National Aeronautics and Space Administration

IT Talk

October - December 2017 Volume 7 • Issue 4

Cybersecurity Awareness—

Think Before You Click!

IT Talk

Oct - Dec 2017 Volume 7 • 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

In this Issue

Message from the NASA CIO

Cybersecurity is a shared responsibility, and each of us has a role to play. Emerging cyber threats require the engagement of all NASA employees, NASA contractors, other Government agencies, and law enforcement.

Cybersecurity is critical to ensuring the integrity of NASA data and, ultimately, the overall NASA mission. October is NASA Cybersecurity Awareness Month. The theme is STOP | THINK | CONNECT.

REMEMBER...

STOP: Before you use the Internet, take time to understand the security risks involved and learn how to spot potential problems.

THINK: Watch for warning signs and consider how your actions online could impact you and your NASA family's safety.

CONNECT: Enjoy the Internet with greater confidence, knowing you have taken the right steps to safeguard NASA and your NASA computer.

I encourage you to remain aware of cybersecurity risks and implement effective cybersecurity practices to protect and safeguard NASA's information and assets, such as facilities, equipment, and human resources. Best practices include the following:

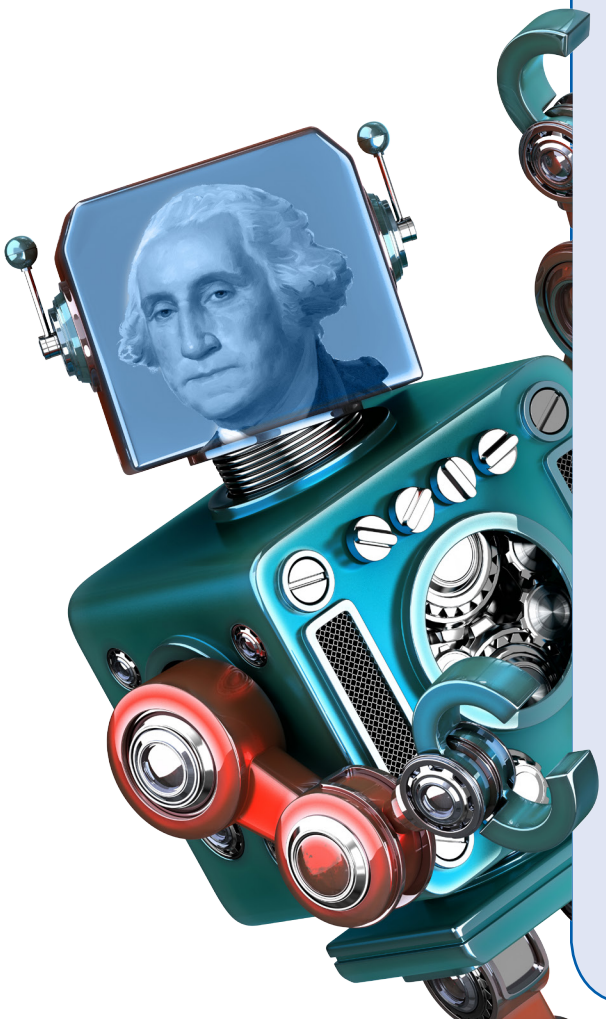
1. Setting strong passwords and not sharing them with anyone.
2. Keeping a clean machine—your operating system, browser, and other critical software can be optimized by installing regular updates.
3. Maintaining an open dialogue with your family, friends, and community about Internet safety.
4. Limiting the amount of personal information you post online and using privacy settings to avoid sharing information widely.
5. Being cautious about what you receive or read online—if it sounds too good to be true, it probably is.

Throughout the month of October, various activities will be conducted at each NASA Center to celebrate National Cybersecurity Awareness Month. In this issue, we'll take a closer look at some commonsense rules to protect yourself and your organization against cyber threats. Remember, effective cybersecurity practices begin and end with you!

~Renee

Securing Our Digital "Robotic" Workforce

By Christine Gex, Center Chief Information Security Officer, NASA Shared Services Center



This summer, the NASA Shared Services Center (NSSC) introduced a new employee to the NASA workforce. Washington Bot is a software application that operates as a virtual full-time employee with defined tasks that simulate human activities. The Bot has been granted access to Government-furnished equipment and accomplishes tasks with high speed and accuracy using Robotic Process Automation (RPA) technology.

The RPA technology, defined broadly, involves the design, creation, and configuration of a computer software robot, commonly referred to as a "bot." The purpose is to perform a predefined and repeatable computer processing action or set of actions. Bots can be created and configured to perform many different types of role-based functions, including, but not limited to, transactional processing, data manipulation, and reporting. This technology is still maturing and emerging in the areas of cognitive technologies and artificial intelligence. As the science advances, it will extend the possibilities for more automation: process monitoring, responding to or triggering responses from other computer applications or systems, and possibly other data-processing scenarios.

As with all aspects of information technology (IT), security awareness is at the forefront. IT Security was brought in during conception and is still integrated with the project. The project and security teams treated Washington Bot like any other employee and application. This security approach allowed the team to document the processes and systems for upgrade when applying them to future bots. The RPA technology security assessments were completed using National Institute of Standards and Technology (NIST) 800-53 v4, and the Office of the Chief Information Officer (OCIO) IT Security Division provided resources to perform a deep-dive assessment on one of the potential software vendors.

Some of the challenges the team faced were Personal Identity Verification (PIV) Smartcard compliance and training requirements for authentication and access to Government systems. The Identity, Credential, and Access Management (ICAM) team provided the NSSC with a temporary authentication solution, and NSSC continues to partner with the ICAM team to reach a solution for soft credentials and other NASA system integrations.

Last year, the NSSC introduced RPA and participated as a contestant at the NASA Innovative Kick Start Competition with NASA Headquarters. The NSSC's submission was selected from 100 participants, and this competition allowed the NSSC to purchase the first RPA and pilot a proof of concept.

Currently, Washington Bot is in pilot training to support processes at the NSSC Human Resources Services Division, the OCIO, the Office of the Chief Financial Officer (OCFO), and the NSSC Budget and Accounting Division. These pilot efforts will allow the NASA workforce the opportunity to refocus their efforts on analytical tasks. This capability has the potential to support the NASA workforce in new and ever-expanding ways.

NASA Welcomes Newest Class of Citizen Data Explorers

By Dr. Beth Beck, Open Innovation Manager and Information Management Program Executive, Headquarters (Photos: NASA/Michael Porterfield)

In August, NASA welcomed the fourth class of Datanauts into the data exploration ecosystem. Each class of uniquely talented individuals helps us shape our understanding of how to engage citizens in data problem-solving using NASA's treasure trove of high-value datasets. As we interact with each class, we gain valuable insight into the latest techniques and tools used by Datanauts and the communities they represent.

A recent addition to the Information Management team, the OCIO's Lori Parker assumed leadership of NASA's Datanaut initiative. She offers strategic vision on how to infuse the insights we gain from Datanauts into our Information Management technology roadmap. Veronica "Ronnie" Phillips, working with Jason Duley at NASA's Ames Research Center (ARC), coordinates Datanaut activities on a daily basis, providing project support and access to NASA data and expertise. Lori and Ronnie managed the selection process, which is designed to balance diverse skills and experiences fostering curiosity, exploration, and collaborative learning through informal mentorships and self-directed team projects.

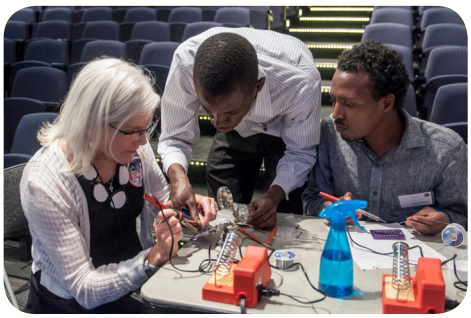
OCIO's Lori Parker welcomes new Datanauts to NASA Headquarters.

The newest class is a balance of 50 developers, storytellers, makers, game designers, hardware experts, and entrepreneurs. Ten of the 50 class members have, or are pursuing, Ph.D.'s, while many more hold master's degrees. They represent an impressive array of disciplines, including astrophysics, biomedical engineering, statistics, cognitive psychology, epidemiology, molecular biology, neuroscience, and physics. Many are leaders in their fields and founders of data/coding organizations. Quite a few participated in International Space Apps events in their communities, and one is a Space Shuttle legacy, inspired by her dad to apply. This year, our ratio of women to men is 80/20; 12 are beginner coders, 31 intermediate, and 7 advanced.

Renee Wynn addresses the 2017 Fall Datanaut Class.

In September, Lori and Ronnie designed and hosted the 2017 Fall Class kickoff activities at NASA Headquarters. Thirty-five Datanauts traveled to Washington, DC, to meet one another, learn from NASA senior leaders, and gain a better understanding of programming and opportunities available during their 6-month engagement. Datanauts came from as far away as Spain and Turkey, as well as Texas, California, and Washington State. We welcomed them with an all-star cast of speakers, including our very own CIO, Renee Wynn. Renee stressed the importance of data for providing new insights into how we see our world, as well as experimentation and collaboration to get the best results. She challenged each Datanaut to get uncomfortable and to learn from one another.

Other notable NASA speakers included astronaut Alvin Drew; Dr. Gale Allen, Chief Scientist; Kathy Nado from the Human Exploration and Operations Mission Directorate; and Dr. Brian Thomas, Agency Data Scientist. Jet Propulsion Laboratory (JPL) engineer Michelle Easter brought her MindMakers team from California to lead a hands-on workshop on binary code and circuit-building.



Dr. Beth Beck builds circuits with Datanauts Allan Anzagira and Nadew Kibret, both Ph.D. candidates.

The Datanauts initiative is an adaptive organism that changes shape with each class. Their individual and collective interests and talents influence the program elements we offer. If discussions at the kickoff are any indication, hold on to your hat. We are in for a ride!

Cybersecurity Awareness:

You Are a Target.

So Think Before You Click!

By Eldora Valentine, OCIO Communications Officer, Headquarters

These days, most of us lead Internet-connected, digital lives. From the kitchen table to the classroom, from business transactions to essential Government operations and services, cybersecurity touches all of us. October is National Cybersecurity Awareness Month. It is designed to educate, engage, and raise awareness about cybersecurity and increase the resiliency of the Nation in the event of a cyber incident. October 2017 marks the 14th Annual National Cybersecurity Awareness Month sponsored by the Department of Homeland Security (DHS). Many Federal agencies, including NASA, are partnering with DHS to promote awareness and improve understanding of the importance of cybersecurity in our everyday lives. So everyone needs to do his or her part to make sure that our online lives at home and at work are kept safe and secure.

Mike Witt, Acting Senior Agency Information Security Officer (SAISO), says, "Securing NASA's data and information technology is a responsibility all of us at the Agency share. By learning best practices, we are better equipped to protect sensitive information and the NASA IT infrastructure."

There are a lot of challenges in this information age. And sometimes technologies that help us do good things can also be used to undermine us or cause harm.

In recent years at NASA, the threats to and successful attacks on our systems have increased significantly. There are many types of intrusions—unauthorized access, denial or disruption of service, phishing, cyber espionage, malicious code (such as viruses), and the list goes on.

"Our goal is to ensure our data and NASA's entire information technology footprint remain secure, from the computer aboard the International Space Station to smartphones carried by Agency employees," says Renee Wynn, NASA Chief Information Officer.

But it does not end there. NASA continues to increase the number of employees equipped with smartcards, which provide enhanced security features to support strong identification and authorization for access to the Agency's networks and systems.

The Agency also monitors its networks 24/7 for cyber threats using automated tools and defenses, as well as a dedicated staff of cybersecurity professionals. Protecting NASA's data through better management of our IT footprint is a critical step in safeguarding the Agency.

So members of the NASA community are reminded to practice good online safety habits by doing the following:

STOP | THINK | CONNECT

STOP: Before you use the Internet, take time to understand the security risks involved and learn how to spot potential problems.

THINK: Watch for warning signs and consider how your actions online could impact you and your NASA family's safety.

CONNECT: Enjoy the Internet with greater confidence, knowing you have taken the right steps to safeguard NASA and your NASA computer.

Help keep the Web a safe place for everyone. We all need to own our online presence. If each of us does our part by invoking stronger security practices, raising community awareness, and educating employees, we will be more resistant to attacks and live in a safer digital society.

For more information and free online safety resources such as tip sheets, videos, and posters, visit: https://www.dhs.gov/stopthinkconnect-toolkit.

You can also find other helpful tips by visiting NASA's IT Security Awareness Training Center at: https://itsatc.nasa.gov/.

NASA Security Tips

By Meredith Isaacs, Communications Specialist, Headquarters

NASA's information and networks face threats from a variety of sources. Some methods bad actors use include phishing, cyber espionage, denial-of-service attacks, and the infection of systems with different types of malware. NASA's measures to combat these efforts include continuous monitoring of systems, a 24/7 Security Operations Center (SOC), phishing prevention exercises, a transition to Personal Identity Verification (PIV) Smartcards and Agency Smart Badges, annual training requirements, and communications alerts for cybersecurity events.

You can help NASA by following these simple cybersecurity rules to protect your devices, Agency networks, and NASA's information:

Software Updates

- Routinely connect your computer to your local network to get current updates and patches.
- When prompted, update your mobile device software for timely upgrades and security fixes.
- Back up your systems regularly.

Phishing Prevention

- Think before you click by verifying e-mail senders, links, and attachments.
- Set unique, long, and strong passwords for each account.
- Know the signs of phishing: urgent language, misspellings, hyperlinked text that does not match the actual URL that pops up when you mouse over the text, unknown senders, and unsolicited "official" correspondence.

Device Protection

- Protect devices from loss or theft at work, in public, and on travel.
- Do not leave your devices exposed in a parked vehicle. If necessary, temporarily lock them in the trunk.
- International travel with NASA devices requires approval from your Center's CIO office. You may be given a loaner.

Cybersecurity Information

- Complete annual Agency and Center cybersecurity training courses, as well as any others assigned to you.
- Follow all instructions if you are transitioned to the PIV Smartcard or a card reader.
- Read and comply with cybersecurity alerts sent by IT services, your Center, or the Agency.

Report all incidents and suspicious cyber activity to NASA's SOC, available 24/7: 877-627-2732 or *soc@nasa.gov*.

Remember, cybersecurity begins and ends with you!

Proactive Solutions: The Cybersecurity Threat Management Program at Goddard

By Hilary Gambale, Strategic Communications Specialist, Goddard Space Flight Center

At the Goddard Space Flight Center (GSFC), the solutions mindset can manifest itself in many ways. In cybersecurity, one of the most effective ways to provide a solution is to proactively eliminate threats that would require one. The Cybersecurity Services and Integration Division (CSID) of GSFC created the Cybersecurity Threat Management Program in November 2016 to provide awareness of imminent and long-term threats to the various information systems at NASA. Cybersecurity at NASA has evolved into a mission-critical operation, utilizing resources to protect some of the most valuable data the Federal Government owns. By allowing the GSFC mission and science environments to be aware of and take action against threats, CSID is preemptively stopping these threats and creating the solutions-oriented cybersecurity posture GSFC needs to lead the world's science development and space exploration into the 21st century.

The CSID Threat Management Program conducts extensive research, collaborating with various partners across the Federal Government to deliver up-to-date and relevant threat information. The Threat Management Program has built relationships with intelligence and counterintelligence communities, such as the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center, the Federal Bureau of Investigation (FBI) Cyber Division, and many other open-source intelligence communities, to learn and obtain information about actionable and plausible threats against GSFC information systems. This information is shared with stakeholders to ensure that they are aware of threats against their information systems. The shared information includes trending malware, detection signatures for the malware, indicators of compromise (IOC), and malicious IP addresses and domains.

In the last few months, CSID has communicated the following threat alerts to the stakeholders:

- Attempt to steal NASA data: 4
- Launch attacks against various operating systems: 1
- Encrypt system drives for extortion: 4
- Compromise system administrator credentials/invalidate antivirus software: 4

To provide effective threat management, it is not enough to simply share a laundry list of information. The Threat Management Team also provides subject matter expertise and analysis of the situation. For example, the information shared about the WanaCry malware helped the stakeholders to detect systems that can be exploited by the malware. The Threat Management Program also provided mitigation techniques that can be applied to firewalls to prevent attackers from gaining access to the exploitable systems.

In uncertain times, awareness can be the only solution. On June 27, there was a threat feed about GSFC IP address ranges that were dumped onto PASTEBIN, a Web site generally used by hackers to dump stolen information or publicize successful hacks, by a threat actor. This threat was immediately communicated to the stakeholders because the intent of the threat actor dumping the information was unknown at the time. By knowing this information, the information system owners were at a heightened sense of threat and knew the probable source of suspicious activity.

Cybersecurity threats are increasingly on the rise, and all users need to be aware of the imminent and long-term threats. From Windows, Macs, and Linux to iPhones and Android phones, there is a rise in exploitation and hacking across all types of operating systems and mobile devices, making our Threat Management Program essential to GSFC operations. The CSID's solution is to mitigate these threats before they have a chance to impact the Goddard environment. For more information about the Threat Management Program, please contact Chuck Ruehling at *charles.c.ruehling@nasa.gov*.

Glenn's External Web Presence Reaches New Heights

By Kristin Ratino, Communications Specialist, Glenn Research Center

A collaborative effort between Glenn Research Center's Office of the Chief Information Officer and Center Operations Directorate has Glenn's external, non-NASA portal websites "reaching new heights." The team was presented the opportunity to improve Glenn's digital presence and better align it with the center's strategic priorities. They addressed this by merging multiple, diversely-managed external websites with independent content strategies into a streamlined and visually engaging digital presence. Another key driver in the redesign effort was an aspiration to demonstrate Glenn's unique research capabilities while connecting with a wide-ranging audience base.

The team focused on improving search engine optimization and providing quick access to the information that is most important to the center's audiences. Spotlight images with links to current content have been added to provide greater transparency into the center's work and to respond to the growing need for access to NASA's data. The fresh and modern design of the sites also enables audiences to engage with the content through easier and more intuitive navigation. Visit the redesigned site at https://www1.grc.nasa.gov/.

Applications Program (AP)—A New Paradigm

By Kellie White, Communications Specialist, Marshall Space Flight Center

The Applications Program (AP) is one of six new Program Offices stood up by the Office of the Chief Information Officer (OCIO). The AP is not to be confused with the Agency Applications Office (AAO), although they will work closely with one another to achieve the missions of the both the AP and the AAO.

AP formulation is a result of IT Business Services Assessment (BSA) Roles and Responsibilities decisions which adjust the organization and governance of information technology service domains. The mission of the AP is simple: anticipate and align customer requirements with solutions that best meet the Agency mission through:

- Providing innovative, secure, efficient cost-effective solutions;
- Maintaining a comprehensive understanding of the Agency's application portfolio, constantly assessing for health of investments and optimization; and
- Advising and counseling customers as they develop solutions.

Led by the Program Executive, this program office oversees the projects and services in the Applications domain and is supported by the AAO, Web Services Office (WSO), and NAMIS (NASA Aircraft Management Information System).

To achieve those goals, the AP will leverage the Application Portfolio Assessment Tool (APAT). This comprehensive, accurate application inventory will assist the AP and associated governance boards in managing and optimizing the application portfolios to meet current and future business and mission needs, as well as in making IT investment decisions. Sound investment planning will ensure IT investment decisions are in compliance with functional roadmaps and technical and architectural standards.

There are several new governance boards designed to manage the AP mission. The Applications Program Board (APB) ensures that: 1) the Applications Portfolio is managed and optimized to meet current and future mission needs; 2) investments are vetted to enable sound business decisions and compliance with technical and architectural standards; and 3) delivery of quality service for all NASA Information Technology (IT) users. This board includes Center Deputy CIOs, Mission Directorate applications leads, and Application Portfolio Management Board (APMB) Chairs.

The APMBs are filled with Portfolio Owners and center representatives with a purpose to guide the portfolio management processes within their respective functional domains. The Applications Portfolio Management–Working Group (APM-WG) will draft application standards, guidelines, and templates for approval by the APB and for use by application teams. Although it may seem like many boards, the AP believes these will provide just enough application governance to maintain control and stability without slowing business down.

A joint AP and Computing Services Program (CSP) face-to-face, held at Kennedy Space Center (KSC) in June 2017, brought together key stakeholders from around the Agency to learn about their "stake" in the AP proposed governance model and the shift to a new paradigm.

To learn more about the AP or Application Portfolio Management (APM) please visit the AP SharePoint site: https://sharepoint.msfc.nasa.gov/sites/ap (Internal only).

JPL's IT Expo:

An Invitation To Innovate, Accelerate, and Collaborate with the OCIO

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

On September 12, JPL's Office of the CIO (OCIO), along with JPL IT partners and organizations, welcomed the JPL community to its 15th annual IT Expo: "Innovate. Accelerate. Collaborate." The event explored new ways to use, manage, and safeguard data to enable onsite and telecommuting (Flex-Work) employees.

With more exhibits and longer Expo hours, the OCIO developed a smartphone guide using the Guidebook app to help attendees plan their Expo experience, including a map and descriptions for over 70 exhibitors and vendors. Throughout the expo, tents displayed applications of JPL's Digital Data Strategy. Attendees engaged in conversations with team members for numerous OCIO products and services, viewed demonstrations of customized IT solutions with partner organizations, were quizzed on their cybersecurity knowledge, experienced virtual reality, and saw how IT is using innovation to bring cool and cutting-edge technologies to JPL. Students from nearby John Muir High School shared how they are infusing emerging technologies into their studies, including a video on their program, which ran on one of three 84-inch Microsoft Surface Hubs stationed at the tent's main entrance. The displays will be installed in each of the three Spacecraft Assembly Facility high bays.

JPL employees explore the IT Expo, September 12, 2017.

JPL's Open Developer Meetups Stimulate Innovation

By David Mittman, Deputy Manager, Planning and Execution Systems Section, Jet Propulsion Laboratory, California Institute of Technology

The Jet Propulsion Laboratory's software engineering community consists of over 1,400 people. With a community of that size, chances are good that someone has already considered, started, or even finished work that will benefit you. Since the introduction of our internal GitHub Enterprise collaboration service, our community has created over 6,000 shareable projects.

The Open Developer Meetup was created in August 2014 as an informal get-together to encourage the community to actively share these projects by highlighting them in short presentations. The presentation format is five to ten minutes for demonstration, followed by five minutes for questions and answers, and each Meetup takes place monthly over the lunch hour. Each Meetup attracts between 30 and 80 attendees, and presentations are recorded and made available on our internal video-sharing site, JPL Tube, where they are tagged and categorized for easy searching. Topics are solicited in a general call to our 500-member mailing list. The Meetup has resulted in increased awareness, code reuse, and collaboration between groups who previously did not interact.

The most successful talks describe a tool's major features and use cases, demonstrate one "getting started" feature and one "power" feature, and finish with links to "learning more" resources and questions. The casual and comfortable atmosphere is well suited to both new and experienced developers; presenters have ranged from interns and early-career hires with no professional presentation experience to developers with multiple decades of JPL experience.

The Meetup leadership team consists of representatives from our Engineering and Science, Information Technology, and Business Operations Directorates, who select and refine presentations and handle meeting logistics and publicity.

IT Strategic Plan Cover Contest

By Meredith Isaacs, Communications Specialist, Headquarters

This June, the Office of the Chief Information Officer (OCIO) invited all CIO office personnel across the Agency to weigh in on the upcoming NASA Information Technology Strategic Plan cover. Voters chose from one of three images, devised by OCIO leadership and hand-sketched and colored by artist Andrew Miller. The images show information technology and its essential supporting role in NASA's vision.

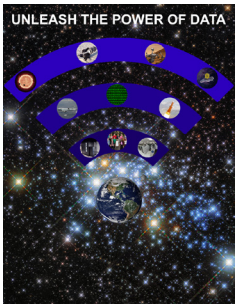
Once the votes were tallied, the "atomic" structure emerged as the winner. Some of our participants also submitted comments and even their own compositions. The final Strategic Plan cover image includes some of this feedback and further refinement from the artist.

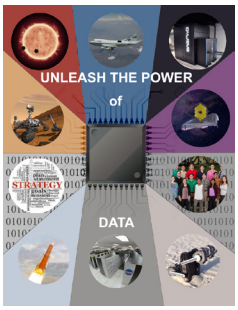
Our Cover

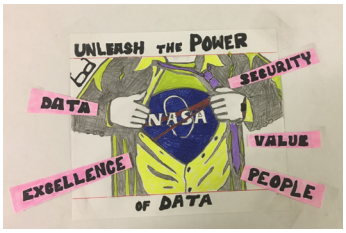
The upcoming NASA IT Strategic Plan cover represents the OCIO's vision, its strategic goals, and the role information technology plays when supporting NASA's vision. Data and information technology enable mission outcomes and support jobs across the Agency through excellence, data, cybersecurity, value, and people (our five strategic goals). This depiction of our vision also salutes the Agency's near-term goals in Mars exploration.

Our Creative Community

Mixed in with the votes, comments, and suggestions, some members of the CIO community created their own illustrations. Kudos to Kevin Samms and teammate Trudy Hill, of Kennedy Space Center (KSC), two prolific designers who sent in several compositions. In another concept, Beth Merrell of Marshall Space Flight Center (MSFC) drew creative inspiration from Superman. Thank all of YOU for your feedback, time, and artistry!







Pictured are various CIO community creations.

Office of the Chief Information Officer Honor Awards

By Meredith Isaacs, Communications Specialist, Headquarters

2017 FedScoop 50 Awards

NASA Chief Information Officer Renee Wynn has been nominated for this year's FedScoop 50 Award in Federal Leadership. This distinction honors "the federal leader helping their agency implement new technologies, strategies and IT programs to lower the cost of government while making it more innovative, agile and effective." Renee came to NASA, and the Office of the Chief Information Officer (OCIO), from the Environmental Protection Agency (EPA) in July 2015.

Dr. Beth Beck, Open Innovation Manager and Information Management Program Executive, has been nominated for the FedScoop 50 Award: Tech Champion of the Year. This honor is for "leaders whose passion for tech made us all think outside of the box." Beth joined the Agency in 1985, serving at both NASA's Johnson Space Center (JSC) and NASA Headquarters.

Winners were selected via online voting August 14 – September 29, and will be announced on November 1. To view all award categories and nominees, please visit *https://www.fedscoop.com/events/fedscoop50/2017/vote/*.

Office of the Chief Engineer (OCE) Outstanding Achievement Awards

Ian Sturken, OCIO Web and Cloud Services Program Manager, and Ahmed (Mickey) Afzal, Web Service Office (WSO) Cloud Security and Cloud Architect SME, received Outstanding Achievement Awards from Chief Engineer Ralph R. Roe for their contributions to the Agency Cloud Provisioning Initiative.

Ian and Mickey were recognized for their outstanding contributions to the successful development and implementation of the capability to provision a software tool and its associated models in the IT cloud environment, from which all NASA centers are able to access, share, and collaborate. The results confirmed the potential for significant cost savings to NASA.

This success was motivated by the Agency's Technical Capability Leadership Initiative and achieved through teamwork between the OCE and the OCIO. Ian is located at NASA's Ames Research Center (ARC) and Mickey is with NASA Headquarters.

Ahmed "Mickey" Afzal, Renee Wynn, Ian Sturken

JSC IT Security Cybersecurity Sportscast

By Jaumarro Cuffee, IRD Strategic Communications Team, Johnson Space Center

Cybersecurity is no game. But during the JSC Information Resources Directorate (IRD) Stand Down Day, JSC IT Security made sport of the National Institute of Standards and Technology (NIST) Cybersecurity Framework during IRD News Hour.

Going head to head in a "Pardon the Interruption"–style sports broadcast, JSC Chief Information Security Officer (CISO) René Smeraglia and JSC IT Security Lead John Skelton kicked off a discussion about the NIST Cybersecurity Framework that became the "method of reporting all cyber risk management activities" by presidential order, providing "agencies with a comprehensive structure for making informed, risk-based decisions and managing cybersecurity risks."

With just 80 seconds, Smeraglia and Skelton gave a blow-by-blow of the five continuous functions in this framework: Identify, Protect, Detect, Respond, and Recover.

A technical glitch stalled the animation that accompanied them, but the dynamic duo were relentless and unstoppable as they covered the details of Identify, which include asset management, business environment, governance, risk management, and risk management strategy. They pounded the court with access control, awareness and training, data security, information protection processes and procedures, maintenance, and protection technology; all parts of Protect. They drilled down into Detect details of anomalies and events, continuous security monitoring, and detection processes—and the crowd went wild. To which Smeraglia and Skelton responded with the details of Respond—response planning, communications, analysis, mitigation, and improvements. With the clock winding down, they covered recovery planning, improvements, and communications for Recovery.

In their big finish, Smeraglia and Skelton offered the audience teasers for the JSC IT Security panels in a later segment of the news, when six experts joined the JSC CISO with sobering details of Cyber Threat Identification, Vulnerabilities Management, Security Controls Assessment, Information System Security Officer through Security Management Services, Program Review, Incident Response, and Center Privacy Management.

This sportscast highlighting the five continuous functions of the NIST Cybersecurity Framework shared with the audience the game plan for NASA to continue building and maintaining a serious defense in the cyber arena.

John Skelton helps to give a play-by-play of the NIST Cybersecurity Framework. (Photo: James Blair/NASA JSC)

National Aeronautics and Space Administration

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

www.nasa.gov