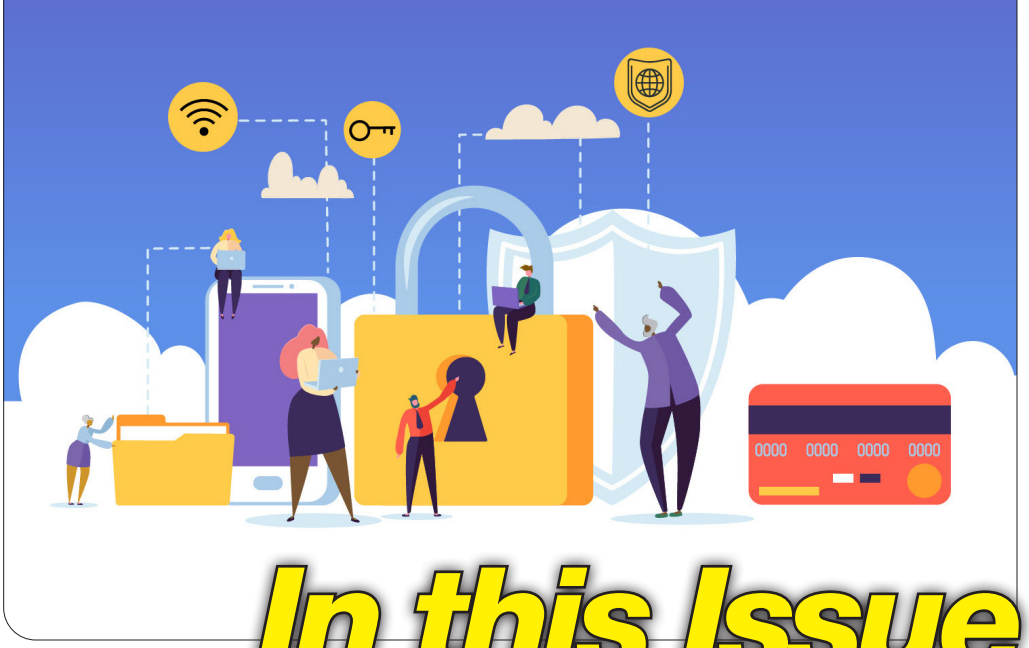
National Aeronautics and Space Administration

IT Talk

Oct - Dec 2021 Volume 11 • Issue 4

Ensuring Cybersecurity While Traveling



IT Talk

Oct - Dec 2021 Volume 11 • Issue 4

Office of the CIO
NASA Headquarters
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

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

Cybersecurity is critical to ensuring the integrity of NASA data and, ultimately, the overall NASA mission. October is Cybersecurity Awareness Month. This year's theme is "Do Your Part. #BeCyberSmart." We all need to do our part to ensure that personally, our online lives are safe and secure while we also fulfill our responsibility to protect NASA's systems and data. In this issue, we'll take a closer look at some commonsense rules to protect ourselves and our organization against cyber threats. Because we live in such a connected world, cybersecurity isn't critical only when we are in the office but also applies at home (which is also our office in many cases these days). It's also important to practice safe online behavior and secure our internet-enabled mobile devices whenever we travel, so a solid cybersecurity mindset while traveling for work or pleasure is a must.

We will also explore how Apple's new "Allow Apps to Request to Track" feature actively provides a stop to data brokers or social media sites from tracking our location or identifying us for targeted advertising.

Additionally, we will update you on how our NASA cybersecurity team has been strengthening our security posture and simplifying our online experience by implementing a new password-free process called User Based Enforcement (UBE). UBE entails reducing and ultimately removing passwords from our environment. Passwords are the number-one cause of data breaches and are challenging (and frustrating) to keep secure. With UBE, you use your PIV credentials/smartcard to authenticate to NASA networks and applications—supporting the Federal requirement (and best practice) of two-factor authentication. UBE is making a huge impact at the agency.

We have a lot of great cyber-related stories in this issue that I hope you will find relevant and interesting. At NASA, I am accountable for cybersecurity, but each one of us shares the responsibility for protecting NASA systems and data through the application of solid cybersecurity practices in our projects and personal lives. During this cybersecurity awareness month, let's all remember to do our part.

Jeff Seaton

NASA Chief Information Officer

End User Services News & Updates

Check out the latest news from the End User Services Program Office (all links are internal to NASA):

- *Virtual Mobility Sessions*
- *Travelling Internationally with a Mobile Device*
- *One-Hour Compute Refresh Process*
- *HoloLens 2 Now Available to Order*
- *macOS Big Sur Upgrades are Underway*
- *Teams: New Features Plus ViTS Integration*
- *Backing Up Secondary Hard Drives*
- *Enterprise-Managed Product Updates*

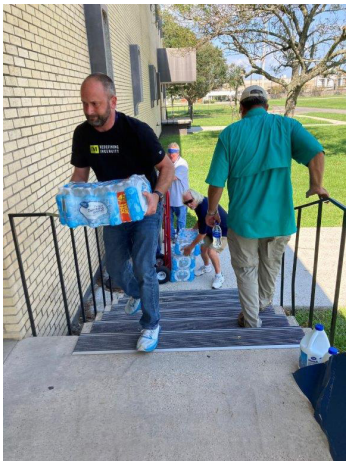
Communications Program Team Provides Supplies and Support to MAF and SSC Personnel After Hurricane Ida

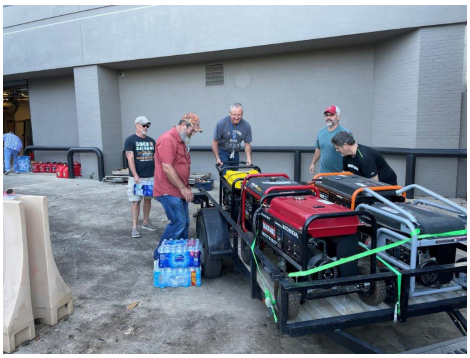
By Sylvester Placid, Communications Strategist, Communications Program, Marshall Space Flight Center

A team from the Communications Program (CP) in Huntsville, AL, provided supplies and support to personnel at Michoud Assembly Facility (MAF) in Louisiana and Stennis Space Center (SSC) in Mississippi following Hurricane Ida.

After establishing a calling tree to contact affected personnel in the region to check on emotional well-being and needed supplies, a five-person team volunteered to gather items and load two trucks and trailers with 91 cases of water, wipes for personal and household cleaning, diapers, box fans, window air conditioners, seven loaner generators and oil, and 19 five-gallon gas containers.

The team delivered and distributed the supplies to MAF & SSC on September 3.





Enterprise Data Platform Q&A

By Tobie Smith, Analytics and Visualization Coach, Marshall Space Flight Center

With the Enterprise Data Platform (EDP) system on the horizon, future users are interested in when and how they can gain access.

Q: When is EDP officially available?

A: The EDP plans to begin rollout at the end of October 2021, following an early October testing phase. The exact date depends upon when the EDP receives its Authority to Operate (ATO). After the go-live date, the EDP team will work with users to migrate their data, models, and visualizations into their sites in the EDP. A kickoff day is planned for November 17.

Q: How is access to it acquired?

A: EDP access will be controlled via the NASA Access Management System (NAMS). Users will select the appropriate site, project, and persona (e.g., creator or viewer). Site administrators will approve each user's access. If additional site resources are required, NAMS will also be used for this request.

Q: Is there training available for EDP?

A: EDP offers a wide array of training based on persona and skill level. For data asset developers, there is on-demand training available through the Tableau and Alteryx websites, as well as within the NASA SATERN Digital Academy tab.

There is also hands-on Alteryx training every Tuesday for beginners and Thursday for intermediate and advanced users through December. Sessions are being recorded for those unable to attend.

During the November 17 EDP kickoff, general training will be made available to the audience, followed by training tracks based on skill level and tools used. Site administrators will have their own training track as they learn the nuances of administering a site within the EDP.

Q: How did the EDP team pick Tableau as the Enterprise visualization tool?

A: The EDP team analyzed NASA enterprise analytic platform user persona requirements as well as objectives and goals for the NASA enterprise analytic environment. This analysis resulted in evaluation criteria for each enterprise tool function. The EDP tool evaluation criteria included supporting open architecture, supporting multiple tenants, supporting modular/reusable products, supporting low code, supporting collaborative work, being compatible with Mac OS, and minimizing life-cycle cost. We initially down-selected to ten industry tools for visualization and then reduced to the top five tools. The final evaluation resulted in a business case analysis document of more than 100 pages and included a third-party assessment. The OCIO Application Program Board process reviewed our tool evaluation approach, initial tool evaluations, technical evaluations of each tool, and tool integration, as well as the program plan for implementation. The evaluation process alone took over a year.

Annual Cybersecurity Awareness Training

The annual cybersecurity training entitled "Cybersecurity and Privacy Awareness Training" (SATERN course ID #ITS-022-001) for fiscal year 2022 was added to all employees' learning plans in SATERN on Monday, September 20, 2021. This course fulfills the Federal Information Security Modernization Act of 2014 (FISMA) requirements for security and privacy awareness training and is mandatory for any NASA employee, whether civil servant or contractor, who uses a computer to accomplish work for NASA.

Using feedback from last year's surveys, the course was created for a remote telework environment using less bandwidth without sacrificing interactivity. New features include a test-out pretest for each module, 508-compliant interactives (as opposed to text-only), and a cumulative quiz at the end of each module.

Every Government employee, and those who work with Government equipment, must be aware of their security responsibilities to ensure that information and information resources are not exposed to undue risks and to understand that all of NASA's information is considered a valuable resource that must be protected.

Individual due dates are determined by the last time a learner has completed cybersecurity training in SATERN. Instructions to look up your last completion date may be found on the *IT Security Awareness and Training website*.

For SATERN assistance, call the NSSC Contact Center at 877-NSSC-123 (877-677-2123) or send an e-mail to *NASA-satern.support@nasa.gov*. Support hours are weekdays, 8 a.m. to 8 p.m. eastern/7 a.m. to 7 p.m. central/5 a.m. to 5 p.m. Pacific.

Ensuring Cybersecurity While Traveling

By Qi'Anne Knox Whitmire, Security Project Manager, Goddard Space Flight Center and Ciana McMillian, IT Security Specialist, Goddard Space Flight Center

Travel-related incidents have been on the rise, putting both travelers and their organizations at risk. The risks vary from border to border, making business and personal travelers targets of cyberattacks. The cost of these crimes can be detrimental to an organization if sensitive data are accessed by an unauthorized source. Furthermore, the long-term effects cost organizations millions and can take years to recover from. This article will review these risks in more detail and provide tips on how to remain cybersafe during travel.

While some threats are obvious, like theft, others are not. During travel, users are at a greater risk of cyberattacks. This increase in risk is largely due to the vast range of threat vectors encountered when traveling, including public wireless network access, outdated systems, espionage, fake charging stations, theft, and Bluetooth connectivity, to name a few. Once an attacker has found their way into a system, these vectors can then be used to expose devices to malware, ransomware, and other cyber-related attacks—all potentially leading to data loss, exposure, or an astronomical financial implication.

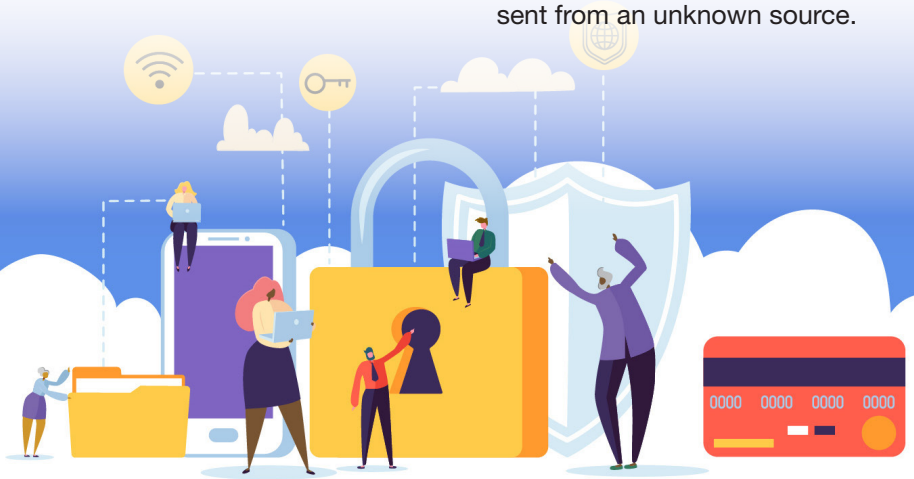
It is important to take necessary steps to always protect user and organization data during travel. This is especially true when traveling internationally, where risks to organization data and systems are greater. While no one solution is failsafe, the following are general recommendations and guidance suggestions that can be used by travelers to help them remain vigilant and cybersafe to significantly minimize risks.

BEFORE TRAVEL

- Take new or reimaged devices such as loaners where possible to minimize the amount of data stored on any device that goes with you.
- Clear out the browser cache and never set the browser to remember passwords.
- Patch devices with the latest security updates to address vulnerabilities prior to travel.
- Update antivirus software and ensure that devices have the latest approved operating systems.
- Maintain a backup of all information taken and ensure full-disk encryption.
- Transport only a minimal amount of equipment needed to complete work to decrease the number of paths a bad actor could take to access data.
- Pare down devices as much as possible to remove data, software, and applications that are not needed for the trip.
- Be aware of NASA policies regarding travel and submit requirements early to allow sufficient time for approval before leaving.
- Be aware of international travel advisories, online behavior laws, and more before travel by referencing the *State Department Country Information* site.

DURING TRAVEL

- Do not access sensitive information such as proprietary data, personally identifiable information, or financial documents, or conduct sensitive transactions over public networks. If a user must access this type of data, a virtual private network (VPN) should be used to secure the connection.
- Do not use the same passwords internationally that are used domestically.
- Toggle off wireless and Bluetooth connections when not in use. Best practice is to use a hardwired connection when possible.
- Do not accept or plug untrusted USB thumb drives or other removable media storage into devices.
- Do not use public charging stations in ride-share cars, hotels, airports, internet cafes, or anywhere USB charging may be subject to spoof attacks that steal or modify data.
- Never leave electronic devices unattended.
- Be mindful of the information shared in conversation or via social media. Though it may seem harmless, this information could make a user a primary target for a cyberattack.
- Report suspicious activities, lost or stolen devices, and any cyber-related incidents to NASA's Security Operation Center at soc@nasa.gov as soon as possible. Do not try to investigate by clicking on links or attachments sent from an unknown source.



Apple's New Privacy Setting—Is Yours Enabled?

By Daniel Cosio, IT Security Specialist, Ames Research Center

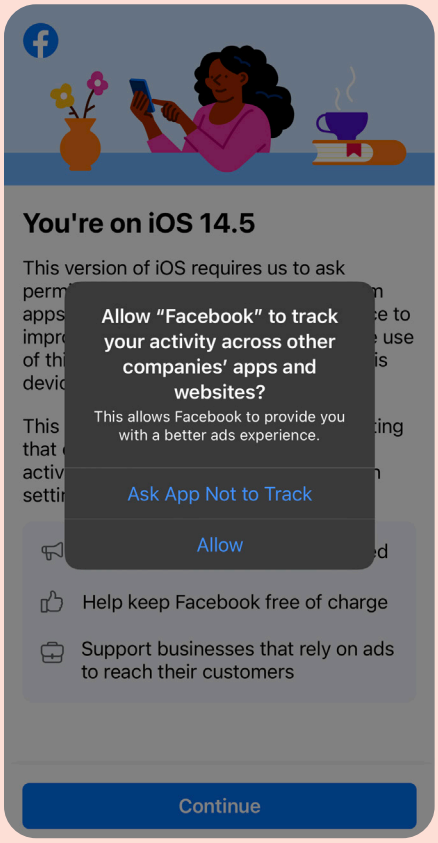
Starting with the release of iOS and iPadOS version 14.5, Apple is giving its iPhone and iPad users more control of how apps use their personal data to track them.

Websites, apps, and social media companies frequently track users' online and offline activities to harvest their personal data. Many smart phone apps and websites you visit collect data from your smart phone and sell it to data brokers. Data brokers are third-party companies that purchase these data to create a comprehensive profile about a user, including tracking a user's location and products a user browses for, as well as identifying a user's purchasing habits.

An Identifier for Advertisers (IDFA) allows advertisers to keep track of a particular device, like a smartphone or desktop computer. This IDFA is not hardware-based, so a vendor like Apple has the ability to modify or disable this tracking function.

Apple's new "Allow Apps to Request to Track" feature actively provides a way to stop data brokers or social media sites from tracking users' location or identifying users for a targeted advertisement campaign. If you were issued a NASA iPhone or iPadOS device, you may want to make sure this feature is enabled. Some of these data brokers and social media sites are not U.S.-based.

To confirm if the "Allow Apps to Request to Track" feature is enabled, on iPhones or iPads, go to Settings > Privacy > Tracking. Once the feature is enabled, the next time it encounters an IDFA, you will get a message (similar to the image above) and will have the opportunity to choose what tracks you. Remember, you need to be at a minimum of version 14.5 to use this new feature.



AFTER TRAVEL

- Change passwords on all devices after returning from travel.
- Do not connect devices back to your organization's network until cleared by the cybersecurity office via scans or preferably a reimage due to potential compromise.

CONCLUSION

Cyber-related crimes remain one of the greatest threats to users during travel simply because it is when the user is most vulnerable. Adversaries take advantage of these weaknesses to access high-value information and systems. Remaining vigilant about your surroundings and following the recommendations provided in this article not only will provide users with peace of mind but will also arm them with the best defense mechanisms to be cyber-smart. Even with the best precautions being taken, this does not guarantee 100 percent that networks, devices, and data will remain secure; however, it does minimize the risk.

As always, users should continue to stay abreast of policies and guidelines provided by their organization, IT travel offices, and export control offices, as well as local and state government. Devices used during travel may be compromised and should be assessed before exposing an organization's network to risks. A rule of thumb is to only take what is needed because less is more! Additionally, taking a proactive approach to cybersecurity is mission-critical versus reacting to breaches in real time, when it is unfortunately too late.

ADDITIONAL RESOURCES

- *CISA Cybersecurity While Traveling Stop, Think, Connect Tip Card*
- *CISA Cybersecurity While Traveling Own, Secure, Protect Tip Sheet 122019-508*
- *Federal Bureau of Investigation Business Travel Brochure*

National Aeronautics and
Space Administration

“Cybersecurity: Stronger Together”

NASA CYBERSECURITY
AWARENESS MONTH

During October 2021, Cybersecurity teams from across the Agency will come together to present a comprehensive enterprise Cybersecurity Awareness Program with weekly topics to emphasize protecting NASA’s assets, improving our security processes, and creating a stronger knowledge-based community.

Tuesday, October 5	12:00 pm CDT	2021 NASA Cybersecurity Awareness Month Kick Off
Thursday, October 7	1:00 pm CDT	DARPA CASE/ACROS Tools
Wednesday, October 13	9:00 am CDT	Solar Winds
Thursday, October 14	2:00 pm CDT	Confessions of a Real-Life Hacker
Tuesday, October 19	1:00 pm CDT	Controlled Unclassified Information (CUI) Transition Status
Wednesday, October 20	1:00 pm CDT	Cloud Services & SAAS Panel Discussion
Thursday, October 21	10:00 am CDT	New Techniques to Boost Your CQ (Cyber Intelligence)
Tuesday, October 26	12:00 pm CDT	Beware of the ROSE’s Thorn
Wednesday, October 27	1:00 pm CDT	History of the Enigma Machine

Visit the ITSATC Web site for more information.

CYBERSECURITY AWARENESS MONTH

Do Your Part. #BeCyberSmart

By Tammy Ashraf, Senior Systems Engineer, Goddard Space Flight Center

Did you know that according to the Cybersecurity and Infrastructure Security Agency (CISA), there are currently an estimated 5.2 billion internet users, which represents 63 percent of the world's population? With so many online users comes a tremendous amount of risk and responsibility for users to protect themselves. Cyber self-defense basics can go a long way toward keeping you and your data out of the hands of bad actors. Every user should own their role in protecting their data and devices by starting with the following basic steps:

USE A STRONG AND UNIQUE PASSPHRASE

When setting up passwords for your online accounts, use a strong passphrase for extra security. A passphrase is a sentence that is at least 12 characters long and should include capital letters, numbers and symbols that are easy for you to remember.

USE MULTI-FACTOR AUTHENTICATION

Along with a strong passphrase, add another layer of security by using multi-factor authentication (like biometrics, security keys, or a one-time code) whenever offered.

UPDATE YOUR SOFTWARE REGULARLY

Configure your devices to automatically update or notify you of available updates. Make sure to include your personal computers, smartphones, and tablets to reduce the risk of infection from ransomware and malware.

CHECK YOUR PRIVACY SETTINGS

Any time you sign up for a new account, download a new app, or purchase a new device, check and configure the privacy and security settings for information sharing. Continue to check and update your privacy settings at least annually to make sure you are aware of any changes.

BE WARY OF PHISHING SCAMS

Be very cautious when clicking on links or downloading files in e-mails, texts, and social media posts from strangers. Phishing tactics are used by cybercriminals to get access to your sensitive information.

SHARE SOCIAL MEDIA WITH CARE

Think before you post information about yourself and your loved ones on social media, especially when revealing personal information such as your home location. Cybercriminals could potentially use this information to target you.

USE WI-FI HOTSPOTS WITH CAUTION

Public Wi-Fi hotspots are typically not secure, which means that anyone connected to the public network can see what you are doing on your device. Limit your use of public Wi-Fi and, if you do need to use it, avoid logging into your personal e-mail and financial accounts. Instead, use a Virtual Private Network (VPN) or a personal/mobile hotspot if you need a more secure connection.

Additional tips to stay safe online can be found at *https://www.cisa.gov/cybersecurity-awareness-month*. For information about NASA Cybersecurity Awareness Month activities, visit *https://nasa.sharepoint.com/sites/itsatc/SitePages/October-is-National-Cyber-Security-Awareness-Month.aspx*.

Challenges Posed by Cloud-Based Software

By René Smeraglia, Chief Information Security Officer, Johnson Space Center

Cloud-based software is not a new concept. Most of us have been dealing with applications and services hosted in the cloud for 10 years or more. In fact, the Federal Risk and Authorization Management Program (FedRAMP) celebrates its 10-year anniversary in 2021. The FedRAMP provides a standardized approach to security authorizations for cloud service offerings. Information security practitioners have long since learned that whether FedRAMP-certified or not, every Government application needs to have its security controls assessed and documented in a security plan. Receiving software as a service (SaaS) rather than installing it locally may change the paradigm, but the security community is prepared to adapt. We are frequently reminded that Presidential Executive Order (PEO) 14028, "Improving the Nation's Cybersecurity (14028)," challenged Federal agencies to "accelerate movement to secure cloud services, including software as a service (SaaS)." Less often quoted from the PEO is the caution to do so "in a coordinated, deliberate way that allows the Federal Government to prevent, detect, assess and remediate cyber incidents."

In recent months, the Johnson Space Center cybersecurity team has heard a similar refrain from our security community; many traditional software vendors have transitioned to a SaaS delivery model, and some no longer offer on-premise options. The proliferation of new SaaS offerings has led to a corresponding rise in the number of security plan requests. This can stress resources in our security organizations. Even when the cloud software/service is properly procured, it is often seen as a cost-saving and time-saving measure. Unfortunately, the cost of initiating a security plan and the time needed to achieve an authorization to operate (ATO) has sometimes not been included in planning.

These issues are simple compared to those posed by so-called shadow IT, where some individual users are so eager to implement the "accelerate" part of the PEO that they may unknowingly skip over the security plan and supply chain risk management (SCRM) process. These users sign up for a "free" SaaS subscription that is usually not free, often not legally licensed, and almost never fully secured.

One area where we can work as an OCIO team is to help our customers properly plan the costs and timing involved in obtaining ATO for cloud applications and services. Together, we can help ensure that these flexible and efficient services are also licensed, reliable, and secure.

Communications Program Initiatives Keep NASA's Networks Secure

By Sylvester Placid, Communications Strategist, Communications Program, Marshall Space Flight Center

The Communications Program (CP) is implementing initiatives to help keep NASA's networks secure.

- **Network Access Control (NAC):** NAC improves the security posture of NASA's networks and implements the tools and capabilities required to enable access controls to networks across Centers. NAC is critical for the Agency to understand who, how, and what is authorized to access our network infrastructure. CP completed NAC enforcement on NASA's corporate networks earlier this year.
- **Software-Defined Access (SDA):** SDA deploys an innovative approach to network security across NASA's networks, enabling "just in time" provisioning of network access for any credentialed user or device while keeping out intruders and unauthorized personnel. This moves NASA toward a "zero trust" network architecture, which has been proven to prevent data breaches. SDA streamlines and automates the decisions and manual configurations needed for network security policies and reduces the need for reactionary patching and updates.
- **Virtual Private Network (VPN):** CP continually updates VPN clients and infrastructure to ensure that personnel working remotely can connect to NASA resources securely. Safeguarding remote connectivity has been particularly critical during the last 18 months of telework as NASA personnel have been accessing NASA data from their home networks.
- **Domain Name System (DNS):** CP manages the public DNS for www.nasa.gov, allowing the world to access the wealth of knowledge and resources on NASA's websites. Over the last year, CP has taken steps to protect against a distributed denial-of-service (DDoS) attack, which would disrupt NASA's ability to connect to the internet and prevent users from accessing NASA's websites and web-based services.

Cybersecurity Advocate Program Flourishes at JPL

By Sara Steffan, Cybersecurity Awareness and Training Lead, Jet Propulsion Laboratory, California Institute of Technology

After launching in early 2019, the Cybersecurity Advocate Program has helped to increase cybersecurity awareness throughout JPL and to communicate important updates from the Office of the Chief Information Security Officer (CISO). The volunteer-based program has recruited members across divisions and organizations within JPL to serve as knowledge-sharing liaisons to collaborate with the cybersecurity team.

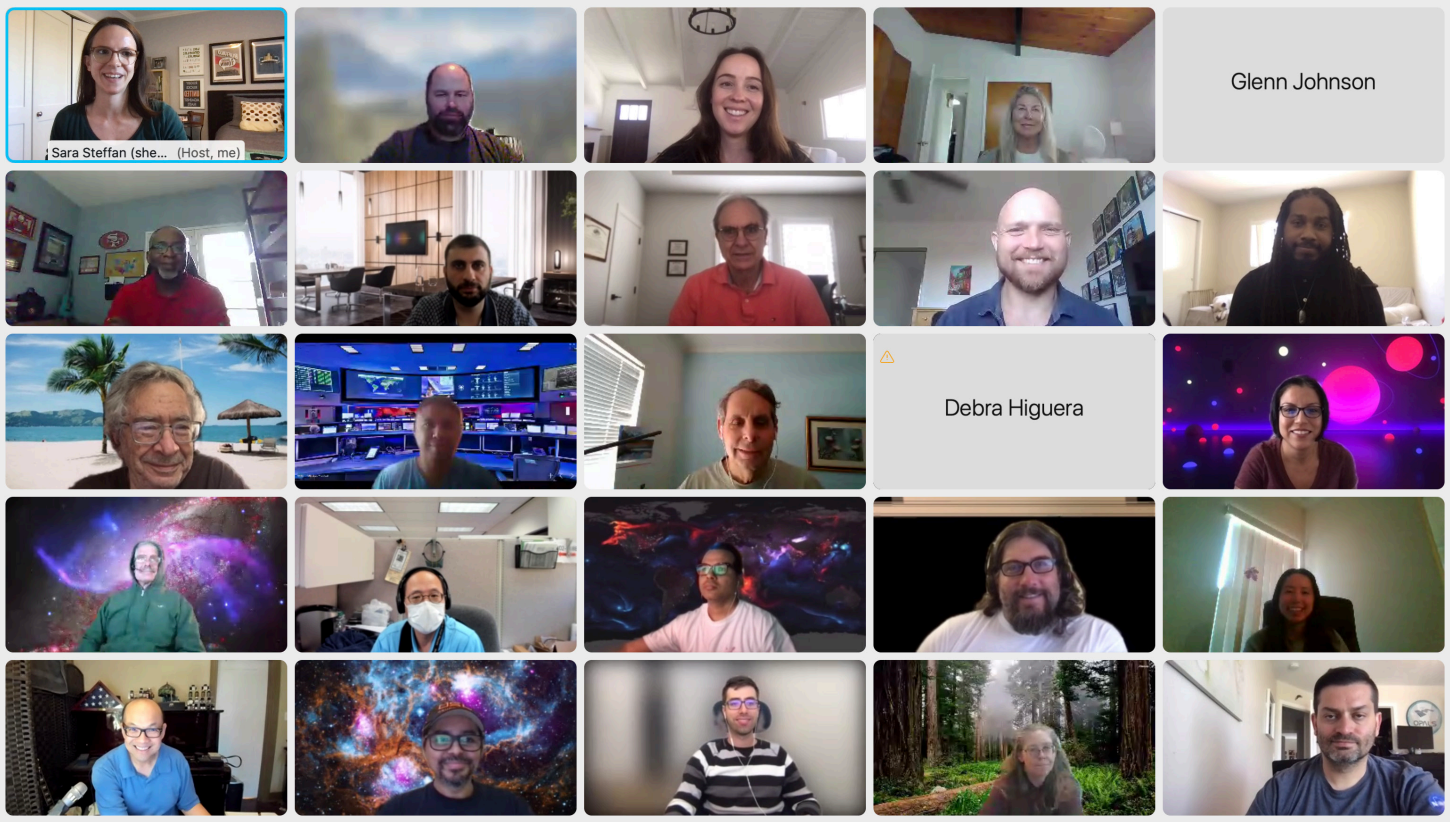
Monthly meetings with Advocates have solicited employee feedback to foster conversation around cybersecurity-related issues they may encounter in their own work. The meetings simultaneously provide a critical platform for members of the Cybersecurity and Identity Engineering and Operations teams to announce upcoming changes, program rollouts, or other security issues in an open format, so that questions can be addressed and anticipated issues can be covered in more formal communications.

"We've had exponential growth in the cybersecurity field worldwide, and JPL has picked up the pace internally as well, growing our cyber workforce and making our own personnel more aware and more vigilant," said Frederick Beck, section manager of JPL Cybersecurity and Identity. "The Advocate program is a key part of this outreach, and we've been proud of how enthusiastic they've been about volunteering their time to learn."

The program started small and has grown thanks to the participation of eager Advocates, including building an internal site to store meeting notes and presentations to increase accessibility. Even since becoming entirely virtual in early 2020, the meetings have consistently brought more than 50 people together to discuss the changing cybersecurity landscape during remote work.

"As an Advocate I have found new appreciation for all the work our cybersecurity team has being doing," said Aram Pagaryan, business administrator in the Autonomous Systems Division. "I'm excited to be part of and engaged with the Cybersecurity Advocate program as it continues to evolve."

Future program goals include expanding to a minimum of one Advocate for every division at JPL. With more representation across JPL, the Cybersecurity Advocate program can achieve many cybersecurity program successes, including growing attendance at cybersecurity awareness events and improving on-time completion rates of annual mandatory NASA cybersecurity training.



Cybersecurity Advocates during a monthly meeting in September 2021.

Data Modeling Helps Guide the DART Spacecraft in a Game of Interplanetary Billiards

By Daniel Horton, End User Services Program Office Communications, Marshall Space Flight Center

In almost every other instance, crashing a spacecraft would be an extraordinarily bad thing. For Skyler Kleinschmidt, it is the end goal of the mission. “It’s not a regular spacecraft you’re used to hearing about,” he admits.

The ultimate destructive goal of Kleinschmidt’s work is unlike many others at NASA. The Double Asteroid Redirection Test (DART) vehicle will ultimately play a game of space billiards, slamming itself at a speed of 6.6 kilometers per second into the secondary body of an asteroid. “Unlike most spacecraft with dozens of scientific instruments, it’s really got one instrument on it, which is essentially a camera that makes sure it’s going to hit the right spot.”

It is not just for a fun game of interplanetary demolition derby, either. The DART mission is designed to test how a future craft could defend Earth in case of a projected asteroid impact. DART is the first mission run by the Office of Planetary Protection, which aims to protect Earth from other potentially harmful bodies in our solar system and beyond.

In September 2022, the DART spacecraft will slam into the orbiting secondary body, Dimorphos, of the near-Earth asteroid Didymos. The spacecraft will attempt to divert the path of this 160-meter-wide moonlet as a test and demonstration for future applications.

“It’s trying to demonstrate a kinetic deflection technique,” describes Kleinschmidt. “We’re like a dragonfly smashing into a semi-truck on the highway.” While that may not sound like much, just a tiny deflection can have a huge impact on the path of an interplanetary object. “If you were taking off in a plane from Los Angeles and going to Washington, DC, you might not notice it if you were off by just a few degrees. But by the end of the trip, you could end up being a few hundred miles away.” By crashing into the Didymos moonlet, DART will attempt to prove that this is possible on a larger scale within our solar system.

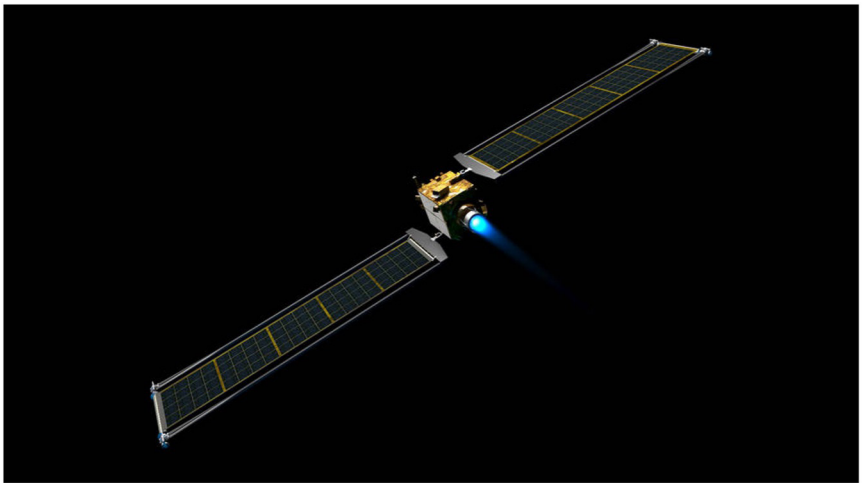


Illustration of DART spacecraft

While supporting the Launch Services Program, Kleinschmidt and his team have been hard at work ensuring the flightworthiness of the payload’s SpaceX Falcon 9 rocket in the past year. They have been able to continue their work remotely thanks in part to End User Services Program Office (EUSO)–supplied laptops that have kept them connected. The load out for Kleinschmidt has included support to run various projection models.

Hitting this interplanetary eight ball with the DART cue ball has taken a lot of this type of data crunching. “Calculating the effects of radiation from space weather on the rocket can take hundreds of simulations,” explains Kleinschmidt. “On launch day, we also look at all the telemetry coming back off the rocket to monitor the health of systems like avionics, propellant tanks, and engines.” Just one reading exceeding a limit can cause a delay if the launch team cannot troubleshoot the issue in time.

As the launch window for DART approaches in November of this year, Kleinschmidt admits that his position has become bittersweet. He mentions that the launch vehicle he provides support for is “the taxi that takes along a passenger. We drop off the spacecraft in orbit and make sure we didn’t break anything on the way up, then we say bye while they do things with cool ramifications for humanity.”

IT Talk

OCIO Designer Wins Graphic Design USA American InHouse Design Award!

Congratulations to Michael Porterfield, OCIO Senior Graphic Designer, for winning *Graphic Design USA's (GDUSA)* American Inhouse Design Award. Porterfield won for his unique design of a new NASA OCIO logo. This is one of 350 projects chosen out of more than 6,800 entries. For nearly 60 years—since 1963—*GDUSA* has been a business-to-business information source for graphic design professionals.

National Aeronautics and Space Administration

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

www.nasa.gov