



IT Talk

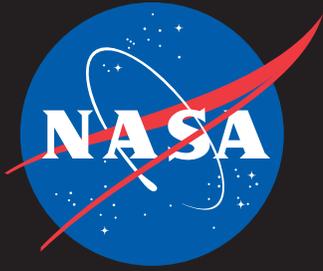
October - December 2018

Volume 8 • Issue 4

Don't let data...



slip through your fingers



IT Talk

Oct - Dec 2018

Volume 8 • Issue 4

Office of the CIO

NASA Headquarters

300 E Street, SW
Washington, D.C. 20546

Chief Information Officer

Renee Wynn

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/ocio

◆ inside.nasa.gov/ocio

(Internal NASA network only)

◆ www.nasa.gov/open/

 www.facebook.com/NASAcio



3 Message
from the CIO

4 Cybersecurity
@Home

6 Don't Let Data
Slip Through
Your Fingers

9 Cybersecurity
and You: A Day
in the Life

13 JPL Open
Source Rover

Message from the NASA CIO

All of us need to do our part to ensure that our personal and work online lives are kept safe and secure. Everyone needs to remain diligent about protecting themselves from hackers and privacy breaches. Scammers of all sorts bombard us through pop-ups, viruses, phishing e-mails, and even phone calls. NASA works around the clock to protect mission and corporate systems, Agency data, and sensitive information. And protection of NASA's data through better management of our IT footprint is a critical step in protecting NASA. Our annual cybersecurity training is intended to reinforce the importance of your role in protecting NASA's data.

National Cybersecurity Awareness Month is an annual designation observed in October. I'm asking everyone to be more cautious and take steps to protect themselves.

- Be aware of phishing e-mails and do not click on unfamiliar links.
- Do not send classified, sensitive but unclassified, or otherwise confidential information unencrypted through e-mail.
- Choose passwords that are strong, long, easy to remember, and hard for others to guess.
- Shut down, hibernate, or lock your laptop every night and whenever you take it out of the building.
- Lock all mobile items overnight.
- Don't leave devices unattended in public places.
- Avoid leaving devices in vehicles for long periods; short-term, they may be locked in trunks. Never leave them exposed in a parked car!
- Encrypt all files that contain Personally Identifiable Information (PII).
- And on a personal note, when using social networks, use the privacy settings to protect your personal information.

We have some great information in this issue to help you protect yourself and your organization against cyber threats.

I hope you enjoy reading this quarter's issue.

~Renee



OCIO and Center CIO leadership visiting Glenn Research Center in Cleveland, OH on August 6-10, 2018.

Cybersecurity@Home

By Meredith Isaacs, Communications Specialist, NASA Headquarters

Cybersecurity awareness is essential at work and at home—following online best practices should be part of your whole day. But many of us do not have cybersecurity experts at home to set protections and guard our information from unauthorized access or loss, making our home networks and devices less secure. Recently, Carl Willis-Ford, Senior Solution Architect for Federal Health Systems, shared vulnerabilities and tips with NASA employees interested in improving their home cybersecurity.

Most homes have a number of Internet-connected devices, as well as the equipment furnished by your Internet service provider (ISP), including home assistants (like Amazon Echo or Google Home), streaming devices (Roku, Chromecast, or Apple TV), appliances (thermostat, refrigerator, or printer), and mobile devices (laptops, smartphones, or tablets). Each has its own cybersecurity vulnerabilities, in addition to those from your own Internet activities.

For home users, cyber criminals are most interested in using your device in a botnet attack. While you may only

see a slow device, the collective botnet can be used to overwhelm a Web site or servers with requests. Keep your equipment from participating by protecting all networked devices.

Unfortunately, there are a number of ways to be vulnerable at home: Are firewalls enabled? Do you run antivirus or anti-malware software on your computer? How many items in your home are connected to the Internet? Where do you download apps? Do you reuse passwords?

According to Willis-Ford, there are several simple steps you can take to protect your home network and devices.

- Change the default Wi-Fi router and administrative account passwords.
- Ensure that the WPA2 security protocol is enabled for Wi-Fi, requiring a password to connect.
- Enable firewalls for computers, devices, and routers. Your ISP does not need those disabled to provide service.

- Disable “remote access” on your router and complete software updates.
- Passwords lacking complexity and containing dictionary words are easy to break. Complex passwords and passphrases are stronger. You can also use a password manager.
- Use whole-disk encryption for your computer; Windows comes with BitLocker, while Apple has FileVault.
- Update your operating system and applications when prompted.
- Be a smart surfer and keep an eye out for potential traps like phishing scams (fraudulent e-mails trying to get you to send personal information or click nefarious links), fake deals, and scareware (phony pop-ups saying you are infected).

Follow these simple recommendations to step up your home cybersecurity!



NASA Administrator Jim Bridenstine made a special appearance at an Information Technology Council meeting on July 24, 2018.

Cybersecurity & Cloud Computing

By Anthony Flores, John Gordon, and Odom Ouk NASA IT Ops/Cybersecurity Pathway Interns

“Nobody understands the cloud; it’s a mystery!” —Jason Segel, Actor

Though it is ubiquitous these days, “the cloud” can still be a concept as disconcerting in its unseen nature as it is admired for its proven value. With its ever-increasing relevance over the past decade, the term now attracts reactions from reverent admiration, to eye-rolls, to cautionary tales of anonymous exploitation. Cloud computing continues to be a game-changer that can exponentially improve how enterprises operate and pave the way for future advances. However, as with any young technology, it faces a challenge in terms of its acceptance within established enterprises such as NASA—what is it, how does it work, and how secure is it really?

What is the cloud?

The National Institute of Standards and Technology (NIST) defines cloud computing as “a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.” For instance, Office 365 provides standard Microsoft Office applications that can be conveniently accessed in the cloud as software as a service (SaaS) applications, relieving NASA of much of the burden (capacity management, maintenance, etc.) of operating its own e-mail servers and other related services, thereby allowing NASA to focus on its core mission: exploration and discovery.

Why do I need to know this?

The increase in security breaches and data theft has urged business leaders to seek viable cybersecurity solutions, one of which is the increased adoption of cloud computing. The NASA Enterprise Cloud A&A Framework, coupled with the Federal Risk Authorization Management Program (FedRAMP), enables NASA to have a framework for holistically measuring effectiveness, enforcing policy, and holding vendors accountable from a security perspective. Ensuring accountability serves to build trust in cloud-provisioning strategies as enterprises, such as NASA placing increased focus on cybersecurity and moving more and more information from NASA-operated, on-premise IT infrastructure to cloud-based solutions that have consistently applied security mechanisms that are validated continuously in alignment with FedRAMP.

What does this mean for you as a NASA employee?

We are happy to inform you that NASA, like all other Federal agencies, is currently undergoing a large shift toward the use of cloud-based services. Some of the benefits offered by a cloud environment include increased agility, security, and scalability. However, agencies must still be able to identify and apply procedures to secure mission-critical cloud-based assets in alignment with agency policies and compliance considerations that accompany this cloud shift—the cloud and you have a role in this change.

What can I do to operate securely within cloud environments while at work?

- Only use cloud services that you know are approved for NASA use. If you are not sure, check first with your Center’s Cybersecurity organization.
- Do not use personal cloud accounts to store or process NASA data.
- Understand the sensitivity of your information and do not store or process information using cloud services that are not suitable for the type of information with which you are working.
- Make sure you fully understand the information provided in the cloud-based segments of FY 2019’s mandatory annual Cybersecurity training—it will help you ensure that your cloud use is safe and NASA interests are protected.

Most organizations hold a wealth of sensitive information, and the astronomical volume of data constantly in transit to the cloud inevitably creates a temptingly lucrative target for cyber criminals. The intensity of even one successful breach can have severe consequences. Data breaches are not limited to outside attackers; sensitive data can also be compromised by human error. Ultimately, we—the cloud service provider, organization, and users—all play a vital role in maintaining a secure and private cloud computing environment. Please be sure to do your part in keeping NASA’s cloud use safe!

References:

- <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf>
- <https://cloud.cio.gov/strategy/>

 Office 365



What To Expect with O365

By Emily Townsend, EUSO Communications Lead, Marshall Space Flight Center

NASA has begun migrating early adopters to Office 365. This migration is important for the agency. It is key to transforming and improving our customer experience, modernizing our IT systems, and staying up-to-date with industry. O365 provides the Agency with modern, innovative, and collaborative technology, and allows our customers increased mailbox sizes, online storage capabilities with OneDrive, and larger attendance per Skype meeting.

Initially, NASA will implement Outlook, Skype, OneNote, and OneDrive (which includes personal storage and file sync and share within NASA). In the meantime, other parts of Microsoft Office (i.e., Word, Excel, Access, and PowerPoint) will continue to function as they do today. Other O365 features, including additional collaboration capabilities, will roll out in spring 2019.

All NASA e-mail-enabled customers will receive an Office 365 account. Office 365 will be configured as an internal service and will require an approved NASA device and PIV card or Agency Smart Badge to gain access.

Refer to *What You Can Expect with NASA’s Office 365* (https://inside.nasa.gov/system/files/o365_whattoexpect_0.pdf) for more information. For FAQs, O365 training videos, and a list of Center points of contact, visit <https://inside.nasa.gov/office-365>. And stay tuned for additional communication from the End User Services Program Office and from your Center!



Don't Let Data Slip Through Your Fingers

By Jeff Sinnamon, OCIO Information Technology Security Specialist, NASA Headquarters

NASA users generate, process, and store data every day. It is an important part of everyone's job to make sure that these data are available to support NASA's missions while at the same time ensuring that the data are secured appropriately. When creating, processing, storing, or transmitting any data, it is every user's responsibility to ensure that the data are handled in accordance with applicable laws and Agency policies and on a system approved for the data.

Doing so can be a significant challenge, especially considering the wide variety of data types here at NASA. Sensitive But Unclassified (SBU), Personally Identifiable Information (PII), Proprietary, Procurement Sensitive, Export Controlled, International Traffic in Arms Regulations (ITAR), and other labels can appear to be overwhelming to even the most experienced of users.

The desire to keep a task on schedule and meet deadlines can be a powerful enticement to use whatever tool or system is easiest to get the job done. Common questions that are raised include the following: What harm can really come from using any common commercial service or tool to store or transmit data? Do I really have to encrypt that e-mail when not everyone who needs this presentation has an encryption certificate? It's easier to just copy

these data off onto a USB stick so I can take it to the contractor's office; there's no problem with that, right?

Unfortunately, just one shortcut in handling data can do significant harm to your computer, your colleagues' computers, NASA, and even the entire Federal Government. It just takes one time.

The use of unauthorized services or tools to handle NASA data not only increases the risk to Agency missions in the event of disclosure, but it can also result in significant financial penalties to the Agency if the data were proprietary or procurement-related. The disclosure of data can also result in penalties at the individual level. As an example, mishandling of data governed by the ITAR can result in a maximum penalty of a \$1,000,000.00 fine and 20 years' imprisonment (22 U.S. Code section 2778).

The good news is that there are approved services and tools available to help you do your job and stay within the bounds of the law and policy. The first step is to know what types of data you are working with and make sure that the data are appropriately labeled. Your program manager or data owner can help you with any questions you may have in this area and direct you to the appropriate training or policy documents.

The next step is to identify what you need to do with the data. Are other NASA employees the only ones who need to see the data? What about contractors or university partners? Are any of them foreign nationals? Do you need to just send data out, or do you need to collaborate? The answers to these questions will help you identify what your use cases are, which will drive what service or tools will help you meet your needs.

Finally, you need to identify services and tools that can address your use cases. At NASA, the best resource is the team led by your Center Information Security Officer (CISO). <https://inside.nasa.gov/ocio/content/nasa-center-chief-information-security-officers-cisos-and-assessment-and-authorization> They can direct you to the tools and services that are approved for the types of data you are using. They also have access to the Risk Information Security Compliance System (RISCS), which has the latest information on what tools and services are approved.

The data that we collect, create, and share at NASA are valuable and can lead to amazing things. The information deserves to be protected accordingly. Please take some time during this Cybersecurity Awareness Month of October to review your data types and use cases, as well as the tools and services you are using.

SECURITY TIPS

By Meredith Isaacs, Communications Specialist, NASA Headquarters

When protecting NASA's networks and data, understanding who and what are accessing and attaching to Agency networks is paramount. With this information, cybersecurity personnel can assess risk, mitigate threats, and protect NASA and its people from malicious actors. The Department of Homeland Security (DHS) expects the frequency of cyberattacks on all networks to increase. From amateurs to professionals, malicious actors look for connections to Agency networks to disrupt, steal, or sabotage. We must be careful of who and what we allow to connect to our networks, avoiding those with bad intentions and preventing unauthorized access due to innocent mistakes.

Many vulnerabilities result from the actions of those unaware that they have introduced risk to our networks. By attaching an unauthorized device to an Agency computer or network (like a personal phone or USB drive) or downloading unauthorized software, users have unknowingly introduced greater risk to the computer, network, and our data. Today, we are also surrounded by Internet of Things (IoT) devices (found in cars, in accessories on our bodies, in appliances, etc.), which can make completing tasks easier while also risking compromise or use against us. By ensuring that only authorized devices and software, which have completed NASA's evalu-

ation and authorization process, are connected, the Agency reduces the risk of data loss.

NASA also has many associates involved our work, from civil servants and contractors, to university and industry cooperatives, to international partnerships. Through appropriate vetting and credentialing, we verify that those with access should have access.

NASA takes very seriously any threat against our devices, networks, data, and people. To protect the Agency, we partner with DHS and other Federal institutions to secure our networks, assess threats, and mitigate intrusions. Efforts include operating under a risk management framework, monitoring networks, employing firewalls, vetting and credentialing users attached to the network, maintaining 24/7 cybersecurity operations, and conducting user outreach and education.

But there are always opportunities for all of us to help protect NASA. Do not download unapproved software, attach unauthorized personal devices to NASA's networks and computers, use unauthorized cloud services, or let others have access to your Agency devices.

Remember, cybersecurity begins and ends with you!

NASA's IT Strategic Plan— Cybersecurity

*By Jonathan Walsh, IT Strategic Planner,
and Meredith Isaacs, Communications
Specialist, NASA Headquarters*

The global cybersecurity landscape is ever-changing. Malicious actors continually strive to find new ways to threaten companies, Government institutions, and private individuals in a quest to steal data and disrupt operations. Therefore, it is of national interest for NASA to maintain the confidentiality and integrity of its data and information systems while also making its data and systems available for mission success.

To ensure the confidentiality, integrity, and availability of its data and systems, NASA identified Cybersecurity as an Information Technology (IT) Strategic Goal for Fiscal Years 2018–2021. Efforts to safeguard NASA's data and IT assets include strengthening the Agency's cybersecurity capabilities, deploying new processes and tools to support risk-based decision making, and using an innovative employee education program to cover a wide variety of cybersecurity topics.

In accordance with this goal, NASA has adopted the National Institute of Standards and Technology (NIST) cybersecurity framework to identify, protect, detect, respond, and recover from threats, risk, and incidents. The Agency is actively implementing the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) tools to modernize NASA's threat detection and response capabilities. Educational opportunities encompass improved cybersecurity training for all personnel, periodic anti-phishing exercises, and role-based training, among others.

As NASA better safeguards its data and IT assets, we can expect to see continued improvement in the Agency's cybersecurity posture resulting from changes such as mobile device management, hardware and software asset management, reduced duplication of cybersecurity tools, updated data classification protocols, and an increase in educational opportunities featuring the latest training methods.

By supporting the achievement of NASA's Cybersecurity goal and objectives, we will help the Agency to securely unleash the power of data.

To view NASA's IT Strategic Plan for Fiscal Years 2018–2021, visit <https://www.nasa.gov/ocio/itsp>.

Questions about NASA's IT Strategic Plan?
E-mail agency-itsp@mail.nasa.gov.

A Look at Goddard's Secure Lab Enclave

Jeff Simpson, IT Manager and Directorate IT Security Engineer, Goddard Space Flight Center

The Secure Lab Enclave (SLE) is a Center-wide solution at Goddard Space Flight Center (GSFC) designed and developed as a joint effort between the Sciences and Exploration Directorate (Code 600) and the Information Technology and Communications Directorate (Code 700) to provide a networked environment that independent Center science and engineering labs can operate as needed to support their local operational requirements. The goal is to maximize the security provided to these labs while managing the operational impact to one-of-a-kind and legacy systems. The SLE environment provides a means to protect these lab computers and instrumentation from hostile network and Internet activity through the use of GSFC-managed and multilayered security controls like firewalls, two-factor authentication, and Continuous Diagnostics and Mitigation (CDM) tools and security standards applied to lab equipment where applicable, while allowing completion of mission lab tasks.

The need for the SLE became apparent after realizing there were many labs GSFC supports across multiple

directorates that were isolated from other NASA networks and thus caused inefficiencies to lab owners when they needed to transfer data. These labs develop and test instrumentation that is core and critical to NASA's scientific research and space flight missions. They also have traditionally operated completely isolated from any external networks. While this practice is largely secure, it often imposes inefficiencies or even significant burdens on the lab owners and staff to transfer electronic data between the lab systems and other NASA systems for further analysis, processing, or dissemination. The isolation of the labs also significantly impeded the ability to implement effective security controls and to remotely monitor or control lab equipment during long-duration tests. The SLE provides a secure means to improve efficiencies with these lab operational requirements.

Candidate labs for this SLE are those with computers or other IT equipment used to control/interface with other delicate hardware instruments such as preflight development equipment, in-flight clones, or postflight instruments, as well as spectrometers and

other tools used for scientific research and mission operations. Some or all of these systems may involve computers whose configurations are "locked in" and static due to their tested hardware interfaces and require special care to protect while allowing the mission goals to be fulfilled.

Several labs are operational in the Secure Lab Enclave as pilot projects. These include the Code 600 Laser Lab, otherwise known as Goddard Laser for Absolute Measurement of Radiance (GLAMR); the Code 600 Direct Readout Lab (DRL) for live satellite data through the SLE; the Code 500 Space Test Complex (STC); and the Code 400 RESTORE-L (mission project in development). Additional lab requirements are being evaluated for the pilot program, and the SLE is expecting an Operational Readiness Review (ORR) and production status to be ready during the fourth quarter of calendar year 2018.

Additional information on the Secure Lab Enclave solution is available from Jeffrey Simpson at jeffrey.m.simpson@nasa.gov (Goddard Code 730).



Members of Goddard's SLE Team (from L to R): Mike Nestor, Jeff Simpson, Tony Taylor, and Matt Matthews. Not pictured: Roger Banting, Greg Goucher, Adrian Misiak, Marilyn Nhan, Dan Corso, and Nima Sheybani-Agdam.

Cybersecurity & You: A Day in the Life

AT HOME

“ When teleworking, use your NASA-approved device and VPN. ”



“ Enable the WPA-2 security protocol and firewall on your Wi-Fi router, protecting the network and devices. ”



“ Don't leave Agency devices or sensitive information in view. ”



AT WORK

Keep your smartcard with you.



Lock your computer when away from your desk.



“ Secure data, information, and equipment at your workstation. ”



ON TRAVEL

“ When traveling, regularly account for Agency devices. ”



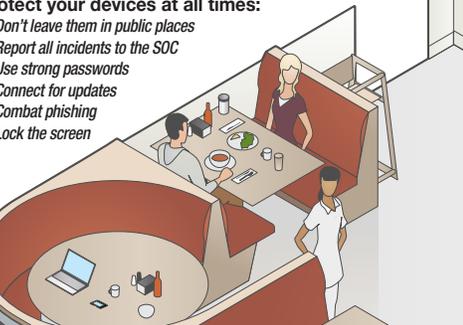
“ Lock NASA devices & info in your trunk while in transit. ”



IN PUBLIC

Protect your devices at all times:

- Don't leave them in public places
- Report all incidents to the SOC
- Use strong passwords
- Connect for updates
- Combat phishing
- Lock the screen



“ When leaving for the day, stow your badge. ”

Remember, Cybersecurity Begins & Ends with YOU!



Johnson Space Center Wins the Hitachi Transformation Award

By Thomas Kromis, JSC Information Resources Directorate Communications Lead, Johnson Space Center

The Hitachi Enterprise Transformation Category Winner for the Transformation Award is the Information Resources Directorate (IRD) at Johnson Space Center (JSC). This award recognizes the partnership between the International Space Station (ISS) and IRD in the development of a new system to meet the growing imagery needs for the ISS. It also recognizes companies that use Hitachi solutions to accelerate their business transformation in innovative and successful ways with the goal of inspiring business and IT leaders in all industries. The IRD Director, Annette Moore, formally accepted the award and spoke at the Hitachi NEXT event in San Diego in 2018. This was a premier event for the digital revolution for business leaders who embrace the digital economy and base decisions on data to ensure success.

In 2013, IRD identified future problems with the process, design, and accessibility of data for IRD customers. IRD created three key focus areas:

customer needs, agency priorities for meeting mission goals, and both enhancing and exploring new technologies such as cloud technology. This was a journey of several years of researching new technology with multiple vendors. Moore states that “demands have changed: volume, quality, density and provide flexibility” and that IRD “needed a system that could adapt to our growing and expanding requirements.” This effort produced innovative ways to archive data and to secure and separate data while engaging with IRD customers to better understand and capture their requirements.

Moore commented that what was important was that we joined in a partnership that “grows with us” and “brings new ideas, strategies and technologies—even ones not originally considered.” After diligent consideration and a Decision Analysis Review, IRD recognized that Hitachi could, not only, meet the current mission needs

of today but also provide a solution with potential for the future.

The technology and approach to archiving data through the Hitachi solution allow IRD to meet evolving stakeholder needs and support the mission, now and in the future, while also reducing costs for both the Government and the customer. Leveraging cloud technology satisfies the needs of IRD customers while also providing a hybrid approach to storing data. This practice allows IRD customers to benefit from the exploration of innovative technologies to improve the process, design, and accessibility of data for their customers.

Historical imagery and records are necessary to support research as NASA looks to develop the next generation of space operations. The IRD Storage Operations Manager, Heather Thomas, agreed “Hitachi allows us to grow with our customers.”



Kirk Shireman, ISS Program Manager and Annette Moore, IRD Director and JSC Chief Information Officer cut the ribbon at the Hitachi Content Platform Ribbon Cutting November 6, 2017 (photographer: Robert Markowitz - NASA - Johnson Space Center)

Federal Information Technology Acquisition Reform Act (FITARA): WHAT IS IT?

In December 2014, a new Federal law was enacted by Congress called FITARA. This new law enhanced the Chief Information Officer's (CIO's) authority and accountability in reviewing and approving all IT requirements before a contract action.

In order to comply with this new law, the CIO's office has been working very closely with both the Office of Procurement (OP) and the Chief Financial Officer's (CFO's) Office to establish new policies and processes to ensure compliance. All three offices have a significant role in implementing this new mandate.

In summary, the CIO is required to review and approve acquisition strategies and acquisition plans that contain IT. If there is no acquisition strategy or acquisition plan, the CIO shall review and approve the action itself.

The OP shall ensure that the Agency shall initiate no contract actions or interagency agreements that include IT unless they are reviewed and approved by the CIO or are consistent with the acquisition

strategy and acquisition plan previously approved by the CIO.

The CFO is to partner with the CIO in managing IT as a strategic resource across the Agency by working with Mission Directorates and Centers to utilize IT data to drive decision making, reduce duplication and inefficiencies, and optimize IT management.

Because this is such a large undertaking, the CIO has delegated review and approval authority to the Center CIOs to ensure that they are taking action at their Centers. Each Center CIO is expected to work closely with the OP and report monthly to the Agency CIO the requirements their office has reviewed and approved.

In order to know what to report, employees need to understand what IT is. The Agency established a tiger team several months ago to define IT:

Information Technology (IT) is any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching,

interchange, transmission, or reception of data or information by an executive agency. It also includes computers, ancillary equipment (including imaging peripherals, input, output, storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.

...will include all commodity IT (hardware and software), ground systems, mission control centers, and data centers.

Onboard flight avionics and flight software that are a non-severable and an integral part of the flight system are not considered IT for the purpose of OMB IT budget reporting....

Defining a device/service as IT does not exclude its classification as an R&D or engineering device/service.

Everyone's hard work in trying to implement this law is greatly appreciated. We have made great strides but still have some work to do, and the Office of the CIO will need your continued support to make this happen.

JPL Data Scientist Michael Cox Honored as a 2018 Rising Star

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

The Government Innovation Awards, presented by Federal Computer Week, Government Computing News, and Washington Technology & Defense Systems, have named Michael "Mik" Cox, a Data Scientist and Internet of Things (IoT) Team Lead in the Office of the Chief Information Officer (CIO), as one of their 2018 Rising Stars. Cox becomes the Jet Propulsion Laboratory's (JPL's) fourth consecutive Rising Star honoree and the fifth since 2010.

Tasked with rapidly exploring innovative new capabilities that will enhance JPL in its mission to use the emerging technology trends, Cox, by teaming with end users and industry developers, has successfully taken many

capabilities from experiments to an operational state with excellent user benefits at an astounding rate.

He was instrumental in the creation of multiple Intelligent Digital Assistants for JPL. Some of these are one for the Acquisition Division, an IoT prototype "ShopBot" that enables approved users to swipe their JPL badge to turn on machine shop equipment, and multiple Chatbots. Cox has collaborated with several industry partners who are designing and releasing new products, services, and technologies. His input has made a positive impact on the industry partners' development, ultimately enabling several to be deemed acceptable for use by NASA and the Federal

Government (e.g., Alexa for Work). Cox also served as a lead for the immensely successful JPL Open Source Rover project, and between two AWS re:Invent conferences, Cox has delivered complex live demonstrations in two IoT State of the Union addresses.

Cox is the only NASA/Federally Funded Research and Development Center (FFRDC) representative on the 2018 list, which can be found at <https://fcw.com/articles/2018/08/23/rising-stars-2018>. The complete profiles for all the 2018 Rising Stars will be available this fall. Cox and his fellow honorees will be officially recognized at the November 8 Government Innovation Awards Dinner in Tysons Corner, VA.

IT Expo at NASA Headquarters

By Scott Johnson, IT Communications Lead, NASA Headquarters

NASA Headquarters' Information Technology and Communications Division (ITCD) hosted "A Day with ITCD," its annual IT Expo, recently. The event provided an interactive forum to build awareness of IT products and services available at NASA Headquarters to support mission success. Attendees were able to visit exhibits and receive details on an array of IT topics, such as Microsoft Office 365, the software library, records and forms management, IT security, and Google G-Suite software.

The purpose of the expo was not only to inform, but to also provide attendees with solutions to IT challenges and requirements. On-the-spot consultations were made available so attendees could receive instant resolution to issues or questions and, if necessary, receive followup by ITCD after the event. Topics included SATERN registration; Identity, Credential, and Access Management (ICAM); NASA Operational Messaging and Directory (NOMAD); the service catalog; information security; training; 508 compliance/user accessibility; business intel-

ligence; document management; the managed cloud environment; mobile application development; SharePoint; surveys; and Web applications.

It is my belief that you can't win over today's business customers with yesterday's fragmented IT delivery methods. As a result, the HQ IT Expo is an element of my strategy to meet business where IT can provide the most benefit.

—**Victor Thompson, NASA Headquarters Chief Information Officer & Director, ITCD**

Live demonstrations were provided to showcase products and services, including multimedia, video development, ACES software downloads, backups, mobile device management (MDM), smart conference rooms, mobility solutions, teleconferencing tools (Skype, WebEx, and Adobe), and telework tools. Visitors were able to see new technologies in use, such as an interactive expo map on a large touch screen. The Headquarters

survey service was demonstrated in real time as participants took a brief exit survey on iPads. "Trending topics" were also highlights, including NASA digital communications, machine learning, automated document tagging, and Internet of Things network analysis. Augmented and virtual reality were demonstrated, along with virtual goggles—a big hit with attendees.

Visitors were also engaged through games such as Wheel of Fortune, a "Who am I?" game for getting to know the ITCD team, and raffles. Mini workshops were held on topics such as Enterprise License Management Team (ELMT) ordering, postmaster and NASA Enterprise Directory (NED) self-service options, the service catalog, and Contracts IT Security 101.

The event was a success in large part due to the collaboration between Headquarters ITCD, its contractor partners, and vendors. It was a learning experience for both attendees and presenters as information was exchanged, challenges were discussed, and solutions were presented.



Live demonstrations of augmented reality (AR) and virtual reality (VR) were just some of the showcased items at the Headquarters IT Expo.



Attendees try out conference room technology at the Headquarters IT Expo.

BSA Corner

By Meredith Isaacs, Communications Specialist, NASA Headquarters

As we enter the final quarter of 2018, we look back over the course of NASA's IT Business Services Assessment (BSA) and the progress made by IT organizations, services, and personnel. The Business Services Steering Committee designed the BSA to find ways to optimize mission support services, including IT.

With approval from the Mission Support Council, the Office of the Chief Information Officer began implementing seven Decision Areas (Roles and Responsibilities, Governance, Computing Services, Communications, Workstations, Collaboration, and IT Security) in early 2016. At the time, IT was characterized by decentralized collaboration, end user, and cybersecurity services, which increased costs and inefficiencies; limited CIO oversight and insight; and too many data centers and unrealized potential for cloud usage.

Over the course of implementation, IT established the IT Capital Investment Review and Center Functional Review for greater investment and compliance insight; adopted a cybersecurity risk framework for heightened network and data protection; supported communications, cybersecurity, and end user enterprise service migration; closed 55 data centers and adopted a Cloud First strategy; and established six IT service programs to manage and deliver enterprise services for our customers.

We are proud of all of the work done in finding efficiencies, reducing duplication, and optimizing IT. We are also excited about what is still to come, including Office 365 deployment this fall, additional contract consolidation and strategic sourcing for cost-effective services, and modernized IT delivering critical IT services efficiently and securely.

Over time, one journey leads to the next. As the IT BSA trails off, on the horizon is an opportunity for greater efficiencies, savings, and support for our people. We look forward to the next turn in IT transformation!

For information about the IT BSA, visit <https://inside.nasa.gov/ocio/bsa>.



JPL Open Source Rover: Global Release and a 2018 Government Innovation Award Winner

By Tom Soderstrom, Mik Cox, and Eric Junkins, Office of the Chief Information Officer, Jet Propulsion Laboratory, California Institute of Technology

The JPL Open Source Rover was released on July 31, 2018. From its simple beginning as an idea at a JPL Pitch Day event, it was initially built by JPL interns with advice from experienced JPLers. Targeted to high schoolers and robotics clubs, the Open Source Rover platform has a parts list of \$2,500 and incorporates several IT concepts, including inexpensive commercial off-the-shelf parts and Internet of Things devices, 3D printing, a modular and expandable software and hardware stack, and of course open sourcing and crowdsourcing.

We chose to release this project in a low-cost, modern way, fitting the ethos of open source and hobbyists. A welcoming Web page introduces the concept (<https://opensource rover.jpl.nasa.gov>) and links directly to the build instructions on GitHub and a forum Web site for community discussion. There have already been productive discussions, and we expect many more, along with additions and modifications to the rover. The team finds these discussions to be truly rewarding and a wonderful opportunity to engage with the global citizenry. It is an example of how JPL and NASA care about the next generation and new ways of working.

The rover was built to be extended. We hope that people will incorporate components like solar panels, accelerometers, science payloads, and advanced programming with Internet of Things and artificial intelligence (AI) and that they will share their results, enabling others to learn from their work. The software stack for the rover is built on a Raspberry Pi and common motor controllers. This combination allows builders to easily add their own improvements with minimal

previous coding knowledge. In addition, for individuals who wish to add hardware components like a robotic arm, we included additional mounting holes and extra power on the rover to support new experiments. Three California high schools have already included it in their fall 2018 curriculum. We plan to use it ourselves as a platform to build and test advanced concepts in AI, sensors, and robotics automation.

There is a tremendous demand for NASA and robotics from the public, and many articles have been written praising JPL and NASA for the Open Source Rover project and its release to the general public. It already has over 4,000 stars on GitHub, and over 90,000 people from around the globe have visited the Web site.

To view a video of the rover conquering a rock pile constructed by Cub Scouts to “stump the rover” at a Cub Scout event, please visit <https://drive.google.com/open?id=178wY9DKKWUC0pjoxl9LDq2l4lx84RfjL>.



The JPL Open Source Rover was recently selected as the 2018 winner in the Government Innovation awards put on by 1105 Media publications. This is the first time JPL has won this award. See <https://governmentinnovationawards.com/>.

OCIO Awards

Congratulations to the NASA Office of the Chief Information Officer (OCIO) Team for winning the RSA Excellence Archer Award! NASA utilizes RSA Archer for IT and security risk management using the RSA Archer Assessment and Authorization (A&A) use case. NASA has standardized and coordinated their entire A&A process using RSA Archer, allowing the leadership tier to see all security plans and make sound risk-based decisions via an automated process. The project has also allowed NASA to work closely with the Department of Homeland Security to improve reporting for the Federal Information Security Management Act (FISMA).

And huge applause also goes to NASA's Web and Managed Cloud Services Office for winning the Box Orchestration award at the Box Works 18 Summit. The award recognizes customers that have leveraged Box to make the biggest impact on internal processes and tools to boost collaboration and content management through cloud platforms. The Web and Managed Cloud Services Office is the first Federal customer to successfully implement a FISMA Moderate environment that meets International Traffic in Arms Regulations (ITAR).

This month, two teams from the OCIO are being recognized during the Agency Honor Awards ceremony. Both are receiving the prestigious Group Achievement Award, honoring outstanding group accomplishment that has contributed substantially to NASA's mission. Congratulations to both of these teams, and thank you for securely unleashing the power of data.

The first team receiving the award is the Extravehicular Activity (EVA) Enterprise Data Integration Team, for their work resolving the EVA suit data silos discovered after an incident during a spacewalk when the suit began taking on water. The team was able to help the EVA office consolidate their data for improved safety and decision making.



IT Talk



Also receiving the Group Achievement Award is our Cyber Executive Order Tiger Team. Led by NASA's Senior Agency Information Security Officer (SAISO) and Associate CIO for Cybersecurity and Privacy, Mike Witt, the tiger team analyzed NASA's mission, corporate, and physical cybersecurity risk and identified areas of improvement under the National Institute of Standards and Technology guidelines.

National Aeronautics and Space Administration

Office of the Chief Information Officer

300 E Street, SW
Washington, DC 20546

www.nasa.gov

