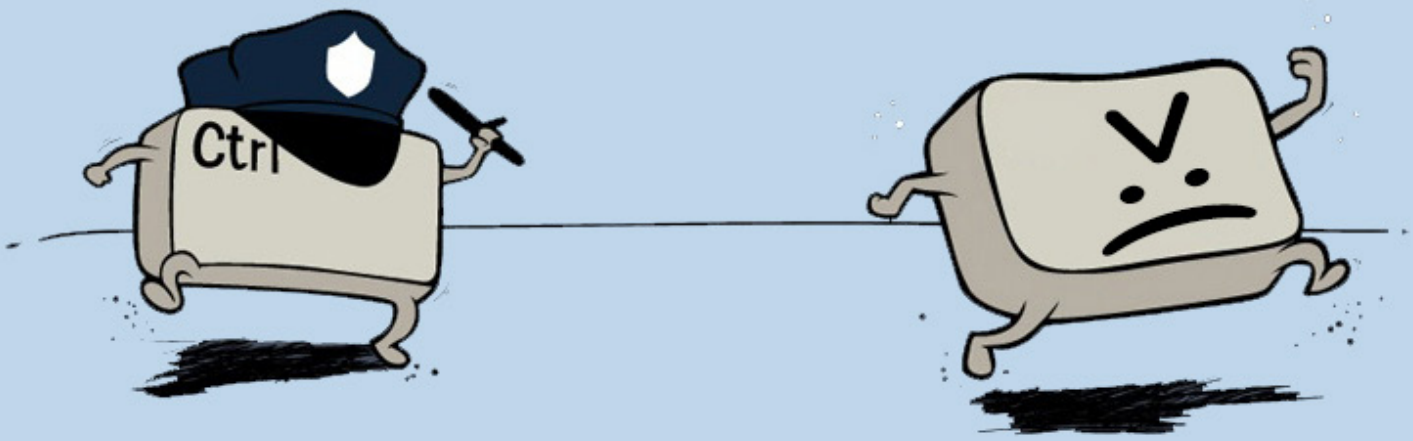
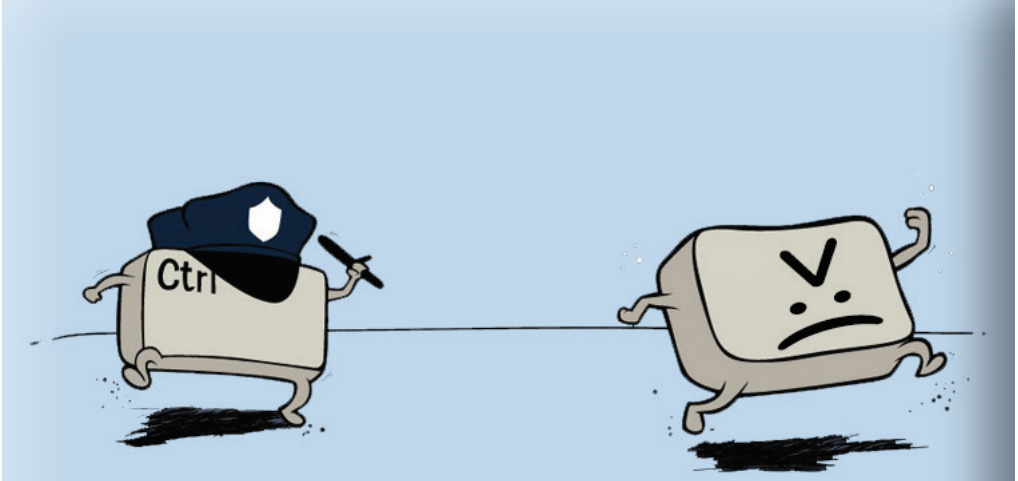
National Aeronautics and Space Administration

IT Talk

January - March 2014 Volume 4 • Issue 1

Get Cyber-Bullying Under Control





IT Talk

Jan - Mar 2014 Volume 4 • Issue 1

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

Chief Information Officer
Larry Sweet

Editor and Publication Manager
Eldora Valentine

Graphic and Web Design
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/

- facebook.com/NASAcio
- twitter.com/NASAcio

In this Issue

Message from the NASA CIO

The New Year is a time when we look forward to the future. Some of us like to think about the great memories that the last year has given us, and others would rather not remember the last 12 months at all. One of my goals for the New Year is to not stress out about the things I have little control over, but instead to embrace our situation as it is, move forward in a positive manner, and accept this as our new reality. These days, many Federal agencies are forced to look for ways to do more with less. We might not like it, but we need to deal with it. I still believe we can make 2014 a stellar year in IT. Keeping some strategic resolutions will save money and improve productivity. Here are my top 10 2014 New Year's resolutions.

1. IT Security—ensure that NASA data is more secure. Our equipment and information must be protected against vulnerabilities and breaches.
2. Firm up NASA's policies and position on bring-your-own-device (BYOD) and embrace mobile technologies.
3. Strengthen the NASA Chief Information Officer (CIO) Leadership Team by embracing collaboration with CIOs at the Centers and building trust within the Office of the CIO (OCIO) and throughout NASA.
4. Develop an IT program that adjusts to the challenging budget environment by being more adaptable and flexible, moving toward more "services on demand," adopting more cloud services and new offerings, and improving IT service performance (for example, I3P).
5. Improve IT governance by addressing each recommendation outlined by the Inspector General (IG) and approved by the Mission Support Council, assessing roles and responsibilities for IT decision making, and looking at current model execution.
6. Develop a Digital Government Strategy and Open Data Policy.
7. Continue to show IT's value.
8. Better leverage cloud capabilities that enable mobility and cost reduction.
9. Stop worrying about what we cannot control, and focus more on what we can do better that enables our customers.
10. Ensure and embrace a healthy work-life balance for all employees.

I look forward to another year of working with all of our dedicated team members. I wish each of you a happy, healthy and successful 2014.

~Larry

New Johnson Space Center CIO Named

By Jaumarro Cuffee, JSC I3P Outreach Lead/ITAMS

Annette Moore was selected as the Chief Information Officer (CIO) for Johnson Space Center, and Director, JSC Information Resources Directorate (IRD) on Oct. 22, 2013. Moore says the two jobs require a lot from her. "The two roles often call for me to be advocate, advisor, counsel, mediator, mentor, and many other things."

Moore considers enabling team members to work from anywhere, cloud computing and telepresence as promising initiatives. Looking at industry leaders like Google and Amazon, Moore says the Agency has done awesome things. "We put a man on the moon --- on the ISS… I want us not to be satisfied with what we've done but to continue to look at what more we can do and what we can do differently. When it comes to those technologies I want us to surpass what others are doing."

To do that, Moore focuses on inclusion, innovation and people by serving in various informal and formal mentoring programs such as Mid-Level Leader Program (MLLP) Center Champion and sponsoring center Employee Resource Groups.

"As IRD explores and enters into partnership with other entities…then we will have at our hand information, technology, resources, ideas and solutions that will make us more informed, more innovative and creative service providers for our customers," Moore says.

Moore sees the coolest part of her job as working "for" NASA and having an incredible staff. "I get to enable and influence that future. I can't imagine anything more terrific!"

New Kennedy Data Center Complete in 2014

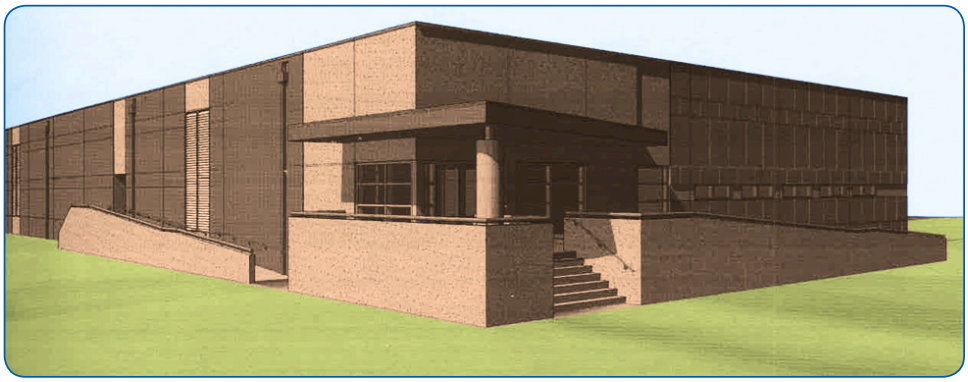
By Bryan "Trip" Banks, IT Project Manager, Kennedy Space Center

A new Data Center will be constructed at the Kennedy Space Center (KSC), with a completion date scheduled for late 2014. The 16,600-square-foot stand-alone facility will be located south of the current KSC Headquarters building.

Compliance with Federal mandates required that KSC reduce from five Data Centers on site to just one. Upon a review of candidate buildings, it was determined that no existing facility could accommodate consolidation goals without requiring costly upgrades and modifications. Current operations in those facilities would be severely hampered by the construction effort, requiring extended facility outages. A business case was presented to the Agency Facilities Management Board in October 2011 and funding was subsequently approved. Facility design began in early 2012, and a construction contract was awarded in September 2013.

The new Data Center will be comprised of a 5,069-square-foot compute space and will employ fan-wall technology for cooling the IT equipment, with a return-air plenum located within the ceiling. The Data Center electrical systems will be rated Tier 3 (Uptime Institute) and include redundant uninterrupted power systems and backup generators, with a "day one" electrical IT load of 380 kilowatts and the capability to expand to 700 kilowatts. The utility electrical power to the building will be provided from mutually exclusive feeds, adding a layer of additional fault tolerance. The Mechanical systems will be at Tier 2 level on "day one."

The Data Center is designed to be self-sufficient and will include a loading dock, storage area, setup and test environment, Operations Center, and service yard. It will also house the KSC Alternate Protective Services Control Center. An administration area with four cubicles is included, but the facility will not have permanent residents, as the Data Center will be predominantly a "lights-out" operation.



The new Data Center allows KSC to reduce approximately 25,000 square feet of current compute space by 80 percent, thereby significantly reducing Center power and administrative costs. Once the functionality of the current Data Center, located within the 48-year-old Central Instrumentation Facility, is migrated to the new facility, the building will be demolished, eliminating the operations and maintenance costs associated with that 136,378-square-foot building.

The new Data Center is designed to be both scalable and modular, quickly adapting to accommodate new IT architectures and technologies, and it will serve as a key component in maintaining the Kennedy Space Center's position as the world's premier launch complex.

NASA Enterprise Applications Competency Center (NEACC) Disaster Recovery: Planning and Testing before a Disaster Occurs

By Kathy Rice/IS01/NEACC Communications Lead (Interview with Benjamin C. Jones, NEACC Support Systems Manager)

When the threat of disaster becomes a reality, how prepared are our IT professionals to handle disaster recovery at the NEACC? A disaster recovery plan (DRP) is a plan for business continuity in the event of a disaster that destroys part or all of a business's resources, including IT equipment, data records, and the physical space of an organization.

In June 2013, the NEACC utilized a major release test phase as an opportunity to conduct a remote replication—asynchronous (RRA) exercise. An integrated test cycle (ITC) test environment was moved to Kennedy Space Center (KSC) to have end users conduct normal testing, as part of the RRA test. When asked about the test approach, Benjamin C. Jones said, "The test approach criteria included defining the disaster recover [DR] test scope, documenting the technical failover process, and validating the recovery process for the impacted applications and data. The goal of the test was to determine the amount of data loss if the systems were brought

(Continued on page 5.)

Ames Helps Pave the Way for NASA's Future Use of Cloud Computing Services

By Raymond O'Brien, Chief, External Projects and Services Division, Ames Research Center

A combination of Federal policy, paired with an increasing understanding of cloud computing within NASA, has created new opportunities and challenges for the Agency Office of the Chief Information Officer (OCIO). Cloud services, if properly leveraged, can offer lower costs, seemingly infinite scale and capacity, and almost immediate access to computational services, ultimately benefitting project teams and organizations who adopt this powerful new service. However, obstacles to institutionalizing cloud services still remain. The OCIO, in partnership with IT Experts at Ames and several other Centers (e.g., JPL, LaRC, MSFC, and JSC), has been working to develop NASA's approach for cloud security compliance, technical integration, and business processing. The work is targeted at enabling broad cloud adoption, while ensuring proper levels of IT security, policy compliance, and integration with existing NASA IT services and business functions.

One of the largest challenges associated with cloud computing is adapting to a model of shared-responsibility for computer security. We've grown accustomed to on-premise infrastructure where security is solely NASA's responsibility. Now the physical infrastructure, and native software used to deliver commercial cloud services, exists outside of NASA. To address IT Security risks, the Federal Government will soon require all commercial cloud services adhere to the Federal Risk and Authorization Management Program (FedRAMP). FedRAMP provides a standardized approach for security assessment, authorization, and continuous monitoring of cloud products and services. Due to the complexity of FedRAMP, Ames is helping OCIO develop FedRAMP-aligned Agency approaches for analyzing the security posture of commercial cloud providers and for developing Agency-level "umbrella security plans" to minimize the administrative and security burdens on NASA cloud service consumers.

Another hurdle to cloud adoption is integrating commercial services with existing Agency IT services. NASA's IT Service Operators must be involved as they are essential to architecting and implementing the approaches needed for effective integration. For example, cloud services should work with in-place NASA authentication and access mechanisms, and also provide NASA's OCIO Security Operations Center (SOC) with adequate access and visibility for monitoring, analyzing, and mitigating any threats occurring in the cloud. Ames, with its partners, is operating a pilot on behalf of the OCIO, demonstrating the levels of integration required to provide NASA with secure, efficient, and effective access to commercial cloud services, while also providing proper Agency-level visibility and management oversight.

A third area challenging cloud computing adoption is the business side of the equation, including identifying the best purchasing and payment approaches for gaining access to cloud services. Ames is currently piloting a cloud-service acquisition approach, with a goal of demonstrating how the OCIO can implement a responsive NASA-wide cloud acquisition vehicle, and provide streamlined cloud service ordering and payment processes. Two pilots are being conducted (one by Ames, one by Langley) to demonstrate how the online ordering and funding process can be made as quick as administratively possible today, shorten the timeframe between ordering a cloud service and gaining access to it, and ensure NASA financial and acquisition requirements are still met.

Leveraging early experience gained from the discontinued Nebula cloud project, along with expertise from other NASA Centers and Offices, Ames is actively working with the OCIO to facilitate NASA's responsible, secure, and effective use of cloud computing.

It is exciting to be part of this powerful initiative, in the early stages of cloud service adoption. With its diverse collection of missions and projects, the entire Agency stands to benefit as it learns to leverage cloud computing and gains more experience with this exciting new form of computer services known simply as "The Cloud."

(Continued from page 4.)

down unexpectedly. Additionally, the expectation was to raise awareness of the RRA failover process and DR in general, and validate the NEACC's DR strategy and plan."

The DR technical checkout identified anomalies with server replication. As a result, the failover scenario will be evaluated prior to the next test. Awareness of the RRA failover process and DR, in general, was increased by conducting the test and engaging all lines of business before, during, and after the DR test. Jones noted that the DR test required significant cooperation between network and data center service providers in order to execute the failover/recovery, according to the planned script.

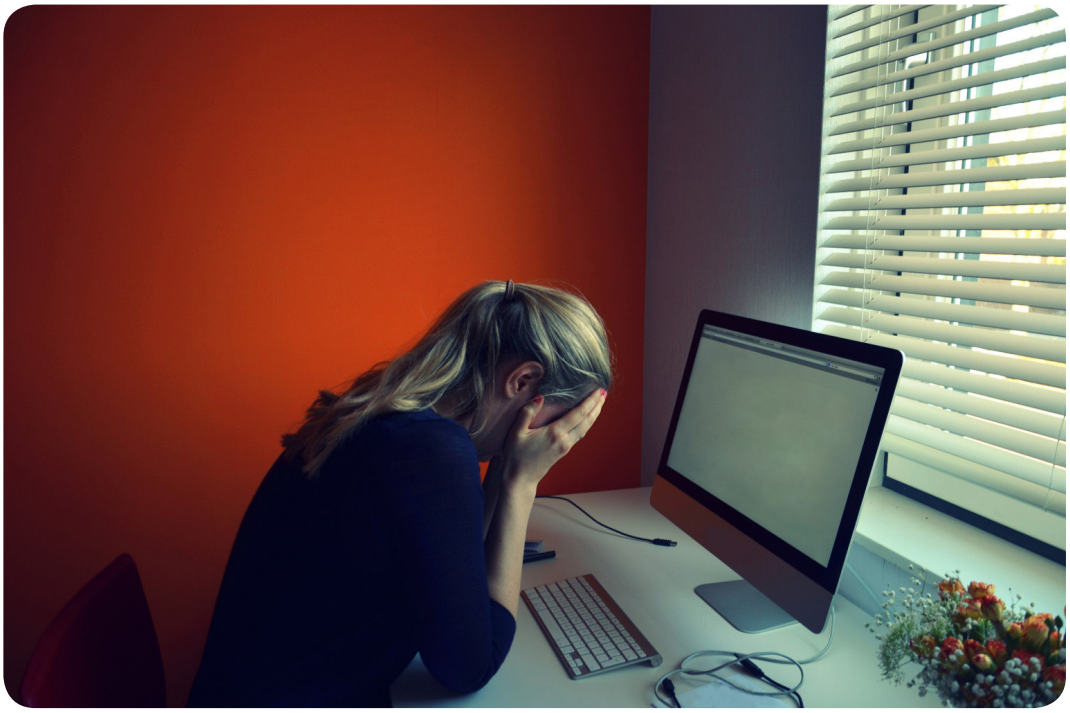
The DRP strategy was validated by successfully recovering target systems within the 72-hour recovery time objective (RTO)/recovery point objective (RPO) window. The actual recovery time was 26 hours. All applications performed as expected and target databases were successfully recovered at KSC.

In summary, Benjamin C. Jones said, "This test was a major milestone and a resounding success! We moved five ITC application environments to KSC and got them back up at Marshall Space Flight Center [MSFC] in less than four days. We met our objectives, captured a great deal of data, and now have a better understanding of what could happen in a disaster. We will sort through the data and develop a post–disaster recovery report with clear steps to address what we have learned."

Cyberbullying—21st Century Violence Attack

By Ericka Brown, Project Support Assistant (DMI)/NASA Information Technology Security Division

Cyberbullying is a term familiar to computer users and IT professionals. Bill Belsey, cyberbullying expert, defines it as follows: "Cyberbullying involves the use of information and communication technologies such as e-mail, cell phone and pager text messages, instant messaging (IM), defamatory personal Web sites, and defamatory online personal polling Web sites, to support deliberate, repeated, and hostile behavior by an individual or group that is intended to harm others."



Children and teens have been greatly affected by this new wave of bullying though a growing number of adults are being attacked as well. Cyberbullying is different from other forms of bullying in that (1) attacks take place using electronic technology, (2) victims do not always know nor likely have had personal encounter(s) with their attacker and (3) victims can be targeted without provocation. Reports have been found wherein bloggers have attacked fellow bloggers due to a disagreement of opinion wherein it was later learned that the blogging cyberbully was experiencing a personal trauma therefore admittedly attacked based on their personal experiences and lashed out at their victim at random. Another report illustrated how a social media user received comments on pictures on their Facebook page which rapidly went from unkind to aggressive and threatening. In each scenario we see that the victims did not personally know nor provoke the cyberbullies. But you can see how using public websites can prompt this very serious crime.

Research shows that children and teen victims are often too afraid or too embarrassed to speak with their parents or others about their experiences with cyberbullies. The tactics used in cyberbullying (malicious language, photographs, and untruths) can have devastating effects on their targets and the healing and/or recovery time can be extensive. Unfortunately, when these attacks are concealed and/or go unchecked too long the victims can lapse into a depression and, in extreme cases, victims have committed suicide.

But, we can help prevent and stop cyberbullying! Eric Dunbar, author of “How to Fight Cyber Bullying,” has outlined four tips that succinctly encapsulate the myriad suggestions offered to protect us against cyberbullies. He’s penned an acronym which we should find fairly easy to remember: NASS. NASS offers a straightforward approach for adults (and youth) in cybersecurity protection:

Never *give out your personal information online (passwords, photographs, home addresses, etc.).*

Always *resist retaliation but do report any harassment to your Internet Service Provider (ISP).*

Stop *responding to the cyberbully as cyberbullying is a form of mental terrorism.*

Save *suspected emails or text messages as these can be used as evidence if bullying escalates.*

If you find you or someone you know has become a victim of cyberbullying, "How to Fight Adult Bullying" by braniac offers tips, a few of which have been paraphrased below:

- *Do not forward malicious electronic message. Reply to sender (or reply all) that the target and their family/friends could be hurt by the message and its distribution therefore the sender should refrain from sending you similar messages in the future.*
- *Block, report and flag any and all electronic messages by a cyberbully.*
- *Go online for resources to help deal with cyberbullying (i.e. National Crime Prevention Council) or create a cyberbullying support group.*

(Continued on page 7.)

(Continued from page 6.)

As a parent you can do the following:

- *Do not erase or delete messages from cyberbullies as it can be used as evidence if a case of cyberbullying is filed.*
- *Use software to block cyberbullies.*
- *Enact privacy settings on social networking pages.*
- *Talk with your children about the dangers of cyberbullying and, if you need help, visit the U. S. Department of Health and Human Services website, www.stopbullying.gov, to obtain more information on this topic.*

The worldwide web is a powerful, dynamic and invaluable tool that can be enjoyed more fully with the proper precautions. Hopefully, these tips will prove useful in your cybersecurity protection. Remember, you are not powerless! Stay informed, do your research and, when necessary, contact your local law enforcement agency who is equipped to work to protect you and your family from further cyberbullying.

Cyberbullying stops when everyone takes a stand to fight back.

Cyber Security Concerns for Parents

Recently Stennis Space Center held a brown bag session titled "Cyber Security Concerns for Parents." The guest speaker was Chief David Allen of the Waveland Police Department. Chief Allen has over 20 years of service in law enforcement. He was formerly a criminal and cyber crime investigator. The Waveland Police Department also participates in a Federal program called the Internet Crimes Against Children Taskforce (ICACT). Chief Allen presented information on sexting, cyberbullying, sextortion, and various popular mobile applications.

Sexting is sending sexually explicit messages or images using a mobile device. Sexting is usually the initial inappropriate social activity in the younger generation. Sexting cases are increasing and participants are as young as 10 years old. This type of activity is a spinoff of cyber bullying and sextortion. Cyberbullying is bullying online via computers or mobile devices. Sextortion is being tricked or threatened into sending illicit pictures or videos.

There are many mobile applications on the iPhone and Android devices used to hide information relating to sexting, sextortion, and cyberbullying. Kik Messenger is a popular mobile application used among early teens. It allows children to send pictures and text messages without using their real names. An application called SnapChat is used to send pictures to other SnapChat users. Those pictures have a 10-second self-destruct function. Other applications, such as Instagram and Vine, are used to transmit sexual content and have been associated with abuse as well.

Many children believe when text messages and pictures are deleted, the information is gone from the device, but this has been proven otherwise. Cellbrite, which is used by the Waveland Police Department, is an application used for mobile forensics. It can be used on any type of mobile and GPS device. This application will circumvent the passcode, if applied, and allow the deleted data to be extracted from the device. The hardware device has plugins and the software have various levels to extract the data.

Session participants received the following final guidance:

- Understand and know your child's mobile device,
- Demand the password of any application your child has on his or her phone,
- Watch for anything with a word vault, lock, or encryption, and
- Always monitor your child's device.

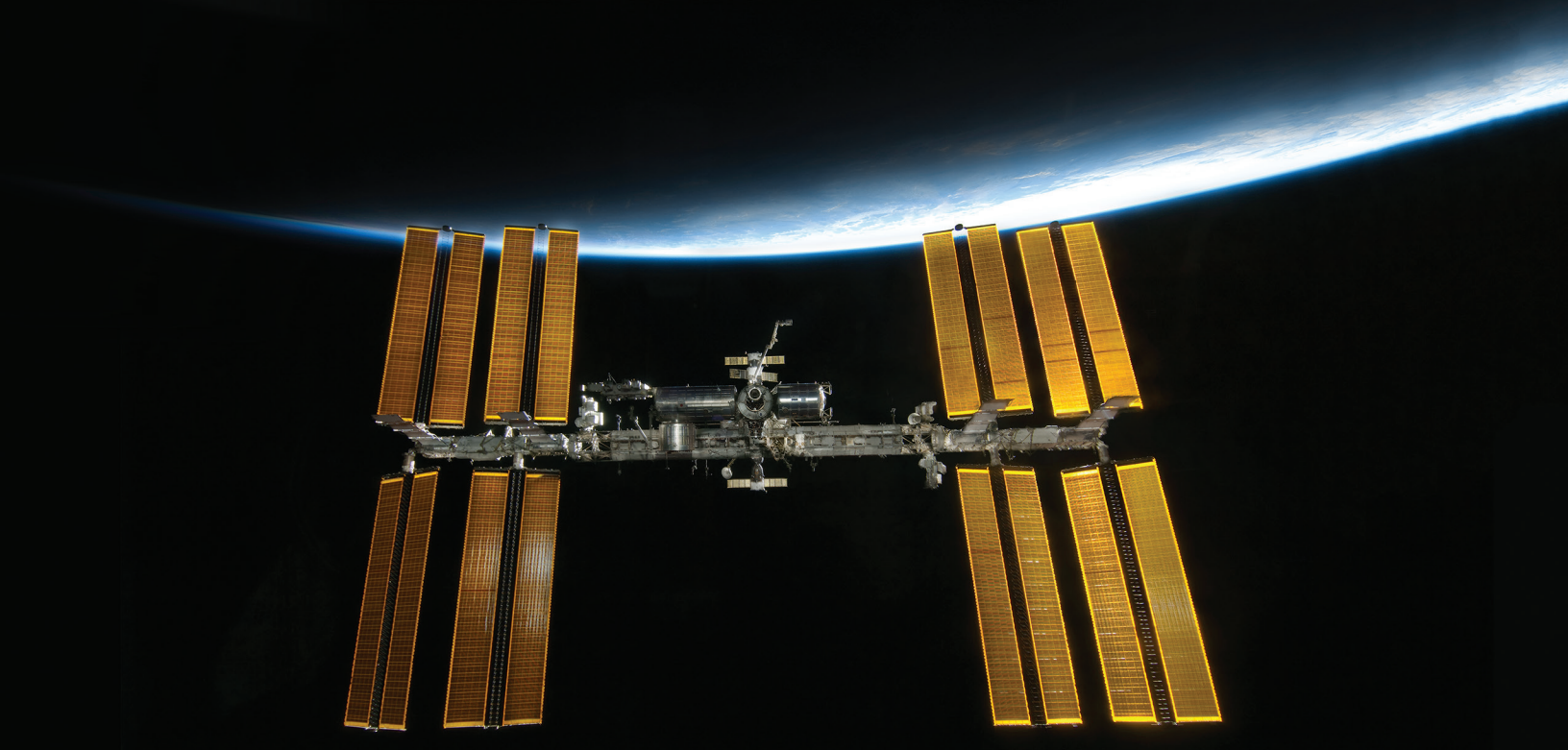
Protection Against Cyberbullying

By Dr. Brenda L. Ellis, Program Manager, IT Security Awareness and Training Center, Glenn Research Center

Cyberbullying is not only inappropriate because it violates appropriate online behavior; it can also be damaging to people. It includes the use of electronic technology and cyberspace to threaten or cause personal harm to others. Examples include sending angry text messages, starting and spreading rumors through e-mails, and posting embarrassing pictures and videos on a social networking site. Once these items are sent or posted, it is difficult to retrieve and delete them. The simplest form can be the use of e-mail or a social networking site to send or post information for personal intimidation. A more extreme case involves gaining unauthorized access to a computer system and using that system to bully another person.

The media often report on teens bullying teens, but adults also engage in the act to damage reputations or to incite desired reactions. What should you do if you are a victim of cyberbullying? It is important to recognize and act quickly and appropriately to reduce the amount of damage or embarrassment. The IT Security Awareness and Training Center (ITSATC) provides tools and activities to educate employees on how to modify one's behavior to produce and maintain a secure working environment. The FY14 Annual IT Security Awareness and Privacy training contains a submodule on scareware and using cyber-security best practices to protect systems from unauthorized access. To further educate employees on how to protect themselves while using social networking sites, ITSATC will be hosting a Webinar on social networking in July 2014.

If you believe you are a victim of cyberbullying in the workplace, contact your supervisor. If you believe that your computer system has been compromised, contact the NASA Security Operations Center (SOC) at 1-877-NASA-SEC (877-627-2732) and your Center's *Chief Information Security Officer (CISO)* immediately. The page is only accessible to NASA employees.



Spot the Station 1 Year Anniversary

Did you know you can see the International Space Station (ISS) over your house? Brighter than the planet Venus, the ISS is visible to more than 90 percent of Earth's population throughout the year around dawn and dusk. NASA's Spot the Station service (*http://spotthestation.nasa.gov*) makes seeing the ISS easy for more than 4,600 locations worldwide. After launching on November 2, 2012—the 12th anniversary of human occupation of the ISS—Spot the Station has gained more than 520,000 subscribers worldwide to its e-mail/SMS notification service, and it is in the top three *www.nasa.gov* sites in overall traffic.

Spot the Station is a collaborative effort between the Human Exploration and Operations Mission Directorate, the Johnson Space Center (JSC) Public Affairs Office, and JSC Mission Operations Directorate. Spot the Station allows users to check upcoming ISS sighting times and locations, as well as the available viewing opportunities for visiting vehicles such as Soyuz, Dragon, and Cygnus. Users can also sign up to receive notifications of upcoming passes via e-mail or text messages up to 12 hours ahead of time. Sign up today and never miss a Space Station pass again!

Keeping NASA Data Safe with Ironkeys

By Ryan Black, NASA LaRC, Information Technology Infrastructure Branch (ITIB)

Keeping NASA's data safe and secure is a top priority at Langley Research Center (LaRC). Our deployment of Ironkey devices, known as the "world's most secure flash drives," reflects our commitment. Ironkeys are Federal Information Processing Standards (FIPS) 140-2 Level 3 validated and utilize Advanced Encryption Standard (AES) 256-bit hardware encryption. They range in capacity from 2 gigabytes all the way to 64 gigabytes, to meet the needs of the user. The Ironkey is also waterproof and protected by anti-malware software, so users can feel at ease when traveling with their data.

At Langley, we have Enterprise Ironkeys allowing for centralized administration. An Ironkey administrator can prevent any mishandling of a lost or stolen Ironkey by disabling or initiating a self-destruct command remotely. Even if an Ironkey is obtained unlawfully without a user's knowledge, the Ironkey itself will self-destruct after 10 unsuccessful login attempts. This centralized management also allows for customer support should a user forget his or her password. The security and protection provided by Ironkey enables our user community to carry the data they need and remain secure with the addition of a managed solution.

For more information about how LaRC is implementing Ironkeys, contact Ryan Black at *ryan.t.black@nasa.gov*.

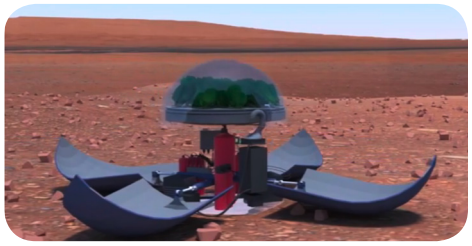
Space Apps Challenge Update

By Beth Beck, Open Innovation Program Manager

NASA and other space agencies around the world are preparing for the third annual International Space Apps Challenge. Participants will develop mobile applications, software, hardware, and data-visualization and platform solutions that could contribute to space exploration missions and help improve life on Earth.

The 2014 challenge will be held April 12–13. Here's a glimpse of a couple of the 2013 winning apps, which represent wide-ranging solutions to challenges on Earth and in space.

The Best Mission Concept, Popeye on Mars, offers a reusable greenhouse for Mars, comprised of a fully equipped aeroponic system to grow spinach over a 45-day mission.



The Most Inspiring App, T-10, saves time for astronauts by using the location of Station and real-time weather data to alert astronauts when conditions are good to snap photos of designated locations on Earth. Astronauts can indicate when they will look out the cupola down on Earth so T-10 app users can wave back at the crew. The T-10 Apps team received "Astro-monials" from Station crew about the need for T-10 on Space Station.

In 2014, half the challenges will come from NASA and represent its major mission directorates and other key investments, and half will come from other organizations, such as space agencies, industry, and global partners. To learn more about the International Space Apps Challenge, visit *http://spaceappschallenge.org*.

Winners Corner

Congratulations to the Open Innovation Team at NASA for being one of eight winners of the 2013 Nextgov Bold Awards. Deborah Diaz, Deputy Chief Information Officer (CIO), along with Nicholas Skytland, led NASA's Open Innovation Team to create the International Space Apps Challenge. This was the largest hackathon to date. The event brought together thousands of people to collectively tackle 58 challenges, create software and hardware, and create data visualizations that addressed real-world problems.

For more information about the awards, visit *http://www.nextgov.com/cio-briefing/2013/07/dozen-agencies-produced-19-finalists-tech-innovation-awards/67661/*.

Diaz has won the 2013 FedScoop 50 Federal Leadership Award. The FedScoop 50 Awards recognize the achievements of 50 of the Federal IT community's best and brightest minds and innovators. This year, hundreds of individuals and programs were nominated, and more than 20,000 votes were cast. The full list of the 2013 FedScoop 50 Award Winners can be found at *http://fedscoop.com/fedscoop-50-awards-honor-dcs-government-tech-elite/*.

Finally, several individuals within the NASA Office of the CIO have received Headquarters Honor Awards. The awards recognize employees who have made significant contributions to the HQ community. Congratulations to everyone for their outstanding accomplishments!

The winners include the following:

Civil Service/Contractor Team—International Space Apps Challenge Team

Exceptional Performance—Jackie Gill

Cooperative External Achievement Award—Karen Petraska

Special Service Individuals—Vicky Essick

IT Infrastructure Integration Program (I3P) Update

Communications Services Office (CSO)/NICS

The I3P Program contract formulation included provisions for ITIL v3 Service Management Framework implementation. ITIL v3, which originated in the United Kingdom's Office of Government Commerce (OGC), is a compilation of best practice guidance for IT Service Management to assist in the improvement of IT service delivery. Under leadership and direction from the Communication Services Office (CSO) Manager, Beth Paschall, CSO readily adopted ITIL v3 to improve service delivery to Communications customers. Utilizing the NASA Integrated Communications Services (NICS) contract, CSO began its implementation of ITIL v3 by establishing a core group of ITIL experts, certified under the Capabilities track of v3. This team provides stewardship for all aspects of ITIL implementation, training, and continual service improvement.

Under the leadership of this group, CSO/NICS has established internal processes and procedures within all areas of the Service Management Lifecycle; to include: Strategy, Design, Transition, Operations, and Continual Service Improvement (CSI). The team ensured success by involving management and support personnel in ITIL v3 training, NICS-specific ITIL process training as well as process ownership, definition, implementation and maintenance. To date, the team has lead implementation of thirteen processes providing an integrated service delivery model. The implemented processes are: Incident Management, Problem Management, Change Management, Request Fulfillment, Service Asset and Configuration Management, Service Level Management, Service Catalog Management, Release and Deployment Management, Capacity Management, Strategy Management, Supplier Management, Service Portfolio Management, Continual Service Improvement.

The remaining ITIL v3 processes are in work and scheduled to be implemented by the 2nd Quarter of CY2015.

End-User Services (ACES)

Instant Messenger/Presence Upgrade Complete: Microsoft Lync 2013 is now the Agency solution for instant messaging (IM) and presence. To learn more about IM/Presence, refer to documentation available at *http://nomadinternal.nasa.gov/nomad/documentation.html*.

Transition from WebEx to Lync: NASA implemented Lync Web Conferencing in early December. Currently, Lync Web Conferencing and WebEx are available to users. The pilot to test the features of Lync 2013 began in late October and ended in early December. NASA extended WebEx for a three-month period to ensure appropriate time for testing. An Agency-wide message was sent with links to training and additional information.

Nighttime Computer Patching: Patching has now moved to nighttime! Software and security patches are now released each Tuesday night between 8:00 p.m. and 2:00 a.m. local time to minimize disruptions during work hours. These patches help protect against security vulnerabilities and maintain current software versions. To take advantage of Tuesday night patching, computers must be powered on, logged off and connected to the NASA network. Please see the ACES Web site for instructions to ensure your system is in the correct state to receive nighttime patching.

OS X 10.8 Upgrades for Macintosh: NASA has completed Mac operating system upgrades from OS X 10.6 to 10.8. and from OS X 10.7 to 10.8.

Enterprise Applications Service Office/NASA Enterprise Applications Competency Center (EASO/NEACC)

The Electronic Forms Initiative (EFI) is replacing the current NASA Electronic Forms System (NEFS) software component (IBM FileNet) with Adobe LiveCycle Enterprise Suite 4. The EFI Initial Operating Capability (IOC), EFI Phase 1, go-live of the platform solution will occur in December 2013.

During FY14, the EFI Final Operating Capability (FOC), EFI Phase 2, key goals are to complete conversion/migration of all forms, scale the platform, replace the NEFS front-end portal, and decommission the IBM FileNet and Center legacy infrastructures. NASA Acquisition Internet System (NAIS) – NEACC Security's latest Hailstorm scanning for the public components of NAIS identified only one Low finding noted for sixteen continuous hours of testing, consisting of 85,000 attacks.

The team has updated the NAIS help page to remove links to Remedy as requested by IT Security (from PWC pen testing). The NEACC BI Team is currently testing SAP Business Objects (BOBJ) in Sandbox using the criteria defined during the evaluation period. BOBJ Versions have been determined and Single Sign On has been implemented for both Analyses for OLAP and Office. Currently, there is an outstanding high vulnerability for the BOBJ server on the security scans. The security team is working with MSFC to provide a fully qualified URL that is needed in order to replicate the issue and to log a message with SAP. This will impact our schedule if not resolved. Detailed planning for the implementation of SAP Business Objects products is in process. The planning includes briefings to the other LOBs, train the trainer dependencies, testing strategy and coordination with 14.2 release activities. Several issues have been identified with the Migration of Cognos to the Windows

platform. The last show stopper was resolved via a hot fix from Cognos.

Enterprise Service Desk (ESD)

The next ESD release is scheduled for June 2014. Design efforts for the release are underway and the team is excited about the upcoming enhancements. Some of these new enhancements include:

- The ability to request a service for a customer at one Center, who is assigned to another, in a TDY status;
- Providing a "service complete" e-mail to a customer who submitted a request through ESRS; Providing a "real-time" status to Knowledge Article (KA) submitters in a published status while opening, viewing or editing a KA;
- Providing additional detail to customers upon completion of service requests;
- Providing customers with Center-specific KA's via advanced search filters on Tier 0;
- The ability for customers to attach comments and to use MS Word copy/paste feature with survey form responses; and
- Providing customers the ability to view the Urgency field from Remedy when viewing incidents tickets.

The start of FY14 marked the 2nd anniversary for ESD on Nov. 1, 2013, moving beyond the transition phase and into a "steady-state" mode of operation. As we look back, the past two years have provided a deeper and stronger relationship with our I3P service providers as we collectively grow the quantity and quality of services being provided to our customers. The ESD Team is able to communicate and work new services, process changes and implement changes in a timelier manner with minimal impact to our customers. Through the past two years, the ESD has welcomed visits from NASA's top management, including: Charles Bolden, Lori Garver, Jeri Buchholz and Larry Sweet to name a few. The ESD Team has seen several successful I3P transitions to include: ACES, NICS, WESTPrime and Tier-1 support to the Space Technology Directorate (STD) and the Standardized Performance Appraisal Communication Environment (SPACE). We look forward to continuing this momentum into the coming calendar year.

Web Services (WESTPrime)

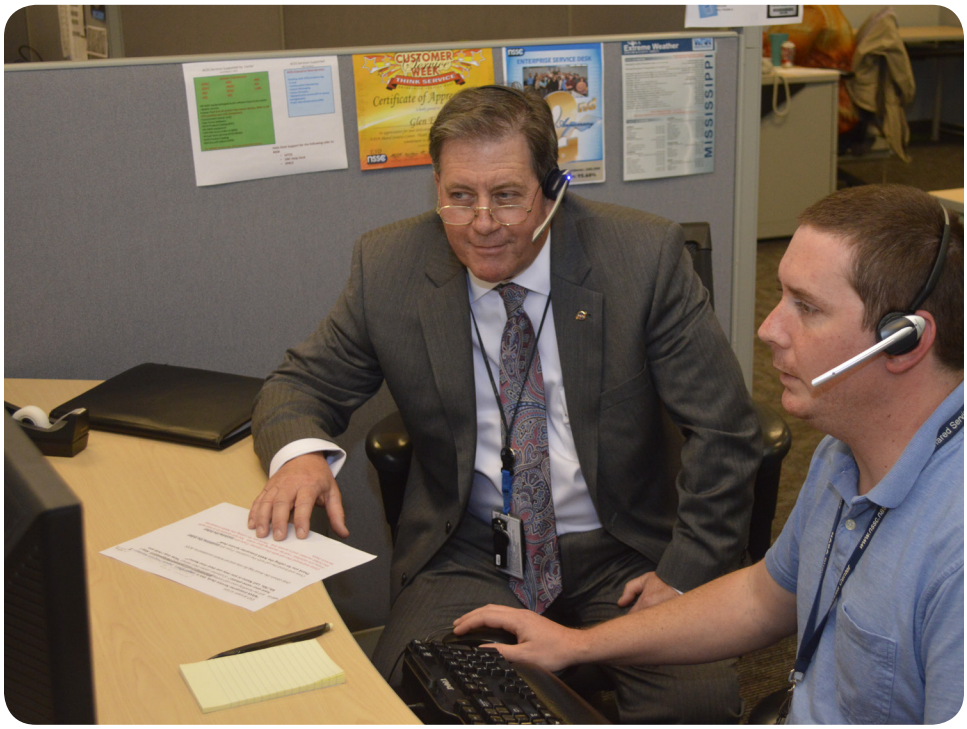
WESTPrime adds the mammoth NASA Engineering Network (NEN) to the list of successful migrations. Teams from WESTPrime and NEN worked to ensure a seamless transition into the WESTPrime Amazon GovCloud environment. Full migration was complete in late August and teams still work closely for ongoing success.

Currently, WESTPrime is building the platform to support the migration of approximately 53 of NASA Headquarters' applications and environments. The services are slated to go online January 14, 2014.

As we head into 2014, WESTPrime will begin to analyze already migrated websites and applications for efficiencies, to include: instance sizing, technical components, changing persistent staging and architectural efficiencies. Standardization of data siloes and repositories will enable WESTPrime to provide cost effective and efficient Platform as a Service (PaaS) and Software as a Service (SaaS), as more and more sites and applications are deployed into WESTPrime's cloud environments.

WESTPrime's Change Management Board has initiated two weekly maintenance windows for site upgrades, updates, bug fixes and enhancements. The weekly scheduled maintenance windows are Thursday's from 8pm – 10pm ET and Sunday's from 12pm-2pm ET.

Sky watchers: WESTPrime supported NASA's Live Streaming Video with over 116,800 simultaneous viewers as the successful MAVEN launch zipped through the sky on November 18, 2013.



NASA CIO Larry Sweet (l) takes a call at ESD.

NASA IT Labs: Behind-the-Scenes Contributions to a Star-Studded Stage

By Kevin Rosenquist, IT Labs Communications Coordinator/Wyle

IT Labs supports NASA by empowering IT Heroes across the Agency to make IT better. In 2011, IT Labs sponsored collaborative projects from Jet Propulsion Laboratory (JPL) and Marshall Space Flight Center (MSFC) that helped evaluate Agency Large File Transfer (LFT) requirements and weigh them against current NASA and industry solutions. At MSFC, Bryan Walls led the "Enhance NASA's Large File Transfer Capability to 100GB Capacity" project to determine if an upgrade to Accellion, the Agency's current LFT solution, would be technically acceptable and the most affordable solution for the Agency's video transfer needs as compared to other similar software capabilities.

Concurrently, JPL's Michael Killingsworth performed a similar analysis with his project "Dropbox for the Enterprise: Secure Collaboration for Mobile Workers," but that focused on LFT from an end-user perspective, versus the specific Agency video needs. Both projects came to the same conclusion. The most effective solution was to upgrade NASA's existing LFT system.

Last December, NASA OCIO, in partnership with the Human Exploration Operations Mission Directorate, upgraded the Agency's LFT solution from 20 gigabytes to 100 gigabytes. With minimal investment, IT Labs was able to support these IT Heroes in finding the best-fit solutions for NASA.

Another innovative IT Labs project from MSFC that is quickly realizing Enterprise service potential is "PIV-Derived Credentials for Strong Mobile Application Authentication," led by MSFC's Jane Maples. By implementing a personal identification verification (PIV)-derived credential capability, NASA users can securely access multiple NASA services from multiple mobile devices while remaining in compliance with Federal IT Security guidelines. This much-needed solution brings NASA one step closer to realizing the vision of "Any device, anywhere, anytime… securely." This is another example of how, with minimal investment and a relatively short development cycle, IT Labs helps further the NASA mission through better IT.

Learn more about IT Labs, these funded projects, and others at *https://labs.nasa.gov* (NDC credentials required).

IT Talk

National Aeronautics and Space Administration

Office of the Chief Information Officer
300 E Street, SW (1225 Eye Street)
Washington, DC 20546

www.nasa.gov