National Aeronautics and Space Administration

IT Talk

Oct - Dec 2022

Volume 12 • Issue 4

Remote Work & Cybersecurity

IT Talk

Oct - Dec 2022 Volume 12 • 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/ocio/ittalk

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

www.facebook.com/NASAcio

In this Issue

Message from the NASA CIO

Making smart cybersecurity decisions—whether on the job, at home, or at school—is crucial in today's ever-changing world. That's why it's important that we all take basic steps to protect our online information and privacy.

During October, I am encouraging everyone in the NASA community to participate in center cybersecurity awareness activities as part of National Cybersecurity Awareness month. Cybersecurity is critical to ensuring the integrity of NASA data and, ultimately, the overall NASA mission. This year's theme is "See Yourself in Cyber," which encourages us to recognize our part in maintaining cybersecurity, no matter the role we play.

In this issue, we'll explore cybersecurity challenges of working from anywhere. It's important that we all understand why remote working poses more of a threat to your security than working from an office. We'll also look at vulnerabilities and ideal ways to work safer and protect yourself and your organization against cyber threats.

And finally, there are several key behaviors we should all follow:

- Use NASA's Virtual Private Network (VPN) when working remote
- Enable multifactor authentication
- Recognize and report phishing and malware to the NASA Security Operations Center
- Use strong passwords
- Update software and apply patches

Cybersecurity begins and ends with all of us. I want to thank everyone for your diligence and commitment to Cybersecurity Awareness Month and helping us stay secure and safe online.

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):

- *Backup Services Subscription Changes Enable Subscribers to Back up Data on Any Computer That Has Druva Installed/Activated*
- *ESD Launches New Look and Feel for Ordering Enterprise-Managed Devices*
- *Ordering Upgrades/Augments for Computer Hardware After It's Delivered*
- *Project Online Now Available to Order*
- *Webex 42.6 Upgrade Introduces 21 Fixes and New Features*
- *How to Move Files to OneDrive to Free up Hard Drive Space*
- *Recent Teams Feature Updates to Enhance Productivity Include Automatic Groupings in Channel Posts, Chat with Self, Assign Co-organizer to Meeting, and Pre-create Breakout Rooms Before Meeting Starts*
- *See What's New with ICAM*

NASA's Digital Library Soars to New Heights

By Charles Beebe, ALPS Scrum Master, Marshall Spaceflight Center

When the NASA Library community's leadership approached our team in 2020 with a request to build a prototype for the Agency Library Portal System (ALPS), we had no idea what a stroke of luck had befallen us! Being selected to prototype the digital library platform of the future for the agency has been a dream come true—we still have to pinch ourselves sometimes.

So, what is ALPS? Put simply, ALPS is the agency's future shared suite of essential digital library tools. Whether you're a postdoctoral research fellow, a librarian, an archivist, or even an intern, the NASA Library community is currently building a prototype of a platform that will allow you to access the majority of NASA's library content quickly and easily from any device on a NASA network. ALPS connects to both external reference collections and internal NASA systems, and it is centralized, cloud-native, and scalable under the hood. This will connect all agency employees to all library resources, regardless of physical location. It will modernize, consolidate, and unify the operation of the agency digital library resources needed for the efforts of the Office of Communications (OCOMM) in conjunction with the Information, Data, & Analytics Services (IDAS) and Application & Platform Services (APS).

The 18-month process of project development was quite an adventure. The project got off the ground just a few months into the COVID-19 pandemic; however, Bob Sherouse (NASA Headquarters), Robin Dixon (Goddard Space Flight Center), Greta Lowe (Langley Research Center), Kate Dunlap (Glenn Research Center), and their teams handled that challenge with the utmost professionalism and made it a delight for us to start getting smart on library tech. Even for a team with years of experience and multiple awards for agency-level custom cloud application development, there was a lot of potential scope to explore for the ALPS prototype! Also, a huge thank-you to everyone in the OCIO who worked with us and our fellow 2021 IT Innovation Fund (ITIF) cohort to secure project funding. We were incredibly grateful to work with the aforementioned Library stakeholders and Lori Parker from IDAS to identify the core features most valuable to the agency's future shared suite of essential digital library tools:

- Replacement of Internet Protocol (IP) address-based access to the agency's subscription portfolio with Launchpad login.
- "Ask-a-Librarian" chat with reference librarians.
- "Discovery" (library search) across all integrated external and internal reference collections.
- Enterprise search via integration with NASA's Enterprise Data Platform (EDP).
- Integration with Galaxie, the agency's digital card catalog.
- Inter-library loan for physical titles.
- An agency-level portal that Library personnel can maintain.
- A center-level Library portal for each center that Library personnel can maintain.
- Visualization of subscription and user analytics via integration with NASA's EDP.

When NASA Library stewardship transitioned from the Office of Strategic Infrastructure (OSI) to OCOMM last fall, Perri Fox (HQ) took the reins from Bob Sherouse and masterfully kept up the momentum needed to close out the 18-month project development period and kick off a 12-month technology demonstration to create an ALPS prototype. Perri and Robin's commitment and engagement as a part of the

Charles Beebe, Scrum Master

Megan McCarty, Frontend Developer

Mckenzie Kane, UX & Design

Perri Fox, Product Owner

Karina Garces, Backend Developer

Gamble Gilbertson, Area Manager

Robin Dixon, Library SME

David Nagarpowers, Backend Developer

Chris Shenton, Cloud Architect

(Continued from page 4)

integrated product team have enabled us to make progress at an exceptional pace and with a keen attention to detail. From interviews with Janine Bolton (Johnson Space Center) and Ken Wright (HQ) to roadmap development in December 2021, it's truly been a treat to have stakeholders who are willing to roll up their sleeves and nerd out with us!

As we've made our way through the first half of the core feature development, we have also been very impressed by the vendors in the library technology community. It turns out we're not the only ones inspired by the NASA Library community's passion! The teams from all the library tech vendors have been great to work with, which has allowed us to fully consider a wide range of best-in-class tools for this new platform. And, of course, shout-outs to our NASA-internal vendors: Michael Pritz (LaRC) and the Galaxie team; Jason Duley (HQ) and the EDP team at Marshall; and Ian Sturken (Ames Research Center), Heather Thomas (JSC), and our other teammates in the Web Services Office.

We've saved the best for last: a huge thank-you to everyone in the broader NASA Library community for their warm reception at this year's Library Face-to-Face at Goddard. From the welcoming and inquisitive atmosphere to their enthusiastic participation during our presentation and the presentations that came before us, we have seen that they all have a passion for their craft. It was super fun to get to meet all of them and play "ALPS: The Game!" with them, and we're excited to work with Perri and Robin to incorporate all of their feedback to bring every patron of the agency's libraries the best possible platform.

The NASA Library community inspires us to do our best work every day, and we earnestly hope to continue this collaboration for years to come.

Goddard Hosts NASA's Annual Cybersecurity Awareness Event

By Hilary Gambale, NASA Headquarters/Goddard Space Flight Center (GSFC) OCIO Code 702 Strategic Communications Specialist, and Shannon Riley, Lead Event Coordinator, GSFC Cybersecurity Training Manager (CTM) and ITSATC Team Member

Every October is Cybersecurity Awareness Month, and this year Goddard Space Flight Center is honored to host NASA's annual Cybersecurity Awareness Month Program Kickoff event on October 5. The event is virtual and involves much planning and coordination between the Goddard Cybersecurity Training Manager and Lead Event Coordinator, Shannon Riley; the Cybersecurity Services (CyS) IT Security Awareness and Training Center (ITSATC) supporting Cyber Protection (CP) within the Cybersecurity & Privacy Division (CSPD); the Federal Business Council; and OCIO communication specialists. The event promotes the theme of *"See Yourself in Cyber,"* which demonstrates that even though cybersecurity may seem complex, ultimately, it's really about simple steps people can take to address it. The agenda for the kickoff event includes three speakers from government and industry who will provide participants with examples of real-world cyber situations, information on the basic steps they can employ to protect their online profiles and privacy, and how all NASA employees have a responsibility for cybersecurity at work.

Opening the event, Special Agent David Ko, who represents the FBI Houston Field Office, will speak about some of the techniques, tactics, and procedures used by Cerber Ransomware actors as learned from his investigation in that case. The keynote speaker is Mike Witt, NASA's Senior Agency Information Security Officer (SAISO) and Chief Information Security Officer (CISO) for Cybersecurity and Privacy. He will focus on the "people" aspect of cybersecurity and encourage NASA employees to see themselves in cyber, no matter what role they play. Attendees will be encouraged to do their part to help protect and safeguard NASA's data and systems, as well as protect themselves from cyber threats on the job and at home.

Closing out the speaker sessions is Tatiana Rodriguez, a Senior Certified Information Systems Security Professional (CISSP)/ Certified Cloud Security Professional (CCSP) Lead Technologist for Booz Allen Hamilton. Rodriguez plans to demystify cybersecurity by explaining how cyberattacks that are in the everyday news can affect individuals at home. She demonstrates that corporations and government agencies are keepers of sensitive information, whether that is personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, or governmental and industry information systems. When that information is stolen, it can affect you personally, especially if your information is part of the data being taken.

In addition to the speaking events, the ITSATC team will be hosting four cybersecurity awareness webinars throughout the month of October for NASA employees. We are looking forward to the 2022 NASA Cybersecurity Awareness Month Program's great success! The kickoff will shed light on an important part of cybersecurity: an individual's role in helping to protect personal and organizational data. With all of the valuable and exciting events that are taking place in October, we can't wait for next year's program.

Remote Work & Cybersecurity

By Kelly Dreyfuss, Strategy and Business Management Officer, CSPD, NASA Headquarters; Leah Skowron, Strategy and Business Management Analyst, CSPD, NASA Headquarters; Dennis DaCruz, Chief Cybersecurity Engineer, CSPD, NASA Headquarters; Brenda Ellis, IT Security Training Lead, CSPD, Glenn Research Center; Jomill Wiley, IT Security Training Specialist, CSPD, Glenn Research Center; Jennifer Jento, IT Security Training Specialist, CSPD, Glenn Research Center

As a NASA employee, you are a known target for cyberattackers, especially when you are connecting to critical NASA information systems from home. Cybercriminals know that telework security could be an afterthought or completely overlooked. They will take advantage of security lapses to gain access not only to sensitive NASA information, but even possibly to anything else connected to your home network.

Don't worry! Here are some simple, effective steps you can take to create a cybersecure home office, and they are relevant whether you are using your NASA devices or your own personal desktop or laptop.

Cybersecurity Tips for Remote Work

1. ***VPN/Wi-Fi Security***
   A VPN, or a Virtual Private Network, connects a user's device to a secure server, making the connection private. That way, internet users can access any website or page without exposing their identity or private data. Connecting to the VPN ensures that you are securely accessing the NASA network. A public Wi-Fi network is inherently less secure than your personal, private one, because you don't know who created it or who else is connected to it. Ideally, you wouldn't ever have to use it; better to use your smartphone as a hotspot instead.

   Ensuring that your home network is secure is paramount for teleworking. Make sure your home Wi-Fi network is private by securing it with a strong password and limiting access as much as possible. Creating a guest network for your router is a good way to ensure that your personal network is secure and only accessible to you. Be aware of what devices are connected to your network as well. Today, everything from smartphones to lights can be connected to your home network. Once you know what is connected, make sure each device has a strong, unique password. Many devices come with default passwords that anyone can learn by searching the Internet; change the password

when you receive the device. Securing your Wi-Fi network is a key component to a secure telework environment. Check out this cool video about securing your home's wireless network: *SSA Securing Home WiFi*.

2. ***Password Hygiene***
Use effective password hygiene such as selecting a unique password or passphrase, minimizing reuse of old passwords, and changing your password on a regular schedule. Using a passphrase instead of a password adds length and complexity, making it harder for cybersecurity criminals to guess and easier for you to remember. Reusing old passwords or using the same password for multiple websites leaves your accounts vulnerable. While it may be tempting to use the same password for everything, it is a best practice to use different passwords for each account.

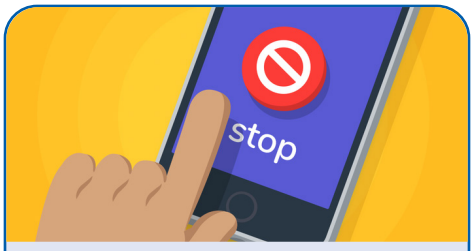
3. ***Software Updates and System Backups***
Software updates offer plenty of benefits. It's all about revisions. These might include repairing security holes that have been discovered and fixing or removing computer bugs. Updates can add new features to your devices and remove outdated ones. When alerted about a software update on any of your devices, be sure to install the latest available version as soon as possible. For more information about NASA Software Updates, please visit our *Knowledge Base article*.

System backups ensure that your system is recoverable in case of malware/ransomware infection, hardware failure, or user error. Backups are an important part of your overall system security. For more information about backing up your NASA system, please read our *Druva inSync Support Knowledge Article*.

4. ***Document Storage and Transmission***
Always ensure that documents can be safely accessed remotely. Use NASA devices and NASA-approved cloud services to store all NASA content. Files stored on cloud servers are encrypted, making it harder for cybercriminals to access. When sharing documents or collaborating, only use agency-approved videoconferencing, collaboration tools, and file-sharing methods from NASA devices such as Microsoft Teams, OneDrive, and NASA Box. For more information, read *The NASA Approved Teamwork Tools List*. Utilize digital documents as much as possible and refrain from printing hard copies of NASA sensitive information. Make sure to additionally encrypt or password-protect any sensitive documents or information you are sharing.

5. ***Social Engineering and Phishing***
Scammers and cybercriminals are always looking for new ways and schemes to take advantage of changing work environments. They may use social engineering sites such as Facebook, Twitter, Instagram, and others to obtain critical information regarding your whereabouts and use the collected data in e-mail or messenger phishing attempts. If you receive a phishing attempt, unusual web meeting requests, or any other suspicious communications on your NASA device, please do not click on anything in the message and immediately report the activity by contacting our Help Desk/Security Operations Center at *soc@nasa.gov*.

As a NASA employee, it is your personal responsibility to protect and manage the current work environment from which you are accessing NASA's information. Exercising proven telework best practices will be essential in continuing to safeguard NASA's information. Remember that your telework location must match or exceed security measures utilized on site. For more tips on working remotely, please review the *Telework Security Overview and Tip Guide* from the National Cybersecurity Center of Excellence (NCCoE). STAY VIGILANT!



Block Harassing Calls to Your NASA Desk Phone or Jabber Client

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

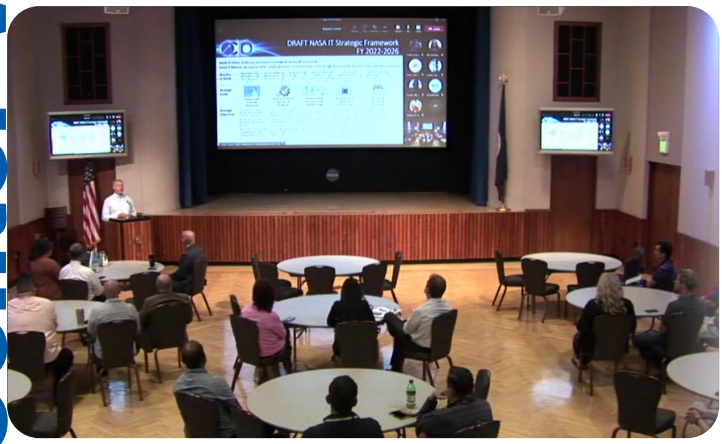
Network and Telecommunications Services (NaTS) has introduced a new service to block harassing calls to your NASA phone number and enhance security. NaTS manages nearly 19 million calls every year across 120,000 NASA endpoints, including desk phones, softphones, analog phones, vIPer phones, and conference room phones. NaTS processed more than 1.5 million calls this past June, with firewall enforcement on more than 10,000 harassing calls.

If you are receiving harassing calls on your NASA desk phone or Jabber client, use the *Harassing Call Block request form* on the Enterprise Service Desk (ESD) portal. **If you feel your life is in danger, please call 911 immediately.** For more details, please refer to this knowledge article (*KB0021507*). If you need to block calls to your NASA mobile phone number, contact the ESD for assistance by calling 1-877-677-2123 and selecting option 2, or by visiting the *ESD portal*.

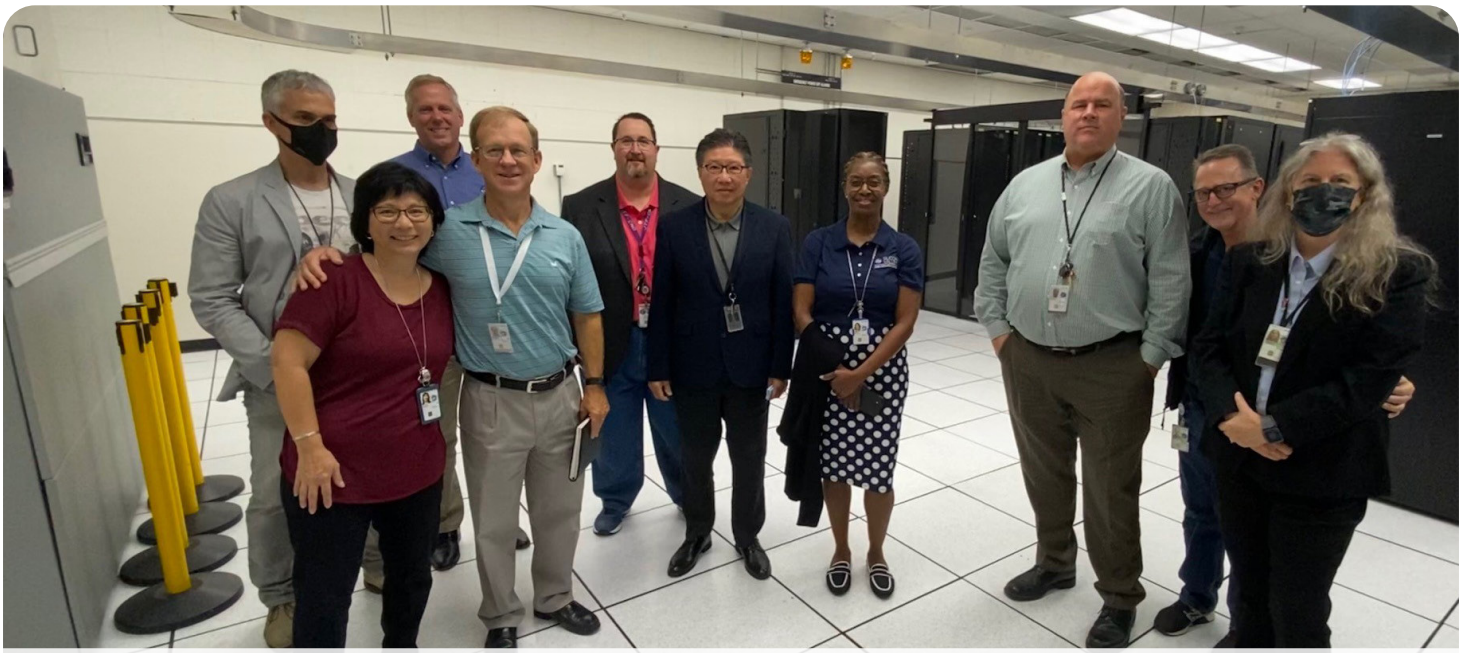
Center Visit Photos

Ames OCIO Welcomes Senior Leaders to the Center. Photo credit: Penny Hubbard

Jeff Seaton presents during a hybrid All Hands, to over 100 Ames OCIO team members. Photo credit: Penny Hubbard



Jeff Seaton visits the Glenn Research Center OCIO All Hands on July 11.



Jeff Seaton and Senior leaders are given a tour of the Ames N233 Data Center. Pictured here – Back Row: John Garrigues-Ames CIO, Jeff Seaton-OCIO, Mike Witt-SAISO; Front Row: Grace De Leon-CCS, Neil Rodgers-DCIO Operations, Robert Chow-AEGIS, Annette Moore-DCIO Strategy, Milt Checchi-Data Center Mgr., Brian Froehling-ASRC and Lorinda Rodrigues-ASRC Photo credit: Bill Notley.

Stealthwatch Enhances Network Security and Supports Presidential Executive Order for Cybersecurity

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

Stealthwatch is a Cisco tool that provides advanced network flow monitoring and analysis within the NASA environment. Stealthwatch provides network traffic visibility and analysis across the current Network and Telecommunications Services (NaTS) legacy local area network (LAN) environment, and the new Software Defined Access (SDA) fabric-based environment. Stealthwatch can be leveraged as a critical resource to help identify and verify micro-segmentation security policies. Micro-segmentation is a critical component of the National Institute of Standards and Technology (NIST) 800-207 Zero Trust Architecture.

The objective is to achieve an end-to-end, zero-trust/least-privilege architecture across the agency with continuous monitoring, analysis, and real-time enforcement for local area networks, data centers, and cloud environments. NaTS has already deployed Stealthwatch at Armstrong Flight Research Center (AFRC), at Langley Research Center (LaRC), and within NASA Communications (NASCOM) mission environments. Deploying Stealthwatch as an enterprise network monitoring tool is part of the NASA response to the *Presidential Executive Order* to improve the Nation's cybersecurity and protect Federal Government networks.

NaTS Implements Distributed Denial-of-Service Mitigation Solution

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

Last year, Network and Telecommunications Services (NaTS) began a project to deploy an agencywide Distributed Denial of Service (DDoS) mitigation solution. An attacker uses DDoS methods to overwhelm a compute server with malicious traffic from numerous clients that reside on networks around the globe. Utilizing a partnership between one of our network equipment vendors and our DDoS mitigation provider, we deployed the solution earlier this year. The solution has already blocked its first large-scale attack since being deployed. Blocking this attack protected NASA network services and ensured network availability to NASA end users.

OCIO Team Receives SFA Award!

Eldora Valentine, OCIO Communications Manager, NASA Headquarters

Congratulations to the cross-center Cloud team, which includes JSC/Aerospace, Microsoft, and Cloud Computing Services/ MSFC Azure for receiving a 2022 Space Flight Awareness Award for the JSC Space Gloves project. The SFA Award recognizes small groups of employees that have demonstrated exemplary teamwork while accomplishing a particular task or goal in support of the human space flight program.

The Extravehicular Activity (EVA) Glove inspection team contributed to the JSC Human Space Flight program by applying Artificial Intelligence and Machine Learning (AIML) to help astronauts on the International Space Station (ISS). Through an innovative pilot, a new prototype model helped detect spacesuit glove damage through rapid inspection.

The glove inspection process is traditionally performed by a group of individuals and requires multiple days to analyze data and develop recommendations. While on the ISS, the AIML model was able to perform diagnostics and generate a recommendation in less than 45 seconds, validating how AIML technology can benefit human space flight.

For more information about SFA awards, visit *https://www.nasa.gov/directorates/heo/sfa/space-flight-awareness*.

IT Talk

National Aeronautics and Space Administration

Office of the Chief Information Officer
300 E Street SW
Washington, DC 20546

www.nasa.gov