced features like **Dataverse**, which allows you to store and manage data more effectively. However, it is important to note that setting up a Dataverse environment involves additional costs beyond the standard licensing. If you are interested in using Dataverse, *visit our website* (all links internal to NASA) to learn more about the costs and setup requirements. You will also gain access to **Premium Connectors**, enabling seamless integration with more systems and data sources across the agency. More info on connectors can also be found on *our website*.

In addition to these features, Power App Premium now enables you to build **Model-Driven Applications**, giving you the ability to create complex, data-driven apps with little to no code. These apps are designed around your data model and provide rich user interfaces without needing to start from scratch.

For more details on the Power App Premium rollout or to explore how these features can enhance your work, we encourage you to connect with the NEAS office. The NEAS team is here to support you in making the most of these new tools. The *NEAS website* includes resources and assistance. *The NEAS Community of Practice* is a virtual hub located in Teams, fostering collaboration among NEAS, vendors, and NASA personnel. We are excited to see how you leverage these capabilities to streamline processes and improve efficiency!

NASA IT Service Management and Artificial Intelligence

By: Walters Ngwa, ITSM ServiceNow Suite Analyst, and John Sprague, IT Chief Engineer, OCIO Service Management Office (SMO)

The Service Management Office (SMO) ensures that Office of Chief Information Officer (OCIO) IT services are delivered to our customers and stakeholders in a timely fashion. To facilitate this goal, SMO is integrating to a single IT Service Management (ITSM) solution across all OCIO Service Lines (SLs), Agency Level Offices (ALOs), and Center CIO organizations. SMO assesses new ITSM features, including incorporating the best technology advancements like artificial intelligence (AI), to enhance how OCIO delivers IT.

Knowing AI has been safely used at NASA for decades and meets the *Executive Order on the Safe, Secure, and Trustworthy Development and Use of AI*, SMO, in partnership with other OCIO teams, is working towards augmenting current OCIO ITSM AI features to continue improving the customer experience with faster search results and less wait time for information.

SMO is working with other organizations to assess the incorporation of new features like Chat Summarization and Generative AI (Gen AI). Gen AI, for example, can create new content like text, images, and even music. While relatively new at NASA, it can be used to optimize search time and utilize past searches to provide more detailed responses, and it can quickly create informative images for use in presentations, documents, and websites. SMO continues to assess new technologies for enhanced customer experiences while ensuring efficient IT service delivery.

For more details about the SMO and how we support NASA and OCIO missions, visit the *Service Management Office (SMO) website* (link internal to NASA).

2023 Agency Honor Awards

Congratulations to the 2023 Agency Honor Awards winners from across our OCIO teams!

EO & DEIA Achievement Award

Mary Collins, Laverne Dickens, Mary McKaig, Shaun Piazza, Anastasiya Plachta, Katie Poole, Courtney Ritz, Jason Smith, Sherrey Williams, Michele Wockenfuss, Taylor Bromante, Jamie Dulaney, Hilary Gambale, Scott Johnson, Wes Meives, Liz Stroud, and Catie Tresslar from the HQ/GSFC OCIO Employee Engagement Committee

Diversity Equity Inclusion and Accessibility Medal

Doug England

Early Career Achievement Medal

Corey Portalatin-Berrien

Exceptional Achievement Medal

- Christopher Blakeley
- Mariah Champagne
- Ann Whitener

Exceptional Engineering Achievement Medal

- James Dumoulin
- Louis Nicoli

Group Achievement Award

- Doug Lemere, Baylee Bourque, Monti Muhsin, Kevin Poe, and Benjamin Stevens from the Building 1111 Consolidation Team
- Stanley Hush, Mark Knop, and Wade Mickley from the Agency African American ERG Collaboration Team
- Theodore (Ted) Sidehamer and Jeremy Yagle from the NASA Engineering Safety Center (NESC) Thermocouple Anomaly Investigation Team
- Matthew (Matt) DeGrave, Stormie Fulton, Sherri Jessup, Karthik Krishnamurthy, Brian McCormick, and Morgan Whitfield from the RSES Contract Transition & Operational Teams
- Anthony (Tony) Arviola, Kevin Boswell, Robert Mestes, and Jonathan (Jon) Welters from the SmartLab Team

MSFC Group Achievement Honor Award

Greg Burks, Tab Black, David Cross, and Bob Dean from the MSFC National Space Science Technology Center (NSSTC) Operations Support Team

Silver Achievement Medal

Jordan Rasmussen from the LaRC Center Operations Information Systems (CODIS) Systems Administration Team

Silver Group Achievement Award

- Donald Edgerly from the 2023 NASA Langley Open House Events Planning Team
- Morgan Whitfield from the RSES Team Leadership

Fall in Love with Cybersecurity

By Jennifer Jento, Training Specialist, IT Security & Awareness Training Center (ITSATC), Glenn Research Center

For the past 21 years, October has been declared Cybersecurity Awareness Month by the President of the United States and Congress. Cybersecurity Awareness Month is a collaboration between the Government and private industry to raise awareness about digital security and empower everyone to protect their personal data from digital forms of crime.

In recognition of Cybersecurity Awareness Month at NASA, the Digital Transformation team is partnering with NASA's Cybersecurity & Privacy Division and the IT Security Awareness and Training Center (ITSATC) to provide meaningful ways to learn and appreciate cyber-security initiatives throughout the month.

This year's campaign focuses on Zero Trust principles, recognizing cybersecurity as a journey rather than a destination. Led by the Digital Transformation team, this initiative aims to enhance our workforce's ability to understand and champion cybersecurity and Zero Trust Architecture (ZTA).

Throughout the month, NASA's awareness efforts will focus on how people can make smart decisions at work, school, and home to remain safe and secure online.

- See *"Fall in Love with Cybersecurity"* (links internal to NASA) for more information about upcoming Zero Trust webinars and resources.
- Visit the *ITSATC site* for cybersecurity awareness resources, webinars, and videos.

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