National Aeronautics and Space Administration

IT Talk

April - June 2016 Volume 6 • Issue 2

Cybersecurity Concerto

IT Talk

April - June 2016 Volume 6 • Issue 2

Office of the CIO
NASA Headquarters
300 E Street, SW
Washington, D.C. 20546

Chief Information Officer
Renee Wynn

Editor and Publication Manager
Eldora Valentine

Graphic & Web Designer
Michael Porterfield

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*
- *insidenasa.nasa.gov/ocio*
  (Internal NASA network only)
- *www.nasa.gov/open/*

www.facebook.com/NASAcio

In this Issue

Message from the NASA CIO

As an IT organization, we're making significant progress. Starting April 1, 2016, we'll begin implementing the Business Services Assessment (BSA) plan. This will help us improve the delivery of IT services across the Agency. We're working on greater effectiveness and efficiencies in a dynamic operating model to meet current and future mission needs.

In the coming days and weeks, you'll hear more about the IT BSA decisions, which direct and/or reaffirm some shifts in operating models for data centers, communications, workstations, collaboration tools, and security. We all play a part in making these positive changes happen.

Transforming our IT business means the following:

- Clearly defining roles, responsibilities, and the governance structure to establish clear authorities of the Agency CIO for management and oversight of the NASA IT portfolio as required by Federal Information Technology Acquisition Reform Act (FITARA) and other policies and regulations.
- Implementing a federated/hybrid approach to data centers so we begin to utilize them as a strategic resource that better supports the missions and "greener" operating model.
- Executing a network transformation initiative to enable a seamless, integrated Agency system that provides reliable, secure, and lower-cost services that facilitate cross-Center collaborations.
- Consolidating end-user services for both workstations and collaboration tools to improve security, maximize efficiencies, and meet growing demands for mobility and work across the Agency and our external partners.
- Maintain a security posture that keeps up with the threats and supports our collaboration across NASA and with our external partners.

As we continue to improve effectiveness, shore up our IT security, and provide service excellence, we stand together across our NASA Centers and are committed to our vision: Reach for new heights, reveal the unknown for the benefit of humankind.

~Renee

NASA Deputy Chief Information Officer Named

Terry Jackson is the new NASA Deputy Chief Information Officer (DCIO). Jackson officially took over the role in March 2016. He has been a familiar face at NASA Headquarters for the past 4 years. Prior to starting his role as DCIO, Jackson served as the Associate CIO for Enterprise Services and Integration for two years. He was responsible for ensuring that NASA enterprise IT services enabled the NASA mission and were economical, secure, and integrated. His areas of responsibilities included end-user services, communications services, Web services, computing systems services, enterprise applications, information management, and Enterprise Service Desk services. Jackson first joined the NASA Office of the Chief Information Officer in 2012 as End User Services Executive and had oversight over NASA's desktop and office automation systems.

Jackson has more than 36 years of IT experience, with 26 at NASA. He joined the Agency in 1991 as the lead systems analyst at Stennis Space Center. Between 2001 and 2004, Jackson served as the Center Services Division manager and was responsible for facilities, security, medical, institutional, and logistics management; he also served as the CIO of Stennis Space Center. In 2004, while assigned at NASA Headquarters, Jackson served as a Senior Engineer in NASA's Shuttle Program Office and served as the Deputy CIO for NASA's Exploration Systems Mission Directorate. In 2005, Jackson was appointed the CIO for the NASA Shared Services Center (NSSC), where he established the IT organization and infrastructure needed to sustain NASA's financial, procurement, human resource, and enterprise IT functions supporting over 50,000 NASA employees. Beginning in 2009, Jackson served as the Deputy Director of the NSSC's Business and Administration office, where he was responsible for budget oversight, facilities management, business operations, and customer communications and satisfaction for the NSSC.

Before joining NASA, Jackson held positions in the private industry for 14 years as software systems manager for Computer Sciences Corporation and Lockheed Martin, supporting various NASA, Navy, and National Oceanic and Atmospheric Administration (NOAA) projects and operations. He also worked for Honeywell Information Systems as a database engineer.

Jackson holds a bachelor of science and master of business administration from the University of Southern Mississippi. He is a graduate of NASA's Leadership Development Program, NASA's Senior Executive Service Candidate Development Program, the Federal Executive Institute, and the Harvard Senior Executive Fellows Program.

Let the CIO Know-Know Before You Go-Go

International Access

By Penny Hubbard, Ames Outreach and Communications Specialist

Did you know that there are explicit procedural directives for taking your NASA IT devices on foreign travel and that accessing NASA services from any device abroad, even personal ones (e.g., iPhones, iPads, laptops, leased desktop computer at a coffee shop), is subject to the same restrictions and procedures? There is also a policy directive that anyone using NASA equipment (e.g., laptop or smartphone) must get written permission from the Center Chief Information Officer (CIO) before traveling abroad with them and accessing NASA services (e.g., Web mail, virtual private network [VPN], or chat). Alerting the CIO to your travel reduces reported attacks on NASA (sometimes it's hard to know if it's friend or foe accessing systems) and also notifies IT Security or the Security Operations Center not to block or suspend your access if it would otherwise appear suspicious.

The Agency has recently been the subject of especially realistic and cleverly crafted phishing e-mails, many deriving from foreign attackers. The almost daily attacks try to get end users to open an attachment or to click on a link. Often, the aim of these messages is to direct users to a very realistic copy of an Outlook or other login page, with the sole purpose of harvesting e-mail or NDC credentials. Once users fall prey to these phishing schemes, the attacker logs into their e-mail accounts using their credentials and can read and delete the users' messages, set up filters, and find other valid NASA e-mail addresses to send further phishing attempts to—only this time, the phishing comes from a genuine, and therefore trusted, NASA e-mail address.

In addition to ongoing vigilance and a healthy skepticism of unexpected e-mail messages, it is crucial, and mandatory, to follow all foreign travel business requirements (see link below). Ideally, you should not be accessing work e-mail while on personal travel; however, if your role requires you to check in during vacations abroad, make sure you alert your CIO and IT Security department that you may be accessing from a foreign country. This way, you won't appear to be a foreign attacker, and your access won't be blocked. It's a win-win for everyone to let the CIO know-know before you go-go.

NASA Policy Directive (NPD 2540.1G) International Travel:

The employee shall use only equipment officially approved for use outside the U.S. for international business meetings, conferences, symposia, etc. The employee must ensure that the hardware remains in their possession while outside the U.S. Any loss, damage, or tampering shall be reported immediately/at the earliest opportunity to the Center CIO.

Under no circumstances should Agency laptops or personal computers be used for official business on international trips unless written authorization is first obtained from the Center CIO.

Foreign Travel Information:
https://www.nssc.nasa.gov/foreigntravel

Consider a Loaner:
NASA travelers must consult with their Center CIO or CISO for NASA IT equipment options for overseas travel, such as the use of loaner laptops or phones. Use of loaner IT equipment—and loading only essential information on this equipment—significantly reduces the potential for exfiltration of information from IT devices while traveling overseas and the possible introduction of malware on IT devices brought back from overseas, which can put the NASA network at risk.

Note: Travelers are also required to comply with the Office of Protective Services, Export Control and State Department requirements for transporting equipment to international locations, and for reporting stolen or lost IT assets. Also travelers should understand that CIO approval for taking IT assets to international locations does not represent OPS or Property approval.

LEAP Cloud Days at JPL

By Tom Soderstrom, Chief Technology and Innovation Officer, and Whitney Haggins, Communications Strategist, Office of the CIO, Jet Propulsion Laboratory, California Institute of Technology

Cloud computing at the Jet Propulsion Laboratory (JPL) has come a long way since its inaugural Cloud Day nearly two IT decades (6 years) ago. At that time, we were just 2 years into the cloud-computing journey. Cloud computing has evolved from its early concept days, gaining recognition initially as a "disrupter" and now as a "critical enabler." The cloud has provided solutions to some of JPL's most complex and difficult computing challenges. Numerous highly innovative and trailblazing innovations have come from JPL cloud experts, and more are invented every day.

The JPL Office of the CIO, partnering with JPL's Missions Systems and Operations Division, kicked off 2016 by cosponsoring Learn, Experience, and Participate (LEAP) Cloud Days. It was a 3-day, multisession meetup and lecture series dedicated to cloud computing as part of JPL's LEAP Innovation series.

The event was hosted at JPL and was an advanced deep dive into cloud computing. It featured 30 presentations from specifically invited JPL and industry-leading cloud experts, including innovators from Accuweather, Amazon Web Services (AWS), Microsoft Azure, NASA, the National Institute of Standards and Technology (NIST), Netflix, Rackspace, and RedHat. Over 1,000 seats were filled as JPLers learned best practices and techniques, benefited from the insights of experts currently on the cloud's cutting edge, and participated in hands-on interactive sessions. They experienced firsthand the tangible benefits gained by applying the principles, concepts, and infrastructure technologies of the cloud. As a surprise for attendees, NASA CIO Renee Wynn, on her first visit to JPL, addressed the JPL community as part of the day's keynote address and shared her vision for cloud computing.

The outcomes from the sessions were

1. a leap forward in cloud computing understanding along with an increase in usage by missions, engineers, scientists, IT staff, and business support functions at JPL and
2. improved capabilities and understanding of JPL's goals and vision by the cloud vendor community. We strongly believe that these benefits will help JPL and NASA for years to come.

JSC has a New Deputy CIO

Donna Shaw is the new Deputy Chief Information Officer for NASA Johnson Space Center (JSC) and Deputy Director of JSC's Information Resources Directorate (IRD). Shaw began her new role on January 25, 2016.

Shaw comes to NASA from the U.S. Customs and Border Protection (CBP) agency under the Department of Homeland Security (DHS), where she has extensive background and experience as the Deputy Executive Director/ Special Program Assistant for the Cargo Systems Program Directorate and as the Deputy Executive Director for the Targeting and Analysis Program Directorate. In both roles, Shaw had responsibility for high-profile IT programs with budgets ranging from $131 million to $141 million. In keeping with her described persona—"determined, agile, purposeful"—Shaw led the transformation of IT organizations within DHS, instituting agile practices and processes to achieve program cures and modernize systems that managed international cargo importations, trade laws, regulations, policies, and procedures. The nature of her work with DHS required close collaboration with teams across DHS on behalf of over 47 partner Government agencies. Her leadership ensured the successful deployment of a transformational trade program that resulted in DHS executive-level approval and removed program breaches.

Through her work in DHS, Shaw created an IT systems environment that brought about strategic and operational changes, both internal and external to her organization. These changes resulted in significant budgetary savings as well as positive return on investment and increased collaboration between her directorate, business customers, partner Government agencies, and the international trade community.

With the increased focus on cybersecurity breaches and threats, Shaw successfully led her directorate in responding to and addressing the actions levied on her directorate as a result of the Cyber Sprint activities. During these activities, Shaw implemented a strategy that successfully addressed and resolved the areas of vulnerability exposed through the Cyber Sprint reporting.

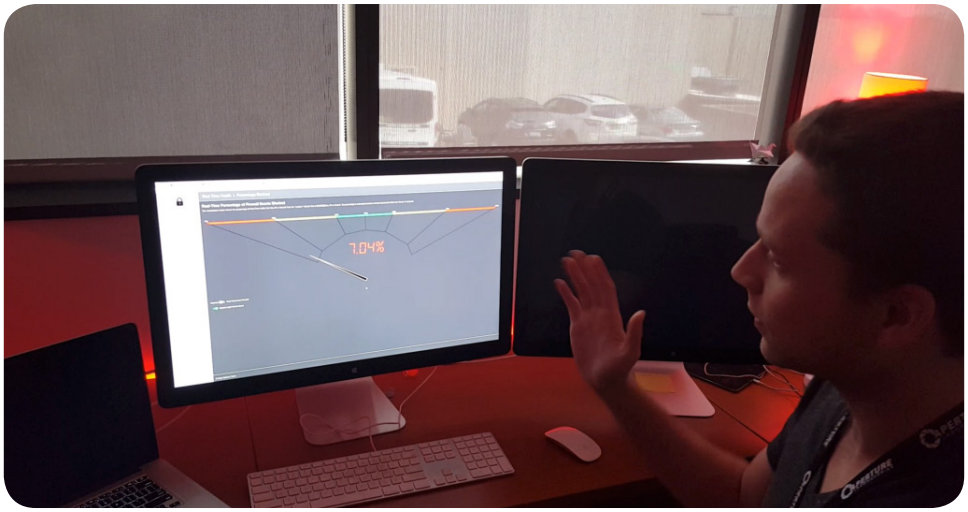
Shaw's extensive background and experience with DHS and leading IT organizations, her appreciation for the criticality of enabling the mission of her organization, and her ability to build and lead teams to achieve high results make her a welcome addition to NASA and the JSC leadership team.

In expressing her excitement about the mission of NASA and absorbing the culture, Shaw shares, "Leaving a global protection position, I don't know where I could have gone with a bigger focus than NASA—the universe."

Cybersecurity Concerto—Lighting Up Cybersecurity Awareness

By Tomas Soderstrom, Chief Technology and Innovation Officer, and Michael "Mik" Cox, IT Data Scientist, Jet Propulsion Laboratory, California Institute of Technology

The best way to get people to care about something is by eliciting an emotional reaction. When you do, they care. In one of our latest creations at the Jet Propulsion Laboratory (JPL), we are using the Internet of Things (IoT) to build a more emotional situational awareness about cybersecurity.



Why do people need to care about (or at the very least be aware of) cybersecurity? Because there are millions of attempted hacks on JPL's Web presence every day. Our job in IT is to build security awareness and show metrics without scaring the heck out of everyone. We decided that if people see our cybersecurity situation in a visual format, they will appreciate it more and apply their significant intellectual capacity to help solve the problem.

The experience we have built as a prototype to demonstrate this situational awareness is called Cybersecurity Concerto. Why Concerto? Because, during a concert, you use both sight and hearing to gain a much richer experience. As JPL's security status changes, so does the color scheme of the Concerto interface. It might go from red to yellow to green or back again. It might just blink red, which could mean "Go investigate. There may be a problem." Concerto also provides visual dashboards and metrics (such as which countries are attacking us and whether their attacks are normal or beyond normal) as well as sound. We can even turn Concerto on from an office using the Amazon Echo voice interface. That's the essence of our Cybersecurity Concerto; you can gain a much deeper situational awareness by using multiple senses.

From Immersive to Predictive Analytics

We are experimenting with using IoT lights to quickly show the state of cybersecurity at JPL. Red lights, for example, are an indicator of a serious security situation. If one such light in the CIO's office has stayed red for more than 30 seconds, our CIO picks up the phone. We've even gone so far as to add sound to Concerto, so you can literally hear the firewall being attacked in real-time, giving insight as to what activity level is normal and what activity level is elevated. If events are hitting the firewall at higher levels than normal, you can then explore deeper using dashboards. We call this kind of experience immersive analytics, and we hope it will give us insight into who is or will be attacking (and when) so that we can be predictive. The next step after this is prescriptive analytics, which means we proactively take care of cybersecurity issues before they become problems.

Another (perhaps surprising) use for IoT devices such as smart light bulbs is to connect them to social networks to monitor cybersecurity health. This can actually be particularly interesting, because occasionally other entities will know that you're being hacked before you do. As an example, when a JPL Web site was attacked a few years ago, we found out first through a social network because the hackers were bragging about their exploit before our response swung into effect. As a prototype of monitoring social networks, we tied the smart lights to Twitter so that when an unusual amount of Tweets about JPL occur, the lights change color or flash. With immersive tools like this, we're more aware of what's happening and are better positioned to react quickly if something goes awry.

Why have we taken the time to build this kind of experience? The answer is simple: Cybersecurity is clearly a business issue as much as it is an IT problem, and no IT department can protect the business completely without the business users' awareness and participation. This kind of awareness is critical, especially in an age when highly personal breaches like the one that happened at the Office of Personnel Management are likely to occur more frequently.

We got used to seeing elevated security levels at the airport but might have felt stuck as to how to respond. With Concerto, if you see something happening at JPL, you can take action. Maybe it's as simple as being more cautious about letting people tailgate through a gate. Maybe you think about not picking up the thumb drive that looks like a freebie lying on

the ground. Hacking in real life isn't what we see in the movies. Malicious individuals don't only target the multimillion-dollar security system … they target the most vulnerable link in the chain: the people using it. By giving people more awareness, we can help to solve the overall cybersecurity challenge more effectively.

Another step we are taking is hosting internal hackathons, in which we teach people how to write code that's more secure and how to share that code with each other. It's not necessarily that IT knows all the answers, but if we can improve security awareness, especially among new developers, they will start building security into everything they code. In this way, security isn't an afterthought, but instead is a driving influence on how to write code and architect applications.

The Concerto Recipe

Once people have seen or heard about Concerto, they ask how it was done. In some ways, it was incredibly easy. One of our favorite sayings here, given our focus on deploying consumer technology, is "Today's toy is tomorrow's tool." To prototype this quickly, here are the constituent parts we use:

- Lights: We use Philips Hue lights, which come with a Wi-Fi hub but do require an Ethernet connection. (We ended up building a converter using a Raspberry Pi single-board computer that converts Wi-Fi to Ethernet.)
- Voice Control: Siri and Alexa have worked well for us.
- Monitoring: We like home automation technology, in part because such systems are inexpensive and easy to experiment with and because, for the most part, they use an open platform. We are using Amazon's IoT functions to monitor the devices and the code that monitors the security alerts.
- Network: We built a device network that the devices attach to so that they are separate from the internal JPL network, and we have added security to the device network. So why build a separate device network? Internet of Things is a terrific place to experiment with situational awareness, but all the IoT devices can present security problems. We have eliminated several security problems by cutting the connection to the internal JPL network. In other words, we have air-gapped the networks, and we have code that passes messages back and forth to indicate what color the light should be. If somebody were to successfully hack the device network, they couldn't use that access to get into JPL's network.

The net result of JPL's organizational response to Concerto is that cybersecurity really matters. And that's music to our ears.

NASA Has a New Senior Advisor for Cybersecurity

Robert W. Powell is NASA's new Senior Advisor for Cybersecurity. This is a key advisory position which provides technical guidance on IT security and reports directly to the Agency's Chief Information Officer. Powell started his new role on January 24, 2016. Prior to assuming this role, he served in the position of Security Services Oversight and Planning Lead for OCIO's IT Security Division.

Powell also led the joint cyber initiative between NASA and the Department of Homeland Security, which leverages non-signature-based technologies for threat prediction and detection. Powell has a lengthy and accomplished career as a cyber professional and technology executive. Prior to joining NASA's OCIO, he led the establishment of the Department of Defense Cyber Information Assurance Range, which is a component of the President's Comprehensive National Cybersecurity Initiative. Powell has also spent time working with Silicon Valley startups focused on network virtualization and cyber-attack simulation.

Throughout Powell's career, he has demonstrated an ability to lead complex technology programs; foster collaboration amongst cyber professionals; and execute initiatives with passion, energy, and tenacity.

Powell is a summa cum laude graduate from Shenandoah University in Winchester, VA. He is a runner-up recipient of the National Security Agency's Frank B. Rowlett Award, and he holds numerous industry certifications in cybersecurity.

April 22–24, 2016, Marks the 5th Year of NASA's International Space Apps Challenge

The International Space Apps Challenge is an open innovation incubator and one of the largest hackathons in the world, hosted by NASA since 2012. Last year, Space Apps attracted nearly 14,000 registered participants, including over 1,000 virtual participants from 133 locations in 62 countries. In 2016, the growth trend continues; participation now encompasses 188 locations in 70 countries—with 35 events in the United States.

Over a 48-hour period, global participants work on challenges that are designed to support NASA's ongoing missions. This year, NASA offers challenges in six mission-related categories: Aeronautics, Earth, International Space Station, Journey to Mars, Solar System and Beyond, and Space Technology. The most popular challenges last year included designing a new space glove, building drones, and mapping clean drinking water from NASA Earth observations. Nearly 1,000 projects were developed during the 2015 Space Apps, many of them open-source solutions with immediate value to NASA and the global community.

Each Space Apps location provides local awards and can nominate two projects for Global Awards and one for People's Choice, which is determined by public vote. The Global Award–winning teams are invited to attend a NASA launch, along with their local organizers.

NASA relies on the local organizers as the rocket fuel that powers Space Apps every year. In the last two years, NASA added three new capabilities to support the local hosts and their local communities to help grow the data-innovation community beyond the hackathon weekend:

1. The Data Bootcamp, developed through NASA's Women in Data initiative, convenes newcomers at the hackathon environment on the day preceding Space Apps for a top-level introduction to coding, data science, technology platforms, and challenge development.
2. The Space Apps Project Accelerator toolkit offers local hosts a guide to set up community incubation for promising Space Apps projects. The intent is to leverage NASA data to seed innovation hubs and grow data science skills in communities around the world.
3. The Space Apps Global Collaborators are part of a new initiative for organizations to offer tools, assets, and expertise to Space Apps locations outside the local community. NASA will provide a list of curated organizations so that hosts can contact the organizations directly to negotiate support for individual events.

The best is yet to come. More information about Space Apps is available at https://2016.spaceappschallenge.org and https://open.nasa.gov/explore/space-apps.

Protecting Data from the Inside Out

By Sandeep D. Shetye, Chief Data Architect, OCIO Technology and Innovation

Given the recent data breaches across Federal agencies, it can be argued that the current methods to mitigate data loss via "leaky" networks and "lost" devices are deficient. Using the recent examples of the Office of Personnel Management (OPM) breach or several lost-laptop incidents in recent years as a guide, these losses have proven to be expensive or have resulted in irreparable damages. Often, organizations are less aware of their data throughout its life cycle than they could be, increasing the potential of deficient protective measures and limiting the capability to assess loss impacts or take appropriate actions in a timely manner.

A Need for Innovation

Considerable efforts have been put into protecting network perimeters to halt incoming malicious activities from nefarious actors, educating the workforce on the dangers of social engineering, and protecting physical hardware and infrastructure access, all with the intent of preventing data loss. While these are without question very important, there are areas where an organization can improve its defenses against data losses by improving awareness through mechanisms that are transparent to "data creators," "data consumers," and "data curators."

Just as devices on a network should be identifiable and have a known relevant role, so should be the data within an organization. As the saying goes, it is difficult to identify risks and take action if you don't know what you are protecting and where it is located. Tagging data is a very important first step in building organizational "data awareness" through existing network appliance capabilities. Centralized data management makes the concept of full awareness more palatable as it is easy to view data, take inventory, and control data access, etc.—but once data leave the centralized location, keeping track of them becomes much more difficult. Providing awareness of application layer data by monitoring the creation, dissemination, and consumption by individuals or departments within an agency through means of tagging, cataloging, and monitoring with "event" signaling can provide significant value, adding one more "cog" in the overall defensive strategy for an organization's data management.

Redirecting Existing Technologies "Inwardly"

Borrowing from the network threat detection and malware industry, we can repurpose and reconfigure concepts and techniques to track data and metadata throughout its life cycle within an organization in the hope of bringing an improved risk analysis and rule-based event signaling to an external actor. Items that are of interest are as follows: what person or service is sending data to whom, what the content of those data might be—up to some level of certainty, and if any protective or evasive action should be taken on a stream/flow of data currently at the network level.

Although this approach does not provide immunity to cyberattacks, insider threats, and data breaches, by focusing on internal and outward data flows, it can provide data security intelligence and data protection.

EVA Office Recognition of Excellence Award

Congratulations to the Extravehicular Activity (EVA) Data Integration Project Team! The group was recognized by the EVA Office for the "Go-Life" effort to enhance real-time mission decision making to improve astronaut safety during EVAs. The EVA Office Recognition of Excellence Award, including an EVA patch that was flown aboard the Space Shuttle Endeavour on STS-134, was presented to each team member in front of the EVA community.

Recently, the team was tasked to migrate over 7 years' worth of spacesuit data (over 8 TB) into the GovCloud environment because of a contract closeout.

(L-R): Cuong Nguyen, Yvonnne Lawley, Dave Foltz, Irina Patrikeeva, James Idemoto, Michael Crawford, Sandeep Shetye, Collin Estes, Mohana Gurram, and David Bell.

IT Infrastructure Integration Program (I3P) Update

Agency Applications Office, Formerly the NASA Enterprise Applications Competency Center

In 2014, NASA began a series of initiatives that focused on evaluating and selecting appropriate changes in Agency operating models to simplify work processes, rationalize capabilities, and achieve efficiencies. NASA established the Business Services Assessment (BSA) to perform an assessment of business and mission support services, looking for opportunities for optimization. The IT assessment was the pilot activity for the BSA.

An outcome of the assessment was a set of Mission Support Council (MSC) decisions, including the establishment of a new management structure for IT Services and the appointment of Program Executives for each IT program. The Program Executive for the Applications program has programmatic oversight for enterprise service delivery and IT authority for the investment review and compliance for all applications across the Agency. Service offices falling under the authority of the Applications Program Executive include the Enterprise Applications Service Office/NASA Enterprise Applications Competency Center (NEACC) and the Web Service Office.

On a parallel timeline, the IT support contract for enterprise applications, known as EAST, was being recompeted. The follow-on contract, EAST2, will provide NASA Centers with the ability to leverage the contract for their applications support. Marshall Space Flight Center (MSFC) has chosen to utilize EAST2 for its applications support.

As a result of these changes, a new organization has been established at MSFC to support the Agency Program Executive roles and responsibilities and to establish an organizational structure that can adapt to incremental scope changes over time.

The NEACC and the MSFC Applications Team have merged to form the new Agency Applications Office (AAO). The AAO's goal is to anticipate and align customer requirements with solutions that best enable the Agency's mission. The AAO will achieve that goal by providing and maintaining innovative, secure, efficient, cost-effective solutions for applications; maintaining a comprehensive understanding of the inventory and health of the Agency's application portfolio; and providing advice and counsel to organizations that choose to develop and maintain their own application solutions.

The AAO will continue to provide the host of business- and workforce-enabling applications, as well as crosscutting services and applications, formerly provided by the NEACC. The AAO will support the Applications Program Executive in areas of portfolio management, enterprise architecture, investment reviews, and other activities required to maintain a current knowledge of project status and risks.

For more information on the services the AAO offers, or to discuss options and best practices on an application solution you need developed, contact *MSFC-AAO-Customer-Care@mail.nasa.gov*.

Communications Service Office

With the implementation of the Mission Next Generation Architecture (MNGA) Core Network, the Communications Service Office (CSO) has just completed the second of three major projects of its integrated and comprehensive communications backbone strategy.

The cornerstone of this strategy is the implementation of the Mission Next Generation Architecture, which provides a secure and flexible infrastructure to support all current and future flight project requirements. Implemented with a redundant, diverse mesh design, the MNGA Core Network consists of four sites (Goddard Space Flight Center [GSFC], MSFC, the Jet Propulsion Laboratory [JPL], and White Sands Test Facility [WSTF]) and has the capability to provide project-specific Layer 3 private networks, thereby improving design flexibility and security.

The distributed design of the MNGA Core Network also improves the Continuity of Operations/Disaster Recover capability of the CSO Mission Network. The final CSO Backbone Strategy project, Mission Backbone Transition (MBT), which just completed its Phase 1 ORR, will transition current Agency Mission Routed Data Customers to the new Mission Network during FY16 and FY17, and it is anticipated that significant cost savings will be realized as legacy mission data circuits are downsized or decommissioned.

Computing Services Program Office

Working with Center Chief Information Officers (CIOs) and Deputy CIOs, the Computing Services Program Office (CSPO) was able to identify Cloud Computing Points of Contact (POCs) at each Center. As activities related to NASA's enterprise implementation of cloud computing increased, these designees were appointed to facilitate and coordinate between their Centers, the CSPO, other required offices, and their Center customers.

The goal is to establish a responsible and knowledgeable set of personnel, working on various cloud activities, and ensuring that processes run smoothly while providing Center customers with the best experience as the Agency increasingly chooses the cloud to meet its computing needs. These Cloud Champions have a variety of functions to perform, including serving as each Center CIO's advocate for cloud computing; facilitating the collection and discussion of requirements with potential customers; informing Center customers about the Enterprise Managed Cloud Computing (EMCC) framework and its options; representing their Centers on several boards, including the Computing Services Service Board (CSSB); and keeping their Center CIOs informed about cloud-related activities, initiatives, and progress on Center-specific cloud implementations. The newly minted Center Cloud POCs also have access to the OCIO and Center technical, information assurance, and business office resources to implement various cloud activities.

Last, but not least, they will be working with their Center CIOs to report progress, issues, and metrics and to inform them about new cloud service offerings, as well as breakthroughs in NASA's cloud adoption. The Center Cloud POCs have already met with CSPO Program Executive Karen Petraska and EMCC Program Manager Ray O'Brien in a kickoff meeting designed to inform, gather input, and determine the best way to move forward into this dynamic and exciting new Agency service. To view a list of our Center Cloud POCs, navigate your favorite browser here: *https://intranet.share.nasa.gov/agency/cloudservices/Pages/About-Us.aspx*.

End-User Services Office

Self Service Manager:
The Agency has introduced a new tool, Self Service Manager (SSM), that allows users to self-install software they are assigned to receive at a time convenient for the user. SSM is available now on all NASA ACES Windows and Mac computers and will soon be made available to non-ACES users. Users who have had software assigned to them (become "entitled") receive instructions on how to use the SSM tool to download the software. The tool was tested last year through Office 2013 deployment and is now being used to deploy various software packages. Over the next few months, all software on each NASA Center's Software Refresh Portal will be migrated to the new SSM tool and the individual Center refresh portals will be decommissioned. One centralized tool will result in better integration and greater efficiency for the Agency. To learn more about the SSM tool, go to the SSM User Guide at *https://aces.ndc.nasa.gov/documents/SelfServiceManagerUserGuide.pdf*.

New E-mail Security Features:
Proofpoint is the Agency antispam/antivirus solution that filters your NOMAD e-mail for spam and protects NASA from virus attacks. When Proofpoint Targeted Attack Protection (TAP) is implemented, there will be changes to the way links in e-mail messages appear and changes to the way attachments are scanned for malware. NASA will enable the Proofpoint TAP service this spring. For details on these changes, refer to Proofpoint Targeted Attack Protection Basics at: *https://nomadinternal.nasa.gov/nomad/files/ProofpointTAPBasics.pdf*.

BlackBerry Retirement:
NASA is phasing out BlackBerry devices across the Agency by February 2017. NASA's Mobile Device Management (MDM) and new Four-CERT Personal Identity Verification (PIV) cards being issued by NASA do not support BlackBerry encryption. Therefore, new BlackBerry devices can no longer be ordered, and BlackBerry users scheduled for refresh beginning in May will be eligible only for a Like-for-Unlike refresh. Users should transition to an iOS or Android device. Encryption for iOS and Android devices is supported by Four-CERT PIV cards and will be enabled as part of MDM Phase 2 implementation later this year. BlackBerry users requiring encryption prior to implementation of MDM Phase 2 are recommended to delay their mobile refresh until the MDM Phase 2 solution is in place.

Enterprise Service Desk

The Enterprise Service Desk (ESD) welcomes GSFC's Applied Engineering Technology Directorate (AETD) as its latest incident-management user. The AETD is the most recent of several non–IT Infrastructure Integration Program (I3P) programs to turn to the ESD for support of its Center-based, non-I3P services. ESD began providing incident-management support to AETD on March 15, taking in and triaging tickets via Tier 0 and Tier 1, and assigning them to AETD directly in ServiceNow when the ESD is unable to resolve the user's issue. GSFC thus joins Headquarters, Glenn Research Center (GRC), and the Space Technology Mission Directorate as incident-management users working within the ESD's system.

The ESD subject matter experts (SMEs) will hold their annual Face-to-Face (F2F) meeting at Armstrong Flight Research Center (AFRC) the week of June 20. Most Center SMEs will be in attendance, with those who cannot attend dialing in from their Centers. The ESD Service Executive and ESD Service Office will be present to run the meeting. Service Office Integration Leads (SOILs) have also been invited to attend. The agenda includes the latest changes to ServiceNow, a deep dive on ServiceNow reporting, and more. Thanks to AFRC for hosting this important meeting.

Web Services

Google Apps for Work Now Available Across NASA:
It took less than 6 weeks for WESTPrime to deliver Google Apps for Work (GAfW). Users and their content were seamlessly migrated from Google Apps for Government (GAfG) to GAfW. With added security enhancements, NASA employees are now able to collaborate securely with internal and external resources. GAfW is a subscription service and requires NAMS authorization and SATERN training.

DevOps Suite Launched in GovCloud
A suite of DevOps tools—Confluence, JIRA, BitBucket (formerly Stash), and Bamboo—are now available in WESTPrime GovCloud and Public/Commercial cloud offerings. The suite is integrated with NASA LaunchPad. The DevOps suite in GovCloud supports Federal Information Security Management Act (FISMA) moderate-level data. WESTPrime has completed content migration, and decommissioning is planned. Access requires NAMS authorization and project owner approval.

Internet Protocol Version 6 Solution in WESTPrime Cloud
Thanks to the engineering expertise of WESTPrime, a solution for Internet Protocol version 6 (IPv6) compliance on the AWS public cloud is now in place. NASA public-facing Web sites at WESTPrime now meet the Government's requirement for IPv6 compliance. IPv6 is not currently supported in the AWS public cloud. To meet the Government mandate, WESTPrime architected a solution that establishes a gateway to IPv6 and IPv4.

Contact Web Services at *https://inside.nasa.gov/webservices* for more information.

NASA CIO Renee Wynn visited AMES in March 2016. Wynn plans to visit one Center every month. (l-r): AMES DCIO Grace DeLeon, NASA CIO Renee Wynn, AMES CIO Jerry Davis, OCIO Communications Officer Eldora Valentine, and Senior Advisor for Cybersecurity Robert Powell.

IT Talk

National Aeronautics and Space Administration

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

www.nasa.gov

NASA CIO