

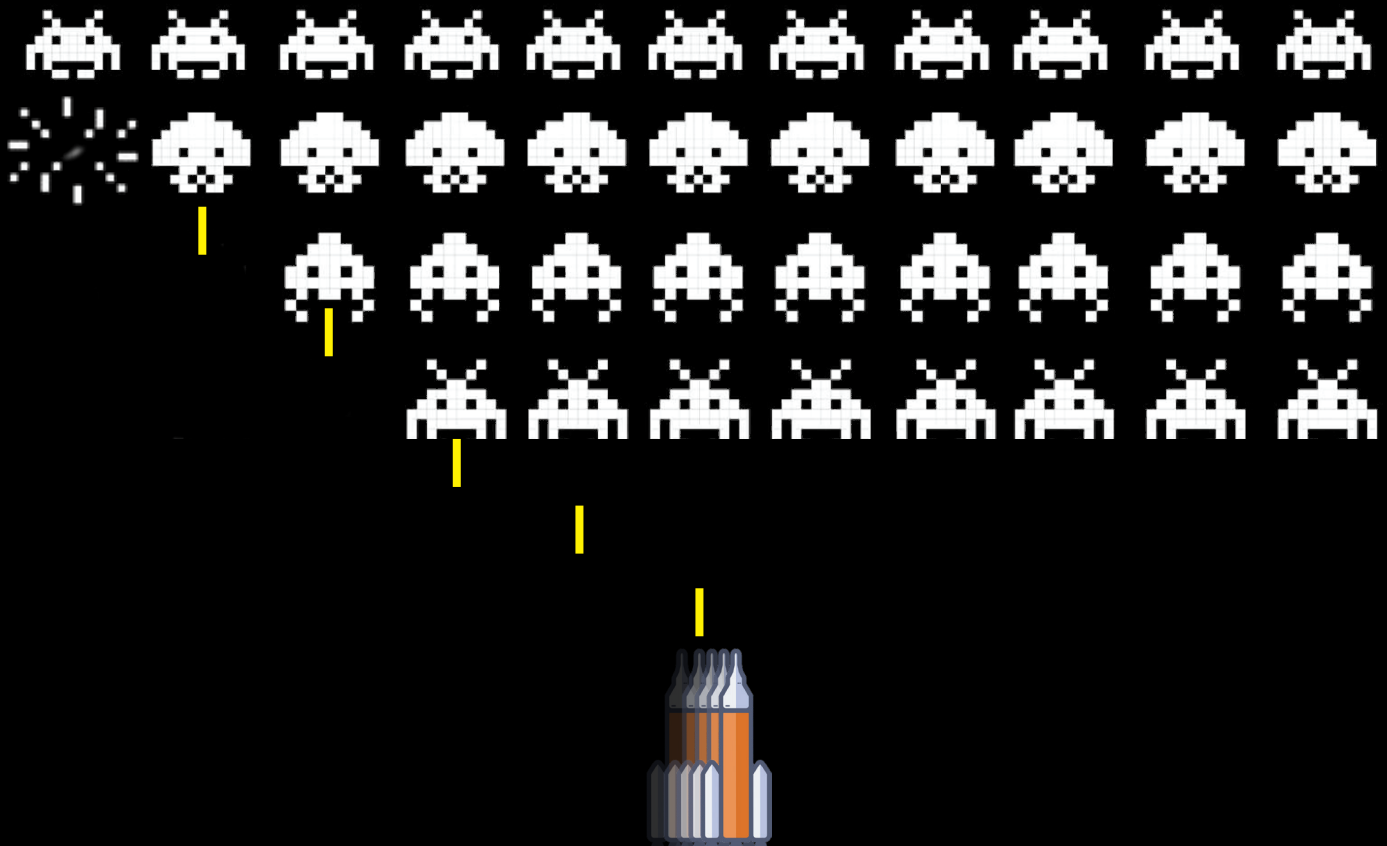


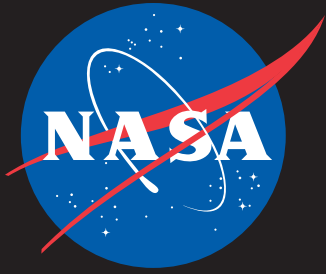
# IT Talk

October - December 2019

Volume 9 • Issue 4

# VULNERABILITY MANAGEMENT





# IT Talk

Oct - Dec 2019 Volume 9 • 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](mailto:eldora.valentine-1@nasa.gov)

To read *IT Talk* online visit:  
[www.nasa.gov/offices/ocio/ittalk](http://www.nasa.gov/offices/ocio/ittalk)

For more info on the OCIO:  
◆ [www.nasa.gov/offices/ocio](http://www.nasa.gov/offices/ocio)  
◆ [inside.nasa.gov/ocio](http://inside.nasa.gov/ocio)  
(Internal NASA network only)  
◆ [www.nasa.gov/open/](http://www.nasa.gov/open/)

 [www.facebook.com/NASAcio](https://www.facebook.com/NASAcio)



**3** Message From  
the NASA CIO

**5** CP Enhances NASA  
Cybersecurity Posture  
with NAC Solution

**6** Vulnerability  
Management

**8** Improve Your  
Cybersecurity Safety  
During Nat'l Cybersecurity  
Awareness Month

**10** A Recipe for  
Innovation

# Message from the NASA CIO

The Office of the Chief Information Officer (OCIO) continues its journey to improve our IT capabilities while better securing our networks and protecting our systems and data. Threats and attacks on our systems never stop. It's critical we safely secure our most important assets, our people, and our data.

In this issue, we'll take a closer look at vulnerabilities and key points to protect yourself and your organization against cyber threats. It's important we all stay on guard to help ensure that NASA's data and networks are safe and secure. If you educate yourself about the small things that contribute to cybersecurity, it can go a long way toward helping to protect NASA.

During October, I am encouraging everyone in the NASA community to participate in Center cybersecurity awareness activities as part of National Cybersecurity Awareness Month. I also encourage everyone to embrace these key cybersecurity best practices in their daily work:

- Protect your data and encrypt all files that contain Personally Identifiable Information (PII).
- Avoid pop-ups and unknown e-mails, and do not click on unfamiliar links.
- Use strong password protection and two-factor authentication.
- Connect to secure Wi-Fi and use Virtual Private Network (VPN) whenever you are conducting NASA business.
- Shut down, hibernate, or lock your laptop every night and whenever you take it out of the building.
- Embrace education and training.

Remember, cybersecurity begins and ends with you.



*~Renee*



*The NASA CIO Staff Meeting Face-to-Face took place at Kennedy Space Center September 16-20, 2019.*





*JPL picked up its eighth consecutive CIO 100 award at the CIO 100 Symposium and Gala in August. Pictured from left: JPL CTIO Tom Soderstrom, JPL CIO Jim Rinaldi, IT Communication Strategist Whitney Haggins.*

## **NASA's Ames Research Center Welcomes New CIO**



John Garrigues joins Ames Research Center as the Chief Information Officer. Garrigues comes to NASA from the Social Security Administration (SSA). At SSA he served dual roles as the agency's Deputy Chief Technology Officer focused on modernizing development techniques and incorporating Agile and DevOps, and the Chief Program Officer of a large software development effort that provided applications for the disability community.

Before his work in software development, Garrigues spent time in various IT Operations roles, including network operations monitoring applications and infrastructure for a nation-wide network comprised of more than 1,600 nodes. He also led efforts to decentralize SSA's data center environment by building and managing their second enterprise-class data center in Durham, NC with a third built in Urbana, MD a few years later.

His career with the SSA follows twenty-two years of service in the military. During this time he held a wide range of assignments, including Marine drill instructor, helicopter test pilot, and Information Systems Warrant Officer. John holds a Bachelor of Science in Computer Studies from the University of Maryland.

## **SSC Selects Christopher Carmichael as New Deputy Chief Information Officer**



Christopher "Chris" Carmichael has been named the new Deputy Chief Information Officer at John C. Stennis Space Center (SSC). His IT career began in hardware and software testing, where he authored several IT regulations for the State of Mississippi. Chris also spent several years in software and web development as a contractor in support of the Department of Defense. His experiences led him to join NASA in November 2009. Chris's keen knowledge of and appreciation for innovation allowed him to pioneer the SSC Innovation and Efficiencies Program (IEP) as

the Chief Technology Officer (CTO). The program is a catalyst to initiate culture change for both NASA and the resident agencies that reside within the Federal City of SSC. His out-of-the-box thinking launched this program with a focus on making collaboration more turnkey at SSC and becoming infused in the everyday lives of its employees. A product of promoting and advancing this new program is SSC's most recent collaboration space, newly named The HIVE—Highly Innovative and Versatile Environment. The HIVE provides the SSC community with a multipurpose space featuring a strong mix of technology designed to encourage employees to work creatively.

Carmichael noted, "I am excited to have this opportunity to change the environment to be more attractive to young talent and to open up lines of communication and collaboration that were not there before in order to provide SSC with the most innovative and efficient means of working."

# Communications Program Enhances NASA Cybersecurity Posture with Network Access Control Solution



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

As part of NASA's Strategy to Improve Network Security (NSINS)—a top priority for the Office of the Chief Information Officer (OCIO)—the Communications Program (CP) is leading the Network Access Control (NAC) initiative. NAC is an integrated, multiprogram activity involving nearly every program office within OCIO.

The NAC solution improves NASA's cybersecurity posture by providing a means to authenticate, assess, and validate users and endpoints, placing and connecting them to the wired and wireless network into network zones compliant with applicable security policies. As we improve the security posture of NASA's corporate networks, it is critical for us to understand who and what are authorized to access our wired and wireless network infrastructure and how they may do so.

“NAC is a dynamic approach to strengthening the cybersecurity of NASA networks. It streamlines how devices access sensitive data while avoiding disruption to mission critical services.”

—Jose Nunez-Zapata, Local Area Network Service Element Manager, CP

All NASA networks are within the scope of NAC, but transitions will be phased across the enterprise. CP “corporate” (nonmission) networks will transition first, followed by mission networks, data center networks, laboratory networks, and remote access or virtual private networks (VPNs). NAC will be implemented for these networks as part of the Department of Homeland Security's (DHS) Continuous Diagnostics and Mitigation (CDM) Dynamic and Evolving Federal Enterprise Network Defense (DEFEND) initiative.

## NAC Network Zones

NAC determines what type of device is attempting to connect to NASA data and routes the device into one of three network zones:

- Corporate Zone (Intranet/Internal): NASA-owned devices.
- Partner Zone (Specialized): Partner-owned devices processing NASA data.

- Visitor Zone (Public): Visitor, guest, or personal devices; devices in this zone cannot process NASA data.

## NAC Client Deployment to End Users

Initiated this summer and continuing through this fall, a new NAC registration client is deploying to enterprise-managed Windows computers. The client automatically configures the device to use a NASA Internal Certificate Authority (NICA) device certificate for network authentication and a new network connection profile for connecting to the NASA internal network. Once enabled at your Center, you will automatically connect to the network using a new connection profile labeled “nasa-device.”

This addition is the first in a series of new NAC capabilities deploying over the coming months.

The NAC registration client for enterprise-managed Mac and Linux devices is undergoing testing and will be deployed at a future date.

## NAC and Wireless Networks at Your Center

Wireless access options will change at your Center. A new multipurpose wireless option labeled “NASA-Connect” will be enabled at all Centers over the next several months. This new wireless option will support authentication for devices that cannot use a device certificate to connect to an authorized network (partner-owned and visitor, guest, or personal devices). Access to the wireless network will change depending on the type of device you are using:

- Enterprise-Managed: If you are using an enterprise-managed Windows device provided by NASA, you will automatically connect using the new wireless profile labeled “nasa-device.” Enterprise-managed Mac and Linux

devices will continue to connect using the “nasa” wireless option until a future date, and specific instructions will be provided to Mac and Linux users.

- Center-Managed: If you are using a Center-managed Windows, Mac, or Linux device provided by NASA as Government Furnished Equipment (GFE), you will continue to connect using the “nasa” wireless option until a future date, and specific instructions will be provided to your Center system administrators.
- Company-Issued: If you are using a device provided by your company to conduct business for NASA, you will need to be transitioned to a new “partner” network. Your Center's Communications Program Subject Matter Expert (SME) (<https://sharepoint.msfc.nasa.gov/sites/cso/contacts/Shared%20Documents/Comm%20SMEs%20by%20Center.pdf>) will facilitate this change.
- Personal Device/Guest Access: If you are using a company device for non-NASA business or a personal device, or if you have visitors needing wireless access, you will use a new NASA visitor network (once enabled at your Center). NASA guest sponsors will use the “Manage Guest User” process in NAMS and apply for an Internet Access Guest Account. NASA-badged users will register their personal (non-NASA) device through the NAC self-registration portal. To connect, users will select the new “NASA-Connect” wireless option on their device.
- Current guest and bring-your-own-device (BYOD) wireless networks at Centers will be transitioned to the NASA visitor network and decommissioned at a future date determined by your Center.

As we implement the NAC solution and enforcement is enabled at your Centers over the coming year, look for additional communications from CP and your Center.

# Vulnerability Management

By Mike Witt, Associate CIO for Cybersecurity & Privacy and Senior Agency Information Security Officer, NASA Headquarters



## What the heck is vulnerability management?

Wikipedia defines vulnerability management as the "cyclical practice of identifying, classifying, prioritizing, remediating, and mitigating" software vulnerabilities.

CSO Online describes vulnerability management as "the process of staying on top of vulnerabilities so the fixes can be more frequent and effective."

Meanwhile, TechTarget.com outlines it as "a comprehensive approach to the development of a system of practices and processes designed to identify, analyze and address flaws in hardware or software that could serve as attack vectors."

The National Institute of Standards and Technology (NIST) Special Publication 800-40 Revision 3 has retitled vulnerability management as patch management, which states that it is "the process for identifying, acquiring, installing, and verifying patches for products and systems."

No matter what you call it or how you define it, the approach is simply to proactively find and fix potential weaknesses in your organization's cybersecurity architecture—with the goal of applying fixes, such as patching or segmenting before attackers can exploit any vulnerabilities.

## So why is it important for NASA to have a vulnerability management framework in place?

Because our operating systems, applications, operational technologies, internet of things, and network vulnerabilities represent security gaps that are being abused by attackers to manipulate our assets and data and to

steal NASA's sensitive intellectual property. Attackers are constantly looking for new vulnerabilities to exploit and taking advantage of old vulnerabilities that may have gone unpatched. This is a reminder that there are consequences to our inaction that include operational, political, financial, and reputational impacts.

One statistic that highlights how crucial vulnerability management is is that since 2017, the Senior Agency Information Security Officer's (SAISO) team has identified and worked across NASA's systems and mission environments to patch more than 2 million critical/high vulnerabilities, but we still have more to tackle. The adversary is not only getting better, they are getting much faster — last year's breach at NASA showed us that.

## Vulnerability Management Best Practices

Vulnerability management frameworks usually include minimum components; let's take a closer look at the practice.

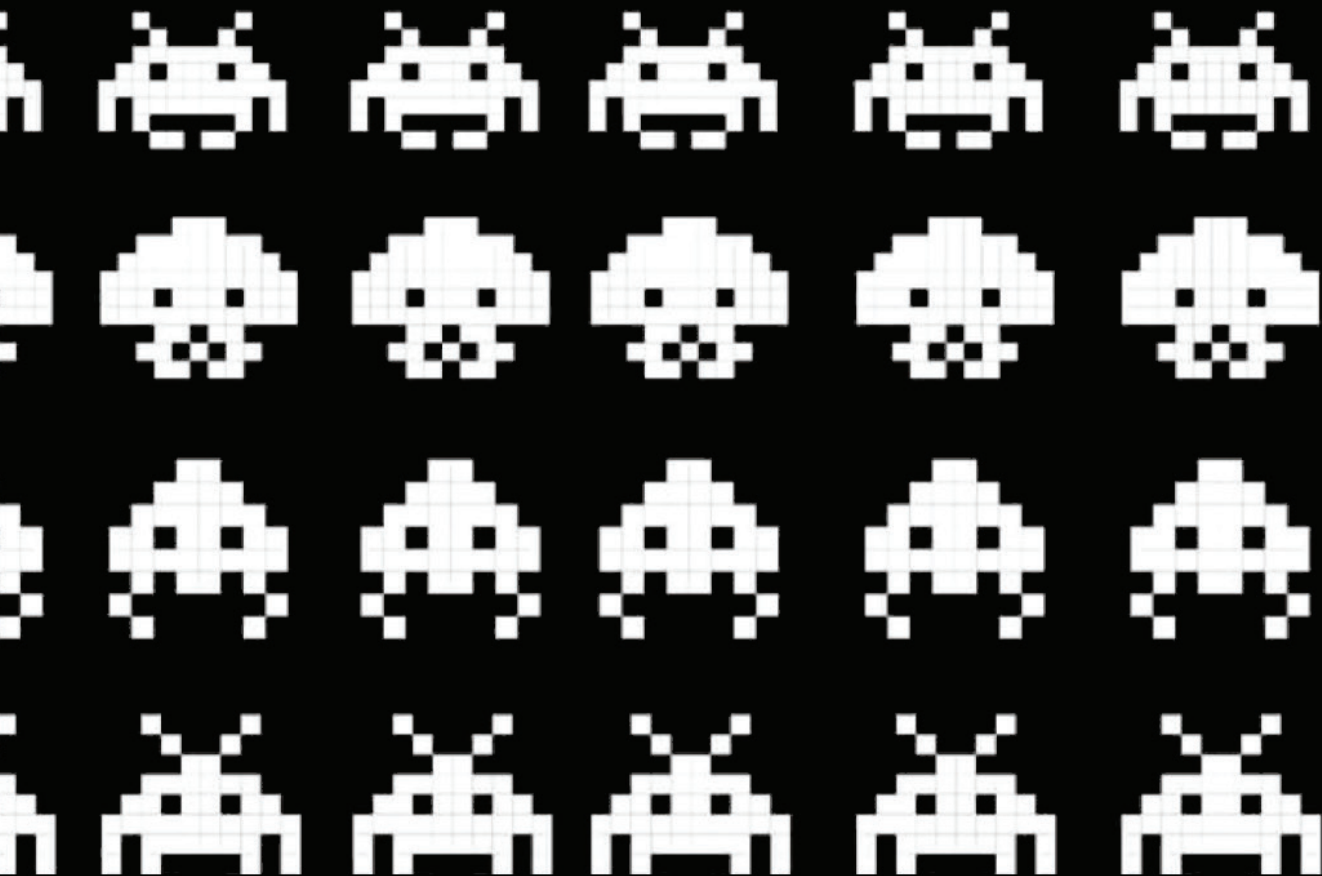
**Policy** — Our first step should include defining the desired state for device configurations. This also includes understanding the users so that we can implement least privileged access to systems and data sources across the Agency.

**Prioritize** — During remediation of a threat, activities conducted must be properly prioritized based on the threat itself, our internal security posture, and criticality of the data residing on the asset. Having a full understanding of our assets and the roles they play in NASA are critical when prioritizing active threats.


**Quarantine** — We not only have a plan in place, but actual capabilities to circumvent or shield an asset from being a bigger threat to other systems and networks within NASA once compromised.

**Mitigate** — Identify the root cause and remediate the security vulnerability.





**Maintain** — Continually monitor the environment for anomalies or changes to policy, patch for known threats, and use antivirus and malware tools to help identify new vulnerabilities.



**Inventory** — We can't mitigate what we don't know, thus we must continually monitor our inventory of assets for anomalies or changes to policy, patch for known threats, and use antivirus and malware tools to help identify new vulnerabilities. This is crucial for verifying that we have addressed all vulnerabilities in our network. This where the Department of Homeland Security's (DHS) Continuous Diagnostics and Mitigation (CDM) tools have helped NASA immensely.

So how will we check for vulnerabilities? Credentialed scans provide deeper insight than a non-credentialed scan. The scan uses credentials to log into systems and applications to provide a definitive list of vulnerabilities and misconfigurations. Because a credentialed scan looks directly at the installed operating system configuration and software, including the version numbers, it can assess items such as:

- Identifying vulnerabilities in the software
- Evaluating password policies
- Enumerating USB devices
- Checking anti-virus software configurations

**High Value Assets (HVA)** — We must know our HVAs, as some systems are more important than others. It is hard to prioritize, but we started this process well over a year ago and are getting closer and closer to identifying an all-inclusive list, which is submitted to DHS on a quarterly basis.

Finally, having a vulnerability management framework in place so that we can define and implement consistent standards, policy, identification, validation, remediation, risk acceptance, and reporting efforts enterprise-wide is crucial for preventing cybersecurity breaches. Without the framework, attackers have more of an opportunity to exploit vulnerabilities and carry out their attacks. So stay tuned as the SAISO moves forward with implementing a comprehensive vulnerability management framework here at NASA—it is long overdue.

OWN  
SECURE  
PROTECT



OCTOBER 2019

National Cybersecurity  
Awareness Month

#BeCyberSmart

## Improve Your Cybersecurity Safety During National Cybersecurity Awareness Month

By Tammy Ashraf, Software Engineer, Goddard Space Flight Center

Being aware of your personal behavior while using the Internet is essential for enjoying a safe browsing experience and avoiding cybersecurity threats. You can take the following actions both at home and at work to be proactive and personally accountable for protecting your information online:

- Keep your privacy settings up to date when using social media websites and mobile applications.
- Create strong, unique passphrases for your online accounts and enable multifactor authentication settings.
- Learn how to spot and avoid phishing scams in e-mails.
- Keep your antivirus software, operating system, and web browser up to date with the latest patches.
- Learn how to safely connect your devices on Wi-Fi networks.

These best practices are a part of October's National Cybersecurity Awareness Month theme, "Own IT, Secure IT, Protect IT."

To learn more about how you can implement cybersecurity best practices, check out these tips to stay safe online:

<https://staysafeonline.org/stay-safe-online/>

## NASA's Security Operations Center is Online

By Penny Hubbard, NASA SOC Communications, Ames Research Center

NASA's Security Operations Center (SOC) is the nerve center for the monitoring and detection of cybersecurity incidents for the Agency. The SOC is hosted at Ames Research Center and provides NASA with continuous threat monitoring, event detection, situational awareness, and incident management capabilities so the Agency maintains a sound and secure IT environment.

NASA's SOC is online with many resources including Cybersecurity tips, Cyber-threat Awareness Bulletins, links to Agency resources, and a SOC Feedback/Question feature. Check out the online resource, and bookmark it for frequent updates and information about NASA's SOC and our cybersecurity posture. <https://intranet.share.nasa.gov/agency/it/security/ops/default.aspx> (link internal to NASA)





# Cybersecurity Family Feud

By Jaumarro Cuffee, Communications Strategist, Johnson Space Center

The Information Resources Directorate (IRD) at Johnson Space Center (JSC) had several info-games at its 2019 “Employee Engagement: Connecting to the Mission” event. The 115 IRD employees and information technology partners in attendance weren’t surveyed, but based on participation, the most popular booth at the event was “Cybersecurity Family Feud.”

It is difficult to get people excited about cybersecurity. Initiatives and practices designed to keep information and infrastructure secure are often seen as cumbersome, too technical, or barriers to innovation and productivity. When users view IT security as adversarial, it increases the challenge for cybersecurity professionals to secure NASA’s data and networks to ensure their availability in support of NASA’s missions.

Although games can ignite excitement, JSC Center Cyber Risk Manager (CCRM) Christina Walthour points out that “various methods are needed to first interest, then engage users in understanding cybersecurity.” NASA provides online training, videos, posters, forums, and events to engage, educate, and remind people about cybersecurity. Professionals like Walthour and the JSC IT security team find opportunities to connect people to those resources and, when possible, introduce an element of excitement.

Another challenge in helping people understand cybersecurity is getting them to recognize the IT that needs to be kept safe. Walthour often hears that “users are focused on the ‘mission,’ and IT is secondary.” Smartphones, VoIP desk phones, desktop computers, laptops, computer tablets, network-connected printers, Wi-Fi, Mi-Fi, and similar devices we use daily (and the supporting infrastructure) are all IT. Walthour reminds people, “There is no way to communicate or send and receive information without IT,” and it “may not be the main focus of your business, but it supports your business and should be thought of in every facet of accomplishing your mission.”

Cybersecurity is not as easy as playing a game, coming up with good answers, and winning or losing. It is an ongoing challenge for everyone. IT professionals can help by setting aside industry jargon to speak in layman’s terms and demonstrate scenarios that resonate with the diverse people they support. Once that connection is made, then the importance of cybersecurity can become more of an ongoing consideration that raises awareness and vigilance. In the long run, it is up to all of us. Take it from Walthour, “you don’t have to be an IT security professional to care, understand, and practice good cybersecurity. [We] need to protect our information and teach others to do the same.”



## COMMUNICATIONS PROGRAM

CONNECT • ENABLE • TRANSFORM

## Communications Program Debuts New Logo and Quarterly Newsletter

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

With the completion of the Communications Program’s (CP) transition from the Communications Service Office (CSO) to a fully established Program office, CP is introducing a new logo.

The new logo represents the breadth of CP network capabilities across geographies and missions. Key capabilities of our solutions—connect, enable, transform—are prominently featured, and the globe from the CSO logo

has been revitalized to represent continuity.

CP is also introducing a new quarterly newsletter for the OCIO community. *Connections* highlights how CP services are connecting, enabling, and transforming NASA missions. The inaugural fall 2019 issue was published in September and is [available here](#) (link is internal to NASA employees).

Look for our winter 2019 issue later this year.

## NASA’s Information Technology Strategic Plan: Metrics Update

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

Innovation, data, and information technology are foundational to our work at NASA, enabling missions like International Space Station operations, new discoveries in our universe, air-transportation system improvements, and cutting-edge science and technology. These capabilities also support NASA’s Artemis program to return astronauts to the Moon to establish a sustainable human presence and enable missions that will take us to Mars and beyond.

NASA’s IT Strategic Plan for Fiscal Years 2018–2021 provides the Agency’s direction to manage IT as a strategic resource to securely unleash the power of data. The Agency reviews progress toward the plan quarterly, evaluates the plan annually, and updates the plan as necessary. NASA published a minor update to its IT Strategic Plan in September 2019 to add performance metrics, address feedback, and clarify alignment with NASA’s 2018 Strategic Plan. The update also highlights the Agency’s approach to optimizing NASA’s IT mission support services by moving toward an enterprise operating model.

NASA’s IT strategic goals focus on service excellence, a data-informed approach, cybersecurity, value, and supporting and preparing our people to contribute to the achievement of NASA’s mission outcomes. To find out more about NASA’s IT Strategic plan, visit <https://www.nasa.gov/ocio/itsp> or e-mail [agency-itsp@mail.nasa.gov](mailto:agency-itsp@mail.nasa.gov).

# A Recipe for Innovation

By Tom Soderstrom, IT Chief Technology and Innovation Officer, Jet Propulsion Laboratory, California Institute of Technology

We all know that innovation is a key success factor for the future. But if innovation were easy, we would already be doing it everywhere, right? We will attempt to answer a few common questions and provide one recipe for IT innovation that's working at NASA's Jet Propulsion Laboratory (JPL).

1. Which technology innovations will provide the biggest bang for the buck? Given that data will continue to grow exponentially over the next several years, technologies and skills that help collect and glean insights from the massive amounts of different data are key. These include the following:

- Internet of Things (IoT) for interacting naturally with data, such as through speech (e.g., Alexa), through touch (e.g., touch screens), and through gesture (e.g., HoloLens). We write Intelligent Digital Assistants (IDAs) to make it easy to interact with the data through these mechanisms.
- IoT for collecting massive amounts of data from inexpensive sensors that we build or buy. All the data are put into the cloud and benefit from the wireless revolution of Bluetooth 5, Wi-Fi 6, and 5G.
- Data visualization tools and skills to help us combine data and visualize it in new ways. We create new user interfaces and visualize both the data items and the speed of the workflow. These range from Data Driven Documents to Python to Splunk to Kibana to Tableau to homegrown visualization tools—but it must all be interactive.
- Analyzing the data in novel ways through analytics and data science. We have rapidly gained insight into fields as varied as cybersecurity, telemetry, engineering data, robotics, science data, and finance.
- Using all aspects of artificial intelligence to make the system better over time. Our current skills include natural language processing, machine vision, machine learn-

ing, deep learning, reinforcement learning, and more. The tools and frameworks are provided by the major cloud vendors and specialized firms, and we provide them requirements based on what we learn.

2. How can we innovate while still getting our daily work done? The key is to solve today's problems with tomorrow's technologies and skills. If they work, we double down on the tools, training, and hiring. If they didn't pay dividends, we abandon or park the project. In evaluating technologies by solving current problems, innovation becomes part of getting our daily work done and not an afterthought. The approach here is focused on problems and teams, rapid iterations, declaring "failure," and pivoting to a different solution as quickly as possible.
3. How should we organize for success? At JPL, we built an innovation lab called "The Innovation Experience Center" with the tagline of "seeing the future today." It's an open environment, an experimental trailer where people with the needed skill sets work, collaborate, and demonstrate prototypes and pilots. We partnered with cybersecurity and facilities to build a secure but open innovative environment that mimics modern startups. We then found early-career hires to help evolve this way of working, and they are working with more experienced engineers to jointly solve actual user problems as rapidly as possible. Many go on to other groups at JPL based on their passion.
4. How do we infuse innovations into the mainstream of what JPL and NASA do, and do it again and again? It's important to partner with other organizations and create a small "one pizza" team to solve each problem or "use case." The use cases come from the partners, and the solutions are jointly created in the Innovation Experience Center, drawing from the skills and tools outlined above. Part of our innovation process is to communicate the results (whether successful or not), including rapid learning, training on the tools, and skills where we saw success.

5. Finally, can we provide some examples where this has worked? This is funded by customer projects and has worked so well that the challenge is to prioritize which work to do. Here are a few of the projects:

- The Open Source Rover was a project that included all the skills and is now being built by high schoolers and hobbyists all over the world.
- The Smart Campus is a new initiative that includes prototypes of sensors and software to make and monitor smart offices/labs/buildings/clean rooms/conference rooms/traffic/commuting/parking/water usage/energy usage (the word "smart" means that it can be measured, automated, and optimized).
- Intelligent Digital Assistants have been created for all aspects of work at JPL.
- Data visualization projects include the anatomy of cybersecurity attacks, how fast tasks move through building spacecraft, where key phrases are, and how they relate from petabytes of documents.
- Analytics and Machine Learning projects include performing predictive maintenance based on machine learning of spacecraft telemetry and Deep Space Network (DSN) antennas, reducing the amount spent on devices, answering questions from petabytes of documents, such as proposals, contracts, and manuals; and using quantum computing to optimize DSN antenna usage.

This recipe's key ingredient is passion to solve current problems quickly and to not strive for perfection on day one but to make measurable progress through rapid iterations. It's proven effective, and it's fun. And why shouldn't we have fun working with deep experts in their respective fields and on the most amazing projects that will literally be out of this world?





*NASA CIO, Renee Wynn; Mission Support Future Architecture Program (MAP) Project Manager, Janet Watkins; and Deputy CIO, Jeff Seaton, kicked off the OCIO/MAP Listening Tour at SSC, the NASA Shared Services Center (NSSC), and Ames. Senior management met with the OCIO Team during All Hands and MAP Overview sessions.*





# OCIO Cybersecurity Awards

*By Eldora Valentine, Communications Manager, Office of the Chief Information Officer*

Congratulations to the Identity, Credential, and Access Management (ICAM) team. They won second place for the National Security Agency's (NSA) prestigious Frank B. Rowlett Award.

The Rowlett Award was created to recognize efforts that have significantly enhanced advancements in the field of cybersecurity. The ICAM team is a joint working group staffed by both the Office of the Chief Information Officer and the Office of Protective Services. Recently, the team was presented with a letter of acknowledgment and special Chal-

lenge Coin from U.S. Army General and National Security Agency Director Paul M. Nakasone.

In addition, special recognition goes to Senior Advisor for Cybersecurity Robert Powell and OCIO Information Technology Security Specialist Jeff Sinnamon for their work in the Enterprise Protection Program. The two received a Group Achievement Award for developing a new initiative federating NASA's efforts to achieve Agency goals for an Enterprise Protection Program.

IT Talk

National Aeronautics and Space Administration

**Office of the Chief Information Officer**

300 E Street, SW  
Washington, DC 20546

[www.nasa.gov](http://www.nasa.gov)

