National Aeronautics and Space Administration

IT Talk

October - December 2016 Volume 6 • Issue 4

WARNING:

Dangerous Turns Ahead!

Staying Safe While Driving Online

IT Talk

Oct - Dec 2016 Volume 6 • 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

October is Cybersecurity Awareness Month. I'm asking all employees to "Stop. Think. Connect." They are simple actions we can all do to stay safer and more secure online.

- **STOP:** Before you use the Internet, take time to understand the risks and learn how to spot potential problems.
- **THINK:** Take a moment to be certain that the path ahead is clear. Watch for warning signs and consider how your actions online could impact your safety or your family's.
- **CONNECT:** Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer.

Cybersecurity is everyone's responsibility! In this issue, we'll learn more about staying secure—not just at work, but at home too!

Organizational changes within the Office of the Chief Information Officer are also contributing to NASA's improved IT security posture. Jeanette Hanna-Ruiz has been hired as NASA's Senior Agency Information Security Official (SAISO). She's working with all our NASA Center CISOs as well as CISOs across the Federal Government on operational IT security and cybersecurity matters. We remain committed to ensuring that the best security practices are implemented at NASA and that NASA remains protected against threats.

We'll also take a look at some initiatives that are helping us do our job better at the Centers. As the IT Business Services Assessment implementation marches forward, we have made significant progress in completing tasks and hitting milestones. I'm happy to say that we are making great strides in posturing ourselves to be more effective and efficient in developing a dynamic operating model to meet current and future mission needs.

I hope you enjoy reading this quarter's issue.

~Renee

NASA Hires New Associate Chief Information Security Officer

In August 2016, NASA welcomed the newest member of its team, Jeannette Hanna-Ruiz, Associate Chief Information Officer (ACIO) for IT Security and Senior Agency Information Security Official (SAISO).

Hanna-Ruiz is a leader with a track record of success in taking on challenging situations and delivering measurable results. She has more than 20 years of experience working in the Government, nonprofit, and private sectors as a senior leader, manager, and consultant. She brings considerable homeland and national security expertise, having worked at the Department of Homeland Security (DHS)–National Security Agency Joint Cyber Coordination Group, the Department of Transportation, and the Department of Homeland Security. She also played an important role in defining DHS's cyber mission and building up the department's cyber capabilities.

In addition to her public-sector experience, Hanna-Ruiz has worked in the private sector for Microsoft, where she was a senior leader in their services business. There, she was responsible for the identity management team and was the lead for the company's public-sector civilian cybersecurity operations. As Director of Cyber Forensics and Cybersecurity, she led the operational delivery team for the Computer Sciences Corporation at the Department of Defense Cyber Crime Center, Defense Cyber Investigations Training Academy. She also is a professor of Cybersecurity at the University of Maryland.

IRD 2.016 Stand Down Day

By Jaumarro A. Cuffee, JSC IRD Communications

As NASA prepares to "Stop. Think. Connect." for Cybersecurity Awareness Month in October, the Information Resources Directorate (IRD) at Johnson Space Center planned a day to Stop. Think. Connect. for awareness and education about the IT Business Services Assessment (BSA) and the Federal Information Technology Acquisition Reform Act (FITARA).

IRD 2.016 Stand Down Day scheduled live and recorded salutations from NASA, JSC, and IRD leadership; presentations from members of the IRD Leadership Team about implementing the seven IT BSA Decisions and FITARA; an interactive learning activity; and an open question-and-answer session.

The IRD team and JSC key IT stakeholders were invited to stop their daily routines and invest time in understanding how IT BSA and FITARA can help evolve Agency IT processes and programs to strengthen buying power, sustain current IT while investing in emerging technologies, and support a more secure IT infrastructure.

Presentations were crafted to share key concepts of roles and responsibilities, IT governance, data centers, communications, workstations, collaboration, IT security, and FITARA for attendees to think about. This insight would enable audience members to submit questions for the afternoon session. The initial TED-style talks were intended to help frame discussions based on facts, help to dispel some of the notions that hinder change, and get everyone to think about how the changes would affect their respective areas and organizations.

A "what's new" trifold, paired with Pokémon, was put together to lead participants through an interactive session. The interaction was designed to encourage reading and processing information about IT BSA and FITARA.

The afternoon agenda included an IRD "Feud" to share a few good answers before connecting the audience with the IRD implementation leads in an open question-and-answer session.

Stopping to focus on IT BSA and FITARA, thinking about the upcoming changes by engaging in activities, and connecting through lively presentations and Q&A sessions, IRD strives to encourage its team members and Center IT influencers to embrace the coming changes and work together to evolve IT processes and programs in support of NASA missions now, and for the future.

Photographs: (NASA/James Blair)

CAS High-End Collaboration Conference Facilities

By the CAS Collaboration Rooms Team

The Office of the Chief Information Officer and Aeronautics Research Mission Directorate (ARMD) have formed a partnership to deploy Convergent Aeronautics Solutions (CAS) collaboration rooms outfitted with high-end collaboration and conferencing capabilities. The CAS Project, within the Transformative Aeronautics Concepts (TAC) Program, is implementing 10 state-of-the-art collaboration facilities. The goals of TAC and CAS are to make rapid and significant advancements in aeronautics technologies. Some of the methodologies to achieve the goals of CAS are leading inter-Center discussions and teaming, simultaneously leveraging and integrating cross-Center expertise, generating ideas, conducting rapid feasibility assessments, and providing opportunities to all researchers to advance aeronautics by participating in CAS processes.

The CAS collaboration rooms, based on Mezzanine technology by Oblong Industries, Inc., provide interactive ultra-high-definition audiovisual collaboration for multiple users (either local or remote) in a shared digital workspace. Although video teleconferencing is not new to the Agency, Mezzanine offers functionality intended to further smooth the road to collaboration. Each room features two clusters of three ultra-high-definition video screens.

One of the features of Mezzanine, gestural interface, is made possible by using the wand controller supported by an array of ultrasonic sensors installed in the ceiling. The wand allows users to easily move/resize images or displays from one screen to another, regardless of where the user is or who shares the material. By shifting the wand forward or backward, the user can shrink or enlarge a display. A quick turn of the wrist enables the user to capture screen shots of any portion of the display. This sort of dynamic interaction helps to bring people from different Centers together and make them feel more like they are in the same room solving the same problems. Collaborative work sessions are accessible by desktop, laptop, tablet, or smartphone. Additional features include touch-based annotations via mobile devices, whiteboard capture to retain key points, and session archiving and meeting restart capabilities.

The 10 CAS collaboration rooms have been deployed throughout NASA's four primary aeronautics Centers (AFRC, ARC, GRC, and LaRC) with the primary intent to facilitate collaborative partnerships on projects supported by ARMD. However, this technology is also applicable to other missions, programs, and institutional organizations.

For more information about this new collaboration environment, please contact any of the following:

Emil Machac: CTO-IT, AFRC

John Stebel: CTO-IT, ARC

Les Farkas: CTO-IT, GRC

Ed McLarney: CTO-IT, LaRC

JPL Selects Wes Gavins as New Chief Information Security Officer

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

Sylvester "Wes" Gavins was selected in July as the Jet Propulsion Laboratory's (JPL's) new Chief Information Security Officer (CISO). Gavins came to JPL from Booz Allen Hamilton, where he was a senior manager and chief technologist over cybersecurity, IT compliance, and system/network security. Prior to joining Booz Allen, Gavins was a captain in the United States Marine Corps (USMC), where he served as a communications and information systems officer. He brings over 25 years of experience in cybersecurity, systems engineering, business analysis, project management, and risk management in the telecommunications, aerospace, defense, and commercial industries.

In his role as JPL CISO, Gavins will

1. provide strategic direction for all cybersecurity technology areas, including applications, networks, and storage;
2. serve as the authority and primary JPL representative on internal and external security architecture teams;
3. be responsible for selecting solutions to enhance security controls; and
4. conduct risk assessments for major Lab-wide processes and make major security risk decisions.

Gavins holds a master's degree in telecommunications systems management. Additionally, Gavins is Certified in Risk and Information Systems Control (CRISC), a Certified Ethical Hacker (CEH), and a Certified Expert Independent Auditor (CEIA).

Warning: Dangerous Turns Ahead

By Robert W. Powell, NASA Senior Advisor for Cybersecurity

Years ago, news of a digital communication advancement promised to be revolutionary, game-changing, and filled with endless possibilities for global business transactions as well as unprecedented information exchange. If you guessed it was the information superhighway, then you would be correct! It's a phrase most would credit former U.S. Vice President Al Gore with having coined during the 1980s. I recall the endless hype and excitement with this new and emerging method for global connectivity and digital information exchange. The name alone just sounded cool! Living in the Washington, DC area at that time, I also recall thinking that if the information superhighway was anything like the DC Beltway, then we could be in for an accident-prone ride fraught with multivehicle crashes and inconvenient fender-benders. Fast-forward about 20 years, and we now recognize that the information superhighway has morphed into an online environment we know as the World Wide Web and the Internet. For me, however, I still maintain the correlation of going online to the experience of driving a car on the DC Beltway: entering an environment that can be at times dangerous and filled with unknowns. Widespread data breaches certainly have the potential to create a dangerous situation when you consider the impact of an adversary having gained Personally Identifiable Information (PII), financially sensitive details, or personally sensitive records such as medical history.

Just as you prepare to enter into the environment of motor-vehicle operations, you should take the same approach when preparing to engage in the world of online data transactions. Safe vehicle operators routinely follow a set of procedures such as checking side and rearview mirrors before entering lanes of oncoming traffic, ensuring that fluids are at proper levels, and fastening seat belts before leaving a parked position. Staying safe online should include a set of routine safety procedures. Below are some cybersecurity safety tips to consider before you merge onto the heavily trafficked world of online data exchange:

- Use strong passwords containing at least 12 characters, with a combination of numbers, uppercase letters, lowercase letters, and symbols; this makes it effectively impossible for someone to guess your password and difficult to use brute force to crack a hashed and salted password without a computer cluster specially designed for password cracking. (To learn more about hashed passwords, go to the site *https://wired.com*, search for the terms "lexicon hashing", and click on the article labeled "Hacker Lexicon: What Is Password Hashing." To learn more about password-cracking clusters, go to the site *http://arstechnica.com* and search for the term "cluster password".)
- Never use the same password for multiple accounts.
- Use separate e-mail addresses for work, banking, and social interactions; doing so will allow you to quickly identify potential phishing attempts. For instance, you should never receive banking-related messages at your work or social e-mail addresses, and if you ever do, you should treat the

Staying Safe While Driving Online

message as highly suspicious and a possible phishing attempt.

- Never click on any links contained in e-mails from individuals you don't recognize; don't let curiosity overcome your ability to stay safe online. My boss often says, "You're not going to win that free iPad by clicking on the link." Even if the e-mailed link comes from one of your known contacts, it's possible that the e-mail address has been spoofed and the link contained within the e-mail is a phishing attempt; my approach is to never click on any e-mailed link without first running it through a site that verifies the legitimacy of URLs, such as *https://virustotal.com*.
- If anyone asks you for your Social Security number (SSN), make sure that the requesting organization truly has a need for it. Unless you're dealing with a financial or credit-related transaction, chances are that your full SSN is not needed.
- If you get spam e-mail, never click on the link within the e-mail to unsubscribe from the sender's service; instead, report the e-mail as spam to your Internet service provider. To learn more about this topic, got to the site *http://www.idtheftcenter.org* and search for the term "spam unsubscribe".
- Always be suspicious of any caller who requests that you provide online account information such as your username or password; legitimate callers from online companies or organizations will already have this information on hand.

In the end, there is no absolute fail-safe way to prevent malicious online activities by motivated bad actors. The hacker community is becoming incredibly sophisticated and is deploying tactics such as social engineering at an alarmingly successful rate. In the same manner that driving a car requires an operator to have a mindset of accident prevention and constant vigilance, "drivers" on the Internet should maintain heightened levels of awareness to safeguard against catastrophes. Remember, cybersecurity begins and ends with you!

Cybersecurity Tips

STOP. THINK. CONNECT.

Be aware of phishing e-mails and do not click on unfamiliar links. Do not send classified, sensitive but unclassified, or otherwise confidential information unencrypted through e-mail.

- Choose passwords that are strong, long, easy to remember, and hard for others to guess.
- Shut down, hibernate, lock, or sleep your laptop every night and whenever you take it out of the building.
- Encrypt all files that contain Personally Identifiable Information (PII).
- Report any suspicious IT security or cybersecurity incidents to NASA's OCIO Security Operations Center (SOC) at 1-877-627-2732. It is available 24 hours a day, 7 days a week.

Cybersecurity is everyone's responsibility! For more information about staying secure at work or at home, visit the IT Security Awareness Training Center Web site at *https://itsatc.nasa.gov/*.

Cybersecurity in the Cloud Gaining Trust—WESTPrime Insights

By Mary Phillips, InfoZen Communications

The perception of cloud computing in Government has changed over the past few years. Once married to private clouds, Federal agencies like NASA are now using public or commercial cloud services to improve IT service delivery and cut costs. When it comes to migrating the mission-critical workloads, security still remains a concern, yet trust is building. Here's why.

In 2010, under the Cloud First policy enacted by former White House CIO Vivek Kundra, an estimated $20 billion of the Federal Government's $80 billion budget was targeted to be spent on cloud services, based on agency estimates reported to the Office of Management and Budget (OMB). The policy directed Federal agencies to move three technology services, like e-mail, to the cloud within 18 months of its inception.

Shortly thereafter, Amazon Web Services (AWS) made a move to equip the Government with its own trusted public cloud infrastructure, which included security at the building and data center level housing Federal Information Security Management Act (FISMA) Moderate. AWS GovCloud was made available to U.S. Government agencies and organizations in Government-regulated industries that met requirements for access. It served the Government's unique needs and regulatory requirements, making it easy to use while also securing and protecting the infrastructure from unauthorized access.

Public Cloud Service Providers (CSPs) like AWS and Microsoft Azure operate on a shared security model where the CSPs are responsible for physical infrastructure and customers are responsible for their application security (firewall policies, network

security, etc.). These developments and proven use cases have further enabled Government employees to shift their view of cloud security in the public cloud. All Federal agencies have been actively using and moving their workloads to the public cloud ever since.

NASA has securely deployed over 150 applications under a contract called WESTPrime. The types of applications include the Agency's premier portal, *http://www.nasa.gov*; *http://images.nasa.gov*; and the *https://science.nasa.gov* public-facing sites. In addition, the Science Mission Directorate (SMD) from NASA has several applications hosted internally on both US-EAST Region and GovCloud in AWS.

In GovCloud, NASA WESTPrime has deployed several applications, including Extravehicular Activity (EVA), the NASA Engineering Network, mission-critical applications like Life Sciences, and Enterprise Search. To date, over 25 internal and Internet-facing Web applications have been deployed and maintained on WESTPrime's Drupal-as-a-Service (DaaS) platform. Identity and access management (ICAM integration with Launchpad, as well as Active Directory) with Multi-Factor Authentication (MFA) enhances and layers security on all of these applications.

Cybersecurity in the cloud is further enhanced by the deployment of various tools like Web application firewalls (WAFs), network monitoring tools, auditing/logging tools, and behavioral analysis/analytics for insider-threat monitoring with continuous improvement of the security posture. This security extends from network to application and devices. Security controls, like the use of pre-hardened instances, system vulnerability scans, and static code analysis, further enhance the security posture.

The perception of the cloud continues to shift positively with success stories. With the correct partnerships and capabilities in place, Government agencies can more fully embrace efficiencies and trust security in the public cloud. And the IT implementers' and integrators' knowledge of FISMA requirements and data-level requirements ensures efficient and secure migration paths to the cloud.

Ames IT Directorate Hosts UC Berkeley Summer Students for the Day

By Jerry Davis, Chief Information Officer, Ames Research Center

Ames Research Center's (ARC's) IT Directorate (Code I) recently hosted high school students from two University of California, Berkley (UC Berkeley), summer camp programs. CYBEAR (Cybersecurity and Cal's Bear mascot), a 6-week GenCyber summer program, engages high school students in cybersecurity, helping them explore their own digital footprint and cyber-physical infrastructures. CYBEAR students and their mentors were provided with security demonstrations on phishing, forensics, and wireless security technologies while at ARC for the day. This summer, students built an entire Lego city, with focus on infrastructure, utilities, transportation, the programming of the software running the city, and how all of these come together. They became aware of all the behind-the-scenes work being done in real cities and how challenging it is to protect cities from those cybercriminals who would disrupt daily operations.

The Summer University Camp for Computing, Engineering, and Science Scholars (SUCCESS) program is a 6-week summer program offered by UC Berkeley's College of Engineering. SUCCESS was created to offer high school students a chance to blend maker techniques and skills with ideas introduced to them by Berkeley engineers and researchers on the leading edge of their fields. Ames has a unique set of Human Systems Integration capabilities ranging from basic research in visual perception, motor control and psychophysiology, to direct applications in both aeronautics and space. In aeronautics, the focus is on air traffic management, mission controller displays, and crew procedures. In space application areas, the focus is on design and development of next-generation mission planning and information systems. Over 120 researchers across a dozen labs work to enable efficient and safe operations toward NASA's aeronautics and space explorations goals. SUCCESS campers were treated to demonstrations and tours of these unique capabilities, at the Unitary Wind tunnel, the Rotorcraft Research Group, and the 20-g centrifuge. After their tours were finished, Code I treated the students and their mentors to lunch and a visit to the Ames gift shop. The photos below were sent with a lovely thank-you card and are signed on the left (SUCCESS) and right (CYBEAR) by all the students.

SUCCESS students on tour in the Rotorcraft Hangar.

Students from the 2016 CYBEAR program posing for a thank-you photo.

BSA Corner

Implementation of the Mission Support Council Decision Plan for the IT Business Services Assessment (BSA) is well underway. Data calls are in; analysis is ongoing; and policies are up for approval. Behind the scenes, the OCIO has been reaching out to stakeholders and Change Leaders for input and questions.

Decisions by Month

For an overview of the decisions at a glance, check out the IT BSA poster on the Inside OCIO BSA Web page (*https://inside.nasa.gov/ocio/bsa*) (must be accessed while connected to a NASA network). To keep you informed and break down the decisions, the OCIO tackles each Decision Area month by month. August, our inaugural month, focused on collaboration tools and content management. During that first month, we:

- Shared a decision recap
- Summarized the governance
- Sourced the tools
- Examined mobile compatibility
- Provided examples of tools
- Understood core suite characteristics
- Demonstrated the benefits of enterprise management with a SharePoint case study
- Defined ways to collaborate
- Looked forward to what's next for collaboration tools

To catch up on anything you missed, visit *https://inside.nasa.gov/ocio/bsa-faqs*.

Look Ahead: Approved Collaboration Tools Portal coming soon!

This September, the OCIO highlighted the Communications Decision Area. We circulated:

- The decisions
- Enterprise communications history
- Impact of changes on Center collaboration
- Understanding of Corporate and Mission services
- Savings "wedge" explanation
- Updates on the status of active initiatives, including External Border Project (EBPro) and Enterprise Internal Border—Network Access Control (EIB-NAC)

In October, we will discuss data centers, promote cloud computing, and invite everyone to the Cloud Computing Community of Interest (COI) forums.

Look Ahead: Agency-wide IT BSA Webinar, featuring CIO Renee Wynn, in January 2017

BSA Achievements

As IT BSA implementation marches forward, we have made significant progress in completing tasks and hitting milestones. As of 8/31/16, 34 percent of tasks are fully complete with nearly 4 percent more that are almost closed. These tasks cover all Decision Areas and include working with the change network, revamping governance boards (the IT Council [ITC] met for the first time on May 25th), completing analyses of Centers and programs, holding Center town halls, and finding savings in enterprise consolidation (e.g., approximately $7 million annually under SharePoint). All of the tremendous work and input from Centers, Mission Directorates, and Mission Support Directorates is foundational and valued.

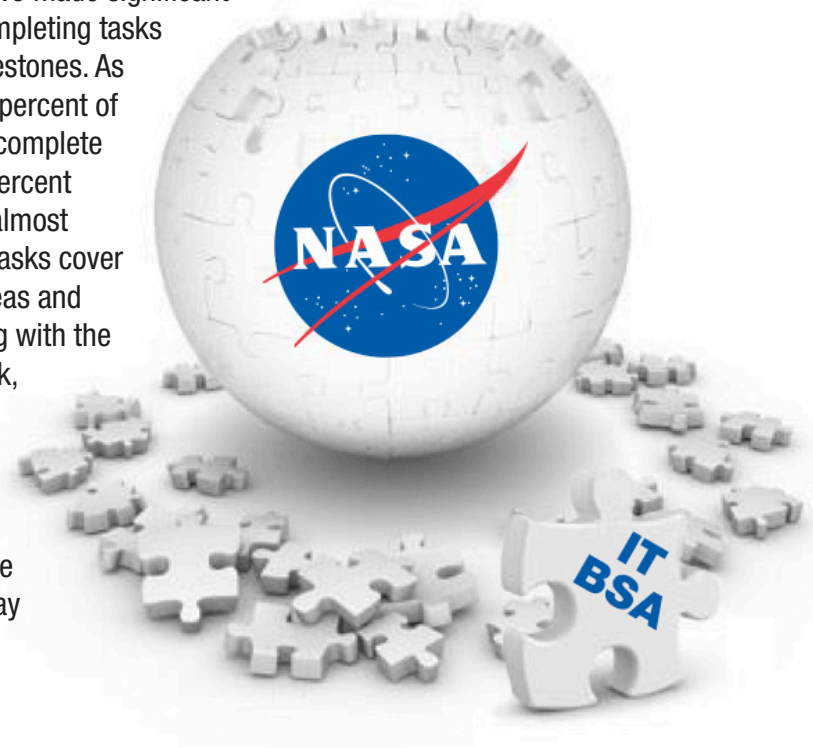
Questions and Answers

For more information about the IT BSA, visit our Web site, which is updated regularly. If you have any questions, please send them to the e-mail address below; you will receive a personal response, and we will post the question and answer to our FAQs. Finally, you can always check in with your organization's Change Leader and communications lead.

Web site:
https://inside.nasa.gov/ocio/bsa

FAQs:
https://inside.nasa.gov/ocio/bsa-faqs

Questions:
HQ-ASK-BSA-IT@mail.nasa.gov



Application Inventory, Application Portfolio Management (APM), and Application Rationalization Vision and Goals

NASA IT Portfolio Management (ITPM) is a risk-based approach to the selection and management of IT projects integrating business and IT planning, budgeting, standards, processes, and governance. This approach includes Center and program portfolio functions that align with the Agency model, can share information for analyzing NASA's IT investments, and report from a set of authoritative sources. Ultimately, ITPM allows total visibility into all IT investments across the Agency to identify duplicative investments, optimize IT capabilities, improve services delivery, and better support Agency priorities. With modified governance, ITPM includes the appropriate stakeholders to prioritize and direct the implementation of agreed-to IT investments.

The Applications Program Office is defining the Agency application strategy and roadmap that will allow for both the evolution of the application portfolio to support the business strategy and the underlying processes and skills needed to do so. As part of the overall application strategy, application rationalization will be performed with the goals of reducing cost and portfolio complexity. The rationalization efforts will inform the investment management processes associated with the application portfolio and will include application health assessments. Application rationalization teams are now in place across the Agency and will be reviewing the current portfolio of application projects, in addition to the projects in the pipeline, for approval in order to establish the impact of these investments on the goals of the application rationalization program.

The Applications Program Office coordinated the Annual Capital Investment Review (ACIR) early in 2016 that required Agency-wide consolidation of application information in the Application Portfolio Assessment Tool (APAT). The data provided through the ACIR is under initial review by multiple teams with short-term actions to

1. review program languages in use today and develop standards for the future,
2. merge System for Tracking and Registering Applications & Web sites (STRAW) and APAT data,
3. improve security posture by mitigating risk, and
4. look for optimization opportunities, including strategic sourcing.

The desired future state, now underway, is to solidify the approach for maintaining an official Agency inventory of applications, including planned investments, and to establish a consistent process that can be used for application portfolio management, application rationalization, and a response to a variety of data calls. Application Portfolio Management will position the Agency to leverage this inventory and potentially reduce application "sprawl." Additionally, as new requirements emerge, this tool provides the capability to look for existing solutions rather than duplicating solutions.

NASA CIOs, DCIOs, and HQ OCIO Staff at the CIO Executive Council (CEC), Hosted at Ames

Photo: (NASA/Dominic Hart)

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