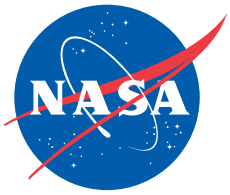
National Aeronautics and Space Administration



IT Talk

July - September 2012 Volume 2 • Issue 3

Balancing IT Security

IT Talk

Jul - Sep 2012 Volume 2 • Issue 3

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

Chief Information Officer
Linda Y. Cureton

OCIO Chief of Staff
John Hopkins

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: 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 CIO

By Linda Cureton

The Agency is responsible for maintaining the security of all of its systems and data to prevent malicious activity and thwart any sabotage of important assets. Recently I had to testify on Capitol Hill regarding theft of an unencrypted NASA notebook computer that resulted in the loss of sensitive data. An impact assessment determined that the loss of that data did not create an increased risk or vulnerability. It was also concluded that the loss of the data contained on the laptop did not impact any NASA mission operations.

Each employee must do their part to protect data. If you were to lose your Government smartphone, iPad, or laptop, what would go through your mind first? Someone now has access to all my important data, my photos? My boss is going to be really mad, and it's going to cost a lot to replace? How about the realization that someone now has access to all your work files and can do real damage that could harm NASA?

NASA takes the issue of IT security very seriously, and we have made significant progress to better protect the Agency's IT systems. In this issue we'll explore how our NASA Centers are going the extra mile to safeguard data.

—Linda

DECOMMISSIONING SPACEBOOK

By Sarah Rigdon, OCIO-NASA Headquarters

Think back three years. In mid-2009, enterprise-scale social media services were not what they are today, yet many large organizations were already aware of social media's low cost ability to address collaboration needs.

Goddard Space Flight Center (GSFC) saw the potential for social media but did not see many third-party applications that met them. Social media could improve business processes, encourage collaboration and information sharing, and build their community of stakeholders and partners. Projects most often fail because of barriers to communication. Social media provides a space to communicate in ways that teams otherwise would not be able to do. Also, NASA's innovation stands to benefit from platforms that facilitate the intersection of disciplines.

Emma Antunes, Web Manager at GSFC, created the homegrown Spacebook social network. It featured user profiles, group workspaces (wikis, file sharing, discussion forums, groups), and social bookmarks. It was especially useful for small teams that needed to collaborate without emailing larger groups. And it was all developed using existing contracts, IT resources, and staff.

In the past three years, the pace at which NASA users have adopted Spacebook is inverse to the pace at which third-party companies have launched enterprise social networking products. Spacebook has provided valuable lessons in user adoption.

The OCIO decommissioned Spacebook on June 1, 2012, and is archiving all user accounts and content. John Hopkins, OCIO Chief of Staff, sees the positive side. "Something that we often fail to do in government is…to not close [applications] when they cease to be viable," he said. Emma Antunes agrees: "We need to be agile and not be wedded to any one thing."

In shutting down Spacebook, NASA uses the lessons learned to build better tools and make better use of existing resources.

ICAM Modernization Project Slated for FY2013

By Kim Edmondson, MSFC

NASA's Oracle Sun Product Suite consists of the Identity Manager, Access Manager, and Sun One Directory. The suite currently provides all of NASA with Identity Management and Account Exchange (IdMAX) workflows for Identity, Credential, and Access Management (ICAM), eAuthentication for access of applications and the Launchpad for user profiles, and the NASA Enterprise Directory (NED). NASA's future ICAM capabilities, be it operations and maintenance or required enhancements, are dependent on continued product support. NASA's current premier support contract with Oracle for the Sun Product Suite will end in 2014.

The ICAM Working Group, led jointly by NASA's Office of Protective Services and Office of the Chief Information Officer, has determined that it is time for the Sun Product Suite to be replaced. The replacement suite will provide NASA with the following:

- Alignment with the Federal ICAM Roadmap (M-04-04, M-05-24, M-11-11). This alignment has a 5-year window for compliance; NASA has developed an ICAM 5-year plan in order to reach this requirement. The Sun Product Suite replacement is one aspect of NASA's plan.
- Innovative technologies that reduce the total cost of ownership, specifically operational costs.
- Cutting-edge technology for long-term infrastructure.
- Improved user experience.

ICAM Modernization Project

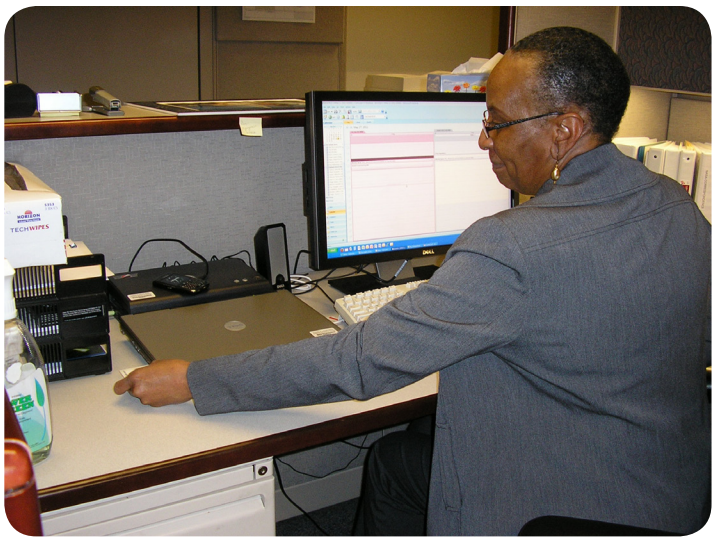
The NASA Enterprise Application Competency Center (NEACC) provides the internal operational and enhancement services of the Sun Product Suite for NASA. The NEACC has been tasked by the ICAM Working Group to begin preparation activities for the ICAM Modernization Project, which is a high priority for the Agency.

The NEACC's Sharon Ing, ICAM Modernization Project Manager says "the project's main objectives during the formulation phase will be to define NASA's requirements and select the Sun Product Suite replacement product by the end of fiscal year 2012." The implementation phase will begin fiscal year 2013 with a targeted completion prior to the end of that fiscal year. Implementation will include installation and configuration of the replacement architecture, migration of system integrations, and migration of business process workflow and data. Ing said, "Center representatives will be required to participate in the project via design reviews and user acceptance tests."

End-User Experience

End users will have an improved experience using a Web 2.0 user interface that allows pop-up screens for ease of use. "The look and feel will be different than today, and it will be more of a mobile solution with an anytime, anywhere capability for some services. To get prepared for this future change, end users need to be attentive to communications that the project should begin distributing early Spring 2013," said Ing.

Look for NEACC's "About Us" on https://bReady.nasa.gov in the months to come for more details on this new NASA project. For more information about ICAM services, check out https://icam.nasa.gov.



Examples of Sun Product Suite capabilities currently utilized at NASA.

Enabling NASA's Mobile Workforce By Securing Application Data

By Jane Maples and Kellie White, MSFC-CIMA

Do you currently use a mobile device to access applications or Web sites? Have you ever stopped to consider whether the information you are sending and accessing is secure? What if you misplaced your phone for a period of time, or worse, what if you lost it? Will unauthorized individuals be able to access those applications installed on your mobile device and initiate transactions on your behalf? NASA's Center for Internal Mobile Applications (CIMA) has worked to ensure the security of data exchanged via any CIMA-provided mobile application. CIMA relies upon Mobile Application Management (MAM), as opposed to Mobile Device Management (MDM), to secure the mobile application. Furthermore, an in-house-developed Secure Mobile Access Point (SMAP) and secure Identity, Credential, and Access Management (ICAM) services are leveraged for authenticating and accessing all CIMA mobile applications. This multilayered security approach relies upon Launchpad for authentication and an application-level personal identification number (PIN) for accessing CIMA-hosted mobile applications. It secures or removes all data at rest and provides a secure channel between the mobile application and the protected NASA enterprise services. Developers can leverage SMAP for their applications to provide the NASA data and services they need in a secure and timely manner.

Features of SMAP:

- Provides a secure mobile public-access point for accessing protected NASA services and data.
- Allows mobile devices outside of NASA locations to access protected NASA services and data.
- Offers full whitelist and blacklist filtering by user, device, application, application version, and Center.
- Provides secure Web proxy services for the CIMA mobile application *Web wrapper, allowing wrapped Web sites to be accessed by mobile devices outside of NASA locations.

The Secure Mobile Access Point implemented by CIMA is effective in securing the mobile application, but CIMA's efforts don't stop there. Currently, CIMA is working with the ICAM team to further enhance the security of the installed mobile applications by implementing an ICAM certificate–based authentication for mobile devices. This additional security measure is expected to be deployed at the end of the calendar year.

While other Federal agencies are struggling with the idea of Bring Your Own Device (BYOD) and how to manage those devices, CIMA's approach to securing your data is to manage the mobile application as opposed to the mobile device. This is referred to as Mobile Application Management (MAM). MAM is application-centric, making it easier to target the things that matter most to NASA—the mobile apps and the inherent data—while leaving the personal device and data alone.

CIMA has presented their MAM approach in various forums with participation from other Federal agencies, with very positive responses. CIMA's MAM solution is looked upon as a viable approach for those agencies not requiring the mobile device to be locked down for security concerns, such as law enforcement agencies.

In addition to CIMA's proven security approach, CIMA also offers a vast array of mobile app consulting, development and hosting, and distribution services. CIMA's catalog of mobile application services and products enable an organization to extend key enterprise information and business processes anywhere, any time through any mobile device. If you would like to learn more about CIMA's security approach and how to take advantage of this approach for your mobile applications, or would like information regarding our service offerings, please contact CIMA by email at msfc-cima@mail.nasa.gov and learn how CIMA is redefining business applications for NASA.

**A Web wrapper is used to deliver an existing Web site as a mobile application.*

Protecting and Safeguarding NASA Information and Information Systems

What if This Were an Actual NASA Headline?

By Evelyn Davis and Valarie Burks, NASA IT Security Division, OCIO

What if this article was the national headline across the United States? Is NASA protecting and safeguarding its information and information systems? Is it possible to protect and safeguard information and information systems 24/7?

How can any Federal agency protect and safeguard information and information systems with the new challenges in cybersecurity? What is the first step in meeting this type of challenge? Over the last few years, NASA has promoted the Annual IT Security Awareness Training, which is a mandate for all Federal and contractor employees. The training is the first step toward teaching the NASA community how to protect and safeguard information. The importance of awareness and various activities such as WebEx training sessions on protecting home computers and learning how to detect, prevent, and safeguard against the various malicious code sent through email and Web sites reinforces training and reminders.

Recently, NASA's Inspector General pointed out in his testimony at a congressional hearing that the Agency had experienced 5,408 computer security incidents in 2010 and 2011. These intrusions resulted in the installation of malicious software or unauthorized access which caused significant disruptions to mission operations, theft of export-controlled data and technologies, and cost the Agency more than $7 million.

In March 2012, the NASA Administrator issued an Agency-wide message on the importance of securing NASA laptops, iPads, and smartphones, which was a major step to strengthen the role of the Chief Information Officer (CIO) and IT security. The Administrator stated, "I take the issue of IT security very seriously—both for our equipment and the information stored on it. Information security maintains the integrity of our programs and ultimately keeps our missions and people safe."

NASA has a wide array of organizational operations that support its missions. These operations may have different risk tolerances. Understanding these differences and the overall risk to the enterprise is challenging in such a large, diverse organization. To date, the Advanced Persistent Threats, called APTs, have compromised computer networks virtually across every Government and department agency and invaded the systems of nearly every major defense contractor. Therefore, the risk level has increased. Our need to protect information systems and the information stored on NASA equipment is greater than ever before.

The rapid growth of the Internet and its various facets, such as social media sites, wikis, blogs, and Web sites, to disseminate information across the masses is no longer novel. This trend has given rise to rogue elements within the cyber community who misuse the privileges of easy access to a wide audience to cause damage to the security and economic fabric of Federal and non-Federal entities.

NASA strives to continue to be a leader in innovation and technology across the Federal sector. To preserve that legacy, cybersecurity at NASA must be an agile, forward-thinking, and cohesive organization thereby allowing NASA to ensure that the projects, programs, and missions are protected and safeguarded against the ongoing global threats from cybercriminals, hackers, and organized groups. To achieve this goal, all NASA employees must take responsibility for safeguarding the security of NASA information. As a united front, NASA employees can protect, prevent, and preserve information and information systems—the key to beginning a cybersecurity transformation at NASA. Cybersecurity challenges over the next decade demand enhanced collaboration, communication, and resources to meet the emerging and ever-changing threat environment.

The Office of the Chief Information Officer and the IT Security Division remain committed to continued improvement of the IT security posture as the NASA IT security program transforms and matures in the 21st century.

Safeguarding Data at NASA Centers

Data has become the lifeline of every business. So it's no surprise that safeguarding data at NASA Centers is an urgent priority. We asked several NASA Centers what they're doing to combat data corruption.

Ames

The Ames Research Center (ARC) IT security team is responsible for managing IT security operations and IT security training and awareness. The IT security team also ensures that Ames complies with Federal Information Security Management Act standards via the Assessment and Authorization program.

Vigilant to cybersecurity threats, the team provides intrusion detection, monitoring, and incident response—often operating behind the scenes—as Ames employees go about their daily tasks. A recent project identified ARC staff and computers as having a higher risk for malicious online and real-world physical threats and how best to protect them. Among other provisions, the team installed advanced data encryption, ensured Public-Key Infrastructure (PKI) credentials were current, and provided training to ensure personnel and proprietary data are secure.

The IT security team provides ongoing awareness activities via Web sites and links to authoritative resources such as presentations and the IT security newsletter. The team hosts a monthly outreach meeting, providing technically advanced team members (i.e., systems administrators) with the latest news on threats, malicious attack trends, Center incidents, and the opportunity for question-and-answer sessions and networking. Security staff proactively meet with the Center's research, science, and CMO organizations to ensure that the office is viewed as a friendly place to seek assistance in protecting the Agency.

The team participates during Cyber-Security Awareness Month, providing residents with informative activities and noteworthy presentations on topics such as "Anatomies of Ownage," "Case Studies of the Painfully Hacked," and "Spot the Phishing Email," as well as other topics from Agency authorities like the Computer Crimes Division of the Inspector General. ARC personnel are invited to participate in "Hacker Jeopardy" and "What's Wrong With This Picture" games. During the annual Ames Chili Cook-off, they lure you into their booth with award-winning chili and the promise of a free gadget if you "just, give them your Social Security Number."

The team is always considering the merits of new security innovations and is currently participating in an Agency project assessing the best way to secure data on personal devices (smartphones, tablets, etc.) to provide freedom of mobility while protecting NASA assets. Vigilance and awareness are key, but if these fail, the ARC IT security team is always quick to act and minimize damage.

Dryden

To support proactive data security, the Office of the Chief Information Security Officer at Dryden Flight Research Center (DFRC) conducts regular audits on all information technology assets. Dryden IT security personnel gather specific data pertaining to each system and record the data in a central audit repository: the Information Technology Security Audit Database. The audit data and results are stored as digital forms within a Microsoft SharePoint application; this application supports digital signatures, attachments, and customizable data entry. Audits are conducted on randomly selected machines from each security plan present at DFRC on a monthly basis. The existing implementation uses role-based account management and supports further development to include automated email notification to relevant parties to facilitate remediation of audit findings. Each system is audited based on existing software, patch levels, NASA baseline configurations, and vulnerability-scan results. Future enhancements to the application include the auditing of user accounts, privileges, and system logs, as well as expanding the focus of audits from configuration to general data protection.

Another way DFRC safeguards NASA data is through the use of the NASA Access Management System (NAMS) tool to leverage enhanced system-specific internal access control. The system owner of the DFRC Lab & Engineering Seats IT system worked with the NAMS subject matter expert to create a customized account management workflow to meticulously qualify and track Lab & Engineering Seat users. The workflow requires a detailed justification for the use of a laboratory or engineering seat (versus a mainstream ACES seat), the user's specific technical requirements, a record of the user's security training, and approval from the user's directorate.

Goddard

Goddard Space Flight Center continues to promote and educate its employees on the importance of safeguarding data, namely Personally Identifiable Information (PII).

For the past two years, Goddard has a road show that is displayed in each building's lobby for approximately two weeks at a time. The display provides a backdrop for the literature available to employees on PII, PKI, International Traffic in Arms Regulations (ITAR), Laptop Security, and Identity Theft, as well as Security Operations Center (SOC) contact information, should a breach occur. During the first quarter of calendar year 2012, 75 posters were placed throughout the buildings at Goddard to raise awareness of data protection, as well breach-response information, which also educates people on how to respond should a

breach occur. Additionally, Goddard utilizes the marquee at the main gates to post brief messages that remind employees to protect their PII. Messages include the following: "ID Theft Can Happen to YOU!" "When in Doubt, Encrypt!" "Thumb Drives With PII Must Be Encrypted."

The Center even orders educational materials from the Federal Trade Commission (FTC) and, most recently, the Credit Union National Association (CUNA).

Glenn

Glenn Research Center's Information Technology Security Office (GRC ITSO) is working aggressively to strengthen the information security posture at the Center and safeguard sensitive data. This is done first by protecting the infrastructure with firewalls and intrusion protection tools. Regular scans are run to detect vulnerabilities and ensure proper remediation. Another way is to identify the personally identifiable information data being collected, stored, and transmitted on the GRC network and ensuring that it is properly protected. In some cases, the amount of PII data being used can be reduced or eliminated.

The process of identifying all PII data that flows through the Center's network can be challenging. One of our processes is to utilize Cenzic Hailstorm to scan Web sites and Web applications for PII data collected on internal and public-facing Web sites. This is done by searching the form fields for input formats and terms, which support PII-type content. For example, a search can be performed to check for formats usually used for Social Security Numbers (SSNs) with the use of a built-in script. Countless other formats can be searched using customized scripts. Approximately 800 external and internal Web sites, applications, and interfaces have been scanned. We have plans to scan another 600 credentialed sites.

Another way we are safeguarding PII data is by working with the developers of all new sites and applications before they go into production. NASA NPR 1382.1 states, "PIAs must be conducted and made publicly available for all information technology (IT) systems, including Web sites, which collect and/or maintain Information in Identifiable Form (IIF) on members of the public." To determine if a full Privacy Impact Assessments (PIA) is required, an Information and Privacy Threshold Analysis (IPTA) is completed, and our developers are asked to complete a worksheet that serves as the initial analysis. The IPTA will determine if the Web application should be provided to NASA Headquarters for further review and assessment.

Headquarters

Cybersecurity is best deployed when everyone is united in the efforts of protecting NASA's sensitive information. NASA Headquarters collaborates with other NASA Centers (and other Federal agencies) to learn and share techniques and best practices for safeguarding data. These techniques are instrumental in ensuring that NASA employees are exposed to current methodologies used for protecting NASA information, which may also be applied for home use.

Recently, NASA Headquarters hosted the cybersecurity awareness presentations, "Protecting Your Privacy" and "Malware Self-Defense." These presentations were made possible through coordinated efforts with the NASA Information Technology Security and Awareness Training Center at Glenn Research Center. Via WebEx, audiences from various NASA Centers were able to collaborate and discuss personal experiences about how they used specific methods for protecting NASA data. The interaction made cybersecurity knowledge-sharing fun and exciting.

NASA Headquarters also provides tailored cybersecurity awareness sessions to organizations during all-hands meetings to address protecting NASA data while performing daily business operations. During these sessions, the focus is on protecting Sensitive But Unclassified (SBU) information (e.g., personally identifiable information) through the use of encryption software; ensuring that hard-copy documents that contain SBU information are properly labeled and routed with NASA's SBU cover sheet; securing mobile devices while on travel; and urging the importance of using loaner devices when traveling abroad.

Cybersecurity awareness is vital when building a foundation for ensuring the availability, integrity, and confidentiality of NASA information and its systems. Once users are aware of how and why it is important to protect NASA data, they can assist with being the first line of defense against cyber threats. Cybersecurity is everyone's responsibility, and awareness is the first step.

Jet Propulsion Laboratory

Protecting the Jet Propulsion Laboratory's (JPL's) networks and data in the face of an increasingly sophisticated threat environment—while also making that data readily available to the scientists and engineers who need it—presents a challenge. To meet that challenge, JPL has implemented a comprehensive IT security strategy, two important aspects of which are the Application Security Program, which infuses IT security into all phases of the development cycle, and Full Disk Encryption, which addresses data protection for a mobile workforce.

Application Security—The Application Security Program focuses on securing applications from hackers who attempt to obtain access to data directly through the application, rather than exploiting vulnerabilities in the operating systems. This program addresses five specific areas:

1. Identify and track applications on both physical hosts and VM environments in the Application Security Registry (ASR). This registry inventories all applications, gathers technical information about those applications for security purposes, and identifies the responsible personnel.
2. Provide developers with application security-scanning tools that scan and analyze Web applications

and source code in multiple programming languages.

3. Work with developers to implement security early in the software life cycle through a lifecycle security checklist.
4. Provide security guidelines for programming languages, security checklists, and fixes for common vulnerabilities.
5. Provide training and awareness through periodic developer security training courses and a quarterly application security newsletter.

Full Disk Encryption—No matter how well we secure our data, our applications, and our networks, a lost or stolen laptop containing unencrypted JPL data bypasses all on-lab security processes and procedures. To protect JPL data on these laptops from unintentional disclosure, all new laptops since 2010 have been delivered with FDE installed. At JPL, Pretty Good Privacy (PGP) software is used to provide Full Disk Encryption. To date, FDE is installed on nearly 4,000 systems, with plans to install it on all legacy laptops by the end of the fiscal year.

JPL's early adoption of FDE has allowed NASA to benefit from lessons learned and given the Agency a significant head start in its own FDE deployment. JPL continues to enhance this effort with plans to further integrate smart card authentication and an expanded effort to protect not only laptops but any device that stores and processes ITAR, PII, and other sensitive data.

A smooth and seamless deployment of this critical technology strengthens JPL's security posture and gives confidence to our external partners.

Johnson

As JSC's Chief Information Security Officer, Mark Fridye's goal is to reduce the security threats through early detection and employee awareness. To make IT security awareness a part of JSC employees' daily routine, Fridye and the JSC IT Security team within JSC's Information Resources Directorate are also doing the following:

- Coordinating IT security road shows for various offices center-wide
- Providing exhibits at key safety events such as the Spring Safety, Health and Environmental Fair
- Conducting periodic webinars on specific IT security topics for employees
- Presenting monthly IT Security safety topics to JSC's senior staff
- Encouraging employees to take all available IT Security training courses
- Emailing monthly safety messages based on the agency's Chief Information Security Officer's awareness calendar, and posting information on the center's internal Website
- Partnering with the center's JSC Safety Action Team and providing IT security tips in their monthly newsletters

To further protect against future threats and loss of NASA data, the team employs a wide range of tools that range from vulnerability scans to anti-virus software installed on employees' computers.

A major issue that poses a risk to NASA's information is loss or theft of mobile devices. The potential loss of data such as Personally Identifiable Information (PII), International Traffic and Arms Regulations (ITAR), NASA proprietary, budget, and technical data can lead to dire consequences such as compromised procurement proposals. Because the impact is unpredictable, JSC IT Security is currently focusing on educating employees on reporting incidents as soon as possible.

Kennedy

During the recent investigation of a lost laptop at the Kennedy Space Center (KSC) it was revealed that most users were not aware of what information was stowed away on their computers. As part of the mitigation efforts to reduce NASA's risk of sensitive data exposure, the Kennedy Space Center's IT security team introduced a Center-wide campaign aimed at raising awareness of a problem that spans all organizations: unprotected sensitive data stored on mobile devices.

The 1st Annual KSC Spring Computer Cleaning campaign kicked off on May 1, 2012. The goals of the month-long campaign were to:

1. Raise awareness of what files are stored on the computer and how to locate them.
2. Reinforce IT Security Training objectives by showing users how to properly protect sensitive data using Entrust.
3. Reduce KSC's potential risk exposure by having Data-at-Rest (DAR) installed.

An intranet Web site was created that consisted of helpful tips and techniques to assist end users in cleaning their devices. It featured a video; a simple cycle to find, organize, back up, delete, encrypt, and maintain files; Frequently Asked Questions (FAQ) pages with step–by-step directions and answers; and links to more information. Posters and flyers were distributed throughout the Center, the video played on kiosks located in main building lobbies, and "helper sessions" were held, where anyone with questions or requiring additional assistance could tap into technical support personnel ready to provide hands-on help for laptops, smartphones, and other devices.

IT security personnel were readily available to present information to organizations at staff meetings. The payback was almost immediate when users found sensitive files or located files they had long forgotten. Feedback was extremely positive with users telling the IT staff that they were going to perform the same checks on their home devices! Most importantly, we helped create a culture change of awareness and users learned how to properly protect sensitive information.

Langley

NASA-issued smartphones and other handheld devices are highly

vulnerable to information theft and online security threats. In fact, smartphones require the same security precautions as a laptop connected to a NASA or public wireless network.

Here are five simple ways to protect your NASA smartphone or any other handheld devices:

1. *Set a password or PIN on your smartphone (NPR 2810.1A, Security of Information Technology).*
   Setting a password is the simplest way to keep your data safe. This makes it less likely that anyone will access your private data if your phone is lost or stolen.
2. *Keep it up to date (NASA-STD-2804L, Minimum Interoperability Software Suite).*
   Make sure you are running the latest smartphone operating system version. Just like a desktop or laptop computer, staying up to date is your first line of defense from hackers and viruses.
3. *Be careful with apps.*
   Make sure to download responsibly: it is safer to use application marketplaces provided by your carrier or phone vendor than to download directly from the Web. Unless you are an information security expert, you should only download apps from the official app stores. Even then, rogue malware can slip through vetting, so have a look at the reviews by other users first.
4. *Turn off WiFi and Bluetooth.*
   The easiest way to stay safe (and conserve battery) is to turn WiFi and Bluetooth off when you aren't using them. When you use Bluetooth, make sure it is in nondiscoverable mode. When you use WiFi, always try to use an encrypted network or use a VPN. Otherwise, hackers can easily "sniff" your data out of the air. Remember, if you aren't using WiFi or Bluetooth, you should turn off wireless communication features to prevent hackers from gaining remote access to your smartphone.
5. *Back up your data.*
   If your smartphone is compromised, sometimes the only way to be sure that the virus is removed is to completely wipe its memory. Also, before leaving on a trip, be sure to back up your data—it only takes a few minutes. If you happen to lose your phone, notify the NASA Security Operational Center (SOC) at 1-877-627-2732 or via the SOC email address at soc@nasa.gov as soon as possible. Remember, you should make regular backups to preserve your information.

Marshall

The Marshall Space Flight Center (MSFC) IT security leadership team recognizes the importance of effectively providing data protection for both the Center and the Agency. To provide holistic information assurance the data must be considered the true asset to steward and protect. Therefore, we are actively developing strategies, architectures, and solutions centered on identifying and protecting data as an asset throughout its life cycle.

Per OMB Circular A-130, Management of Federal Information Resources, the term "information life cycle" means the stages through which information passes, typically characterized as creating or collecting, processing, disseminating, using, storing, and disposing. MSFC IT security and data protection strategies are being implemented to address risk throughout the enterprise information life cycle. Some of these efforts include but are not limited to the following:

- Information Security Governance, Risk, and Compliance Framework Development—The data-asset-focused framework being implemented to address asset identification and inventorying, data-sensitivity requirements management, security operations, and IT risk management.
- Continuous Monitoring Lifecycle—The strategy and architecture being developed to efficiently and effectively manage continuously monitored life-cycle activities that leverage people, processes, and technology. This is focused on data-centric approaches commensurate with a risk tolerance based on National Institute of Standards and Technology (NIST) requirements and standards.
- Privacy and Data Protection Program Management—MSFC is continuously integrating information privacy management and data-protection processes and procedures into the System Development Life cycle and other enterprise activities. This approach includes continuous monitoring and incident-response efforts in order to provide more detailed sensitivity and risk factors to data while addressing threats, vulnerabilities, and incidents.

Stennis

Stennis Space Center (SSC) protects its data with a combination of technical and administrative controls. We have implemented a strong continuous-monitoring program using both Agency- and Center-provided tools. Since the installation of the M86 Web proxy, our incident rate originating from Web-surfing activity has decreased significantly. SSC has also implemented an aggressive vulnerability scanning program that identifies system vulnerabilities and helps discover all devices on the network, both legitimate and rogue. Our integration of a risk and compliance management system that complements the Risk Management System (RMS) has allowed SSC to streamline our Authorization and Accreditation (A&A) program. As a result, the enhanced Plan of Action & Milestone (POA&M) tracking helps us identify and mitigate weaknesses in a timely manner. SSC has also been consolidating hosting locations, which brings more data into a tightly controlled environment that provides greater security, redundancy, and configuration control.

Collaboration that Pays NASA Back

By John Sprague, End User Service Executive, & Ken Freeman NASA Security Operation Center Operations Manager

Your NASA Operational Messaging and Directory Services (NOMAD) email and the NASA Security Operations Center (SOC) teams are working together daily to "prevent" security-related incidents and avoid lost productivity.

A recent NOMAD Summary Report revealed that during a 6-month period NASA received over 240,000 phishing attempts. As defined by Wikipedia, "phishing is attempting to acquire information (and sometimes, indirectly, money) such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication."

Communications purporting to be from popular social Web sites, auction sites, online payment processors, or IT administrators are commonly used to lure the unsuspecting. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake Web site whose look and feel are almost identical to the legitimate one.

The SOC frequently requests NOMAD to block emails based upon an email's "fishy" subject line. The emails have links to Web sites where malware can be downloaded to the users' computers or contain bogus attachments. Many times, the SOC will first learn about a hostile email when a user reports it to the SOC as a possible phishing attack. Other times, the SOC receives third-party information from numerous government and commercial sources.

Using a simple cost-avoidance estimate model, the following calculations can be made:

240,429 emails at 3 percent = 7,212.87

7,212.87 × 10 hours of nonproductive time = 72,128.7 hours

$7,212.87 × 100 hours labor to fix = $7,212,870 in avoided lost productivity costs just in this 6-month period. Not included in this calculation were any lost data, which could be priceless.

The cost-avoidance estimate is based upon a hypothesis that 3 percent of users who receive an email with hostile links to malware would go the "whole nine yards" and unintentionally infect their computers, requiring that their systems be pulled off line. The Center Incident Response Teams would review the system, and the System Administrator would then have to rebuild the system with the standard load and the user's backup files before the Center declares the system safe. This process estimates the user being nonproductive for 10 hours and the average full cost of an employee's time at $100 per hour (a rough figure commonly used). The 3 percent figure is based upon one Center's experience where a well-crafted email message was sent to all users at a Center. Before it was stopped, about 3 percent of the users receiving the message went the whole nine yards and opened the link and downloaded the malware.

If you suspect you have received a phishing email, don't click the link or open the attachment—report it or delete it, and we'll all be the better for it!

For more information on SOC operations, please visit the SOC Web site at https://share.nasa.gov/it/security/ops/Pages/default.aspx. Please note this is a NASA-internal site.

NSSC Relocates Data Center to NCCIPS

By Mae Mangieri, Communication Specialist, NSSC

As the NASA Shared Services Center (NSSC) continues to grow, so does the need for its availability to NASA users. Twenty months ago, the NSSC began planning to improve the availability, reliability, and serviceability of its data center. On April 29, 2012, the NSSC completed this upgrade by relocating from its Tier-1 data center to the National Center for Critical Information Processing and Storage (NCCIPS) facility, located at Stennis Space Center.

NCCIPS is a NASA-managed, Tier-2+ shared data-services facility serving multiple Federal agencies, and providing robust electrical, cooling, and bandwidth infrastructure necessary to support the secure processing of critical Federal information.

"Over the past five years as the NSSC has continued to grow and mature, it became evident to us that our data center was not up to the standard necessary for the NSSC to be able to provide continuous services to all of our customers," said NSSC Deputy Chief Information Officer (CIO) Jim Walker.

The NSSC brought together four teams—CSC (formerly Computer Sciences Corporation), Science Applications International Corporation (SAIC), Hewlett-Packard Enterprise Services, and the NCCIPS staff—to work in collaboration to ensure that the NSSC's IT infrastructure was enhanced, and that the transition was completed efficiently with minimal interruption to services.

"We were looking for a way to provide additional physical security and greater protection from hurricanes and the unexpected, especially since 'Go Live' of NASA's 24/7 Enterprise Service Desk (ESD) at the NSSC," said CSC Project Manager Tommy Thompson. "We also wanted to allow for redundancy of both of our networking and power distribution as well as all the advantages that come from Tier 2."

The impact of this move is not insignificant. The data center's relocation, enhanced infrastructure, and ability to better withstand natural disasters better postures the NSSC for around-the-clock support under all adverse conditions. Critical personnel, financial, IT, and procurement data is now maintained in a nationally recognized and secure data center.

I3P Update

Communications Services (NICS)

On April 1, 2012, the Communications Services Office (CSO) and the NASA Integrated Communications Services (NICS) contract completed transition at all NASA Centers. Many thanks are offered to everyone who contributed to a successful transition, especially the Center Transition Managers. With the "transition" stage complete, the "transformation" phase of the NICS contract is now underway with a number of transformation activities in development to enable the vision of the CSO and Information Technology Infrastructure Integration Program (I3P). Examples of these activities include the development of a long-term service-delivery strategy for the local area network (LAN) and Agency voice services while incorporating the near-term needs of the Centers and our customers. Working groups with both CSO/NICS and Center/customer participation have been initiated for both of these tasks.

During the transformation phase, collaboration among the Centers, customers, Office of the Chief Information Officer (OCIO), and CSO/NICS will be key to the mutual achievement of the Agency, Center, customer, and CSO's goal of creating a secure, high-performance, integrated, and efficient network environment.

End-User Services (ACES)

All Centers have been transitioned to the Agency Consolidated End-User Services Contract (ACES). The End-User Services Office (EUSO) is working diligently with the Centers and Hewlett-Packard Enterprise Services (HPES) to resolve issues related to services provided by ACES. A weekly meeting is held to review action items and issues with the Agency CIO's office and ACES subject matter experts (SMEs).

Office Communicator Web Access is a new service available under ACES. Users can now use Instant Messaging (IM) without the Office Communicator or Mac Messenger client. Office Communicator Web Access allows you to use IM through a Web browser. Users do not need to be on site or connected to a NASA Center through a virtual private network (VPN) in order to use this service. The only requirement is to use a Java-based browser such as Internet Explorer, Firefox, or Safari.

Data-at-Rest (DAR) encryption is being implemented on laptop computers and desktop computers containing sensitive information. A DAR general outreach message has been sent Agency-wide. In July, general deployment of DAR begins for computers containing sensitive information.

The ACES team worked through the backlog of Requests for Quotes (RFQs) within the Service Requests (SRs) system. There is no longer a backlog of RFQs.

A new ACES Steady State Communications Process has been implemented in which all outreach messages are grouped into four categories (alert, action, advisory, and awareness) in order to ensure consistent messaging to our customers on all ACES-related topics. The ACES News, a monthly e-newsletter that provides information to NASA end users about ACES activities, products, services, and processes, has received great reviews. This is just one example of how the EUSO provides end-user-focused messaging.

Enterprise Applications Services (EAST)

The Enterprise Applications Service Office (EASO) has been in close contact with its service board—the Enterprise Applications Services Board (EASB)—over recent weeks in an effort to provide Rough Order of Magnitude (ROM) estimates for 2013 initiatives by Line of Business (LOB). The EASB will make prioritization recommendations to the Business Systems Management Board, which has decisional authority over the budget that comes to the NASA Enterprise Application Competency Center (NEACC) and which funds the Enterprise Applications Services Technology (EAST) contract.

With shrinking budgets, the governance decisions and prioritization of Agency IT initiatives will provide critical guidance for the NEACC as the first Option Decision Package milestone approaches for EAST. The NEACC's scope continues to expand, with the ongoing transition of applications supporting the NASA Office of Education (OE). The completion of that transition in September 2012 will introduce a new line of business to NEACC operations, allowing OE to leverage exciting reporting, dashboard, and mobile application capabilities. The OE initiative is one of many ongoing or upcoming projects and initiatives in the NEACC's pipeline. Key among those projects and initiatives is the continued build-out of critical application capabilities in the Integrated Collaborative Environment (ICE)—Product Lifecycle Management Line of Business on the robust and secure ICE-enhanced infrastructure in support of the tri-program missions. To further enable ICE, a cross-Agency team of functional experts has just wrapped up a series of workshops to define common, flexible configuration management and detailed design processes to support tri-program needs. The NEACC team is beginning to implement these new process capabilities in WindChill 10.0 and will continue to build them out in a series of "sprints" running through the summer and into the fall of 2012.

Enterprise Service Desk (ESD)

Over the last 6 months, the ESD has been providing the NASA I3P community with a self-service Web portal (Tier 0), service request capability, and incident-submission and notification-tool-subscription capabilities. Over this period of time, we have seen customers become more familiar with ESD and its various offerings. This month, Systems Requirements Reviews (SRRs) occurred for ESD 1.2 and ESD enhancements.

ESD 1.2 will implement two critical Information Technology Infrastructure Library (ITIL) modules: I3P Change Management and I3P Problem Management. The I3P Change Management module will be utilized to manage the process for controlling changes to ensure they benefit customers and the I3P program and are implemented without interruption of services. The Change Management process may refer to system changes or process changes. There will be change categories for prioritization purposes (process, service, governance, technical), and the module will outline the roles and responsibilities necessary for efficient change implementation.

I3P Problem Management involves root-cause analysis to determine, reduce the impact of, and potentially resolve (via Change Management) the cause of incidents. This is separate from the Incident Management process, which returns service to the user. Problem Management will be both proactive and reactive. Reactive Problem Management minimizes the impact of incidents happening now, while proactive Problem Management will rely upon heavy utilization of trend analysis and event management to prevent incidents.

Both modules are based on ITIL v3 and will utilize the same tool set used for the 1.0 and 1.1 elements of ESD. These modules will be primarily utilized by OCIO points of contact within the I3P program and Center CIO offices. The Operational Readiness Review (ORR) for ESD 1.2 is expected to occur in October.

At the same time, the ESD project team is working on system enhancements that will benefit CIO personnel, I3P providers, the I3P business office, and I3P customers. The enhancements are a collection of miscellaneous improvements to the basic ESD implementation. Based on customer feedback and lessons learned from production use, slight modifications to the initially requested design are necessary to enhance the usability of the tool for NASA users. Several aspects of the tool will be modified during this project, including interface design data being exchanged with the I3P contracts, features of notifications and surveys, and the availability and display of information on the self-help Web site. Enhancements will occur continuously throughout the project.

Web Services and WESTPRIME

Web services are continuing under the current vendor, whose contract has been extended through April of 2013. Current services include the following features:

- Web-content delivery
- Web site development
- Content management
- Bandwidth management
- Search capabilities
- Collaboration services
- Web hosting

NASA is also shifting to a new Web-services model that uses Amazon Web Services for cloud-based enterprise infrastructure. This cloud-based model supports a wide variety of Web applications and sites using an interoperable, standards-based, and secure environment.

The acquisition strategy for Web Enterprise Service Technology WESTPRIME is to compete this requirement among several sources on the U.S. General Services Administration (GSA) Federal Supply Schedule (FSS) Information Technology 70.

The solicitation is scheduled to be released in the July to August timeframe. NASA expects to release the Request for Quote (RFQ) for WESTPRIME by August 2012 and make an award selection by April 30, 2013. An industry day forum will be conducted shortly after the release of the solicitation to discuss specific information about the proposed acquisition necessary for the preparation of proposals. Topics will include the proposed contract type, terms and conditions, and acquisition planning schedules; the feasibility of the requirement, including performance requirements, statement of work, and data requirements; the suitability of the proposal instructions and evaluation criteria, including the approach for assessing past performance information; the availability of reference documents; and any other industry concerns or questions. This forum will be open to the public.

The goals of the WESTPRIME contract are to:

- Enhance business and technical agility;
- Eliminate vendor-specific dependencies;
- Drive down operational overhead for Web presence;
- Drive down the cost of custom Web and on-demand services for missions, programs, and projects;
- Increase NASA IT security;
- Explore collaborative services across NASA Centers; and
- Improve online customer service delivery through innovative technology.

IT Operations Handbook

The I3P IT Operations Handbook (ITOH) is now available for use by the Information Technology Infrastructure Integration Program (I3P) support personnel. The handbook covers a variety of topic areas including I3P governance, operations management, and communications. Users will find that the ITOH contains links to many supporting documents in order to provide timely information. IT and resource approvers will find the handbook especially helpful since it outlines critical areas that support their work.

Why do we need a handbook? I3P focuses on comprehensive IT service management. It is more than just I3P contracts. The processes, procedures, and governance have all changed in concert with the I3P contracts to provide enterprise IT services that meet customers' needs. The ITOH provides information about the processes, procedures, and governance that customers and those with an I3P role need. The ITOH is a living document that will evolve over time.

The difference between the ITOH handbook and documented procedures is that it provides links to documented Standard Operating Procedures (SOPs). Rather than a static list of SOPs, the ITOH is organized into sections to help users find the procedure they need. While the ITOH is presented in an outline form today, future plans include adding an explanatory text to assist in the navigation of the document.

The handbook is always evolving. You may send your feedback to Corinne Irwin (corinne.s.irwin@nasa.gov) or John Kasmark (john.t.kasmark@nasa.gov). The document is available at http://ocio.ndc.nasa.gov/public/I3P%20ITOH/Forms/AllItems.aspx.

2012 Technology Summit

By Irene Wirkus, NASA Emerging Technology and Desktop Standards

Recently, NASA's Emerging Technology and Desktop Standards (ETADS) team hosted its 2012 Technology Summit. The Summit provided a forum for technology leaders to share insight on industry trends and brief NASA on product portfolios, roadmaps, and corporate direction. Participants in this year's Summit included Apple, AT&T, Cisco, Dell, Fiberlink, Google, Hewlett-Packard, Intel, Lenovo, Microsoft, Research in Motion Ltd. (BlackBerry), Verizon, and VMware.

The Summit, held at the Glenn Research Center in Cleveland, OH, was open to the entire NASA community and available via WebEx videoconferencing for those who could not attend in person. Vendor participants were asked to focus on the following topics during their presentations:

- Incorporating technologies that support, enhance, and secure mobile devices and the remote worker.
- Incorporating technologies that enhance interoperability and collaboration.
- Emerging and submerging industry standards.
- Emerging trends and disruptive technology.
- Upcoming changes to the personal computer platform.
- Establishing a timeline for adoption of Internet Protocol, version 6 (IPv6).

The Summit offered a unique opportunity for NASA to meet with industry IT leaders and discuss ways to meet the IT challenges facing NASA and the Federal Government. The knowledge gained from this exchange helps ensure that future iterations of NASA's Desktop Computing Standards, NASA-STD-2804 "Minimum Interoperability Software Suite" and NASA-STD-2805 "Minimum Hardware Configurations," continue to provide NASA users with desktop configurations consistent with industry trends and NASA requirements. The Summit also provided NASA personnel with an opportunity to gain awareness regarding cutting edge technologies and services that can assist them in their pursuit of mission and project goals. Finally, the Summit served to promote an open and ongoing dialogue with industry leaders so they can better tailor their technology suite to be attractive to Agency customers and supportive of NASA's goals and obligations.

For more information about the 2012 Technology Summit, along with video highlights, WebEx recordings, and vendor presentations, visit the ETADS Web site at https://etads.nasa.gov.

Cisco demonstrates its mobility solutions.

Intel briefing at ETADS.

Hewlett-Packard presents the Z1 "All-in-One" Workstation.

International Space Apps Challenge

By Nicholas Skytland-Open Government Initiative

The International Space Apps Challenge joined together over 2,000 people around the world in creating solutions of global importance related to spaceflight. The code-a-thon-style event took place in cities on all seven continents on April 21 and 22, 2012. The event was part of the United States' commitment to the Open Government Partnership, a multilateral initiative between 55 nations pledging to promote transparency, participation, and collaboration between governments and citizens. The International Space Apps Challenge upheld the pact to "promote innovation through international collaboration."

Space exploration was the ideal catalyst to foster this culture of innovation, and NASA, in collaboration with 9 government agencies and 90 other organizations, hosted the inaugural challenge in 25 cities, 17 countries, and online. The event brought together 2,083 registered participants ages 16-70 to address 71 challenges grouped into four categories including open-source software, open hardware, citizen science platforms, and data visualization.

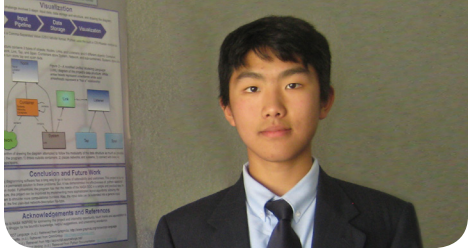
More than 100 unique solutions were developed in less than 48 hours during the event. All solutions were developed in a completely open-source environment, and each has its own unique potential to go even further to address world and space technology challenges.

In addition to the technology developed, the event itself generated considerable media coverage for NASA, resulting in more than 100 articles, including being highlighted on the front page of the British Broadcasting Corporation's (BBC's) Web site. Gov 2.0 Radio (http://gov20radio.com/spaceapps/) provided special coverage for the event that included 45 interviews with organizers, experts, and participants from all locations. The entire event was streamed online to thousands of people around the world, and although it's hard to measure the total viewership, the Twitter stream alone generated 3.3 million hits.

The International Space Apps Challenge was an event unlike any of its kind, and it set the stage for even more technology development through international collaboration in industries around the world.

For more information visit http://spaceappschallenge.org.

Passion Turned to Productivity at NASA Ames Research Center (ARC)



By Penny Hubbard, CIO Communications, AMES

Computer science is a passion for Evan Ye, an INSPIRE* intern at ARC during the summer of 2011. He's always been intrigued by "how a mere snippet of code can harness a computer's power," he said. Building on this fascination, Evan learned how to command computing power, turning it into a success story at NASA, writing an autonomous network diagramming program.

As Evan honed his curiosity into programming skills, he learned C and Java languages, pursuing more sophisticated programs. He learned a gaming program in middle school, discovering that he loved "figuring out how to make objects in the game act appropriately." As captain of his high school chess club, Evan combined two of his favorite activities by writing a full-fledged chess-interface program. He had many setbacks writing the code, but his determination saw him through.

Evan wanted a practical scenario to utilize what he had learned, "to focus not only on theoretical, but also on applied aspects of school subjects." He was involved in INSPIRE, a NASA educational program for high school students interested in science, technology, engineering, and mathematics (STEM) careers. He also went through an extensive application process to become an intern, and he was paired with mentor Dr. S. Terry Brugger at Ames.

Dr. Brugger provided the project description, skills, and aptitude needed for the project, as well as the testing for the final program. Evan worked with Dr. Brugger to evaluate existing processes and gather requirements for network diagramming. Initially, it was a time-consuming, manual-entry process. He wrote a program that takes NASA network data from a spreadsheet and automatically produces a network diagram from it. The significant productivity enhancements saved days of effort for Dr. Brugger, and there is interest in using Evan's autonomous network diagramming program for other systems across the Agency.

Evan had the amazing opportunity to utilize his programming skills in a real team environment, while learning about NASA, working with teams, and opening doors to other programming opportunities. NASA gained a valuable and time-saving program—part passion, part inspiration, and all Information Technology.

Since Evan interned at NASA, he's graduated with honors in the top 5 percent of his class and received the President's Education Award—sponsored by the U.S. Department of Education. He will be attending the University of California, Berkeley, this fall, studying electrical engineering and computer science.

*For more information about the Interdisciplinary National Science Project Incorporating Research and Education Experience (INSPIRE), visit http://www.nasa.gov/offices/education/programs/descriptions/INSPIRE_Project.html.

National Job Shadow Day

Recently Stennis Space Center and the NASA Shared Services Center held a National IT Job Shadow Day event. About 170 high school and elementary girls from area schools visited Stennis Space Center to participate in a day of activities to promote careers in science and mathematics. Stennis Space Center Director Patrick Scheuermann welcomed the girls to the rocket engine test facility, and NASA Deputy Administrator Lori Garver addressed the group in broadcast remarks. Participants then attended a variety of workshop and seminar presentations, including IT speed mentoring, a cryogenics demonstration and a "Dress for Success" fashion show.

The mentoring session began with remarks by the SSC CIO, Dinna L. Cottrell and the NSSC Deputy CIO, Jim Walker. The IT speed mentoring session was conducted by employees from the SSC's and NSSC's Offices of the CIO and supporting contracts. The mentors gave brief descriptions of their background, education and job responsibilities which allowed time for the participants to ask questions. The mentoring session was followed by tours of IT facilities. The girls left with a better understanding of how information technology is used at NASA and with a broader idea of what they can do beyond high school.

The day-long activities concluded with a keynote address by Retired U.S. Army Col. Sheila Varnado, executive director of R3SM (Recover, Rebuild, Restore Southeast Mississippi), and a simulcast presentation from NASA Headquarters.

170 high school and elementary girls from the area schools

Stennis IT Expo

On June 21, 2012 Stennis Space Center held its 8th Annual Information Technology (IT) Expo which was sponsored by the Center's Office of the Chief Information Officer (OCIO). The event highlighted services and capabilities are available through the NASA SSC OCIO and its support contractors. They include ASRC Research and Technology Solutions (ARTS) which provides Information and Technical Services (ITS), HP Enterprise Services, which provides Agency Consolidated End User Services (ACES); and Science Applications International Corporation (SAIC), which provides support for NASA's Integrated Communication Services. The NASA Shared Services Center (NSSC) also showcased the Agency Enterprise Service Desk (ESD).

An executive session launched the annual Information Technology Expo with opening remarks from SSC CIO, Dinna L. Cottrell. The speakers at the executive session included Senior Vice President and General Manager of HP, Marilyn Crouther, who presented on HPES Capabilities, Dr. Pedro J. Medelius, Chief Technologist for ASRC Research and Technology Solutions (ARTS), who presented ASRC's IT Expertise and Strategic Capabilities; and Bobby Collins, Senior Engineer / Collaboration Technologist with SAIC who presented on "Video Teleconferencing."

Stennis CIO Dinna Cottrell tours booth

A seminar entitled "What is Data At Rest (DAR)" was offered to participants of the IT Expo. DAR protects NASA's data on computers while they are powered off. All Agency laptops and desktop computers that store sensitive information will receive DAR by September 10th 2012. For more information go to http://sscintranet.ssc.nasa.gov/specialfeatures/dar.asp (this link is internal to Stennis employees only).

IT Expo attendees also obtained information on Applications Support, IT Security, Video Production and Audio Visual Services, Records and Documentation Management, SSC Online Web Ordering Service (OWEB), and the Stennis Data Center.

Product information was provided by several ACES HP Enterprise Services vendors which included Apple, AT&T, Citrix, Konica, KST, Lenovo, Microsoft, Verizon, Cisco, and Symantec.

The IT Expo provided a great opportunity for SSC employees, NASA, resident agencies, and contractor employees to meet with technology providers and obtain details on their products and services. Door prizes were drawn for attendees who registered. For more information on the highlighted services or capabilities, call the SSC OCIO at 228-688-6246.

National Aeronautics and Space Administration

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

www.nasa.gov