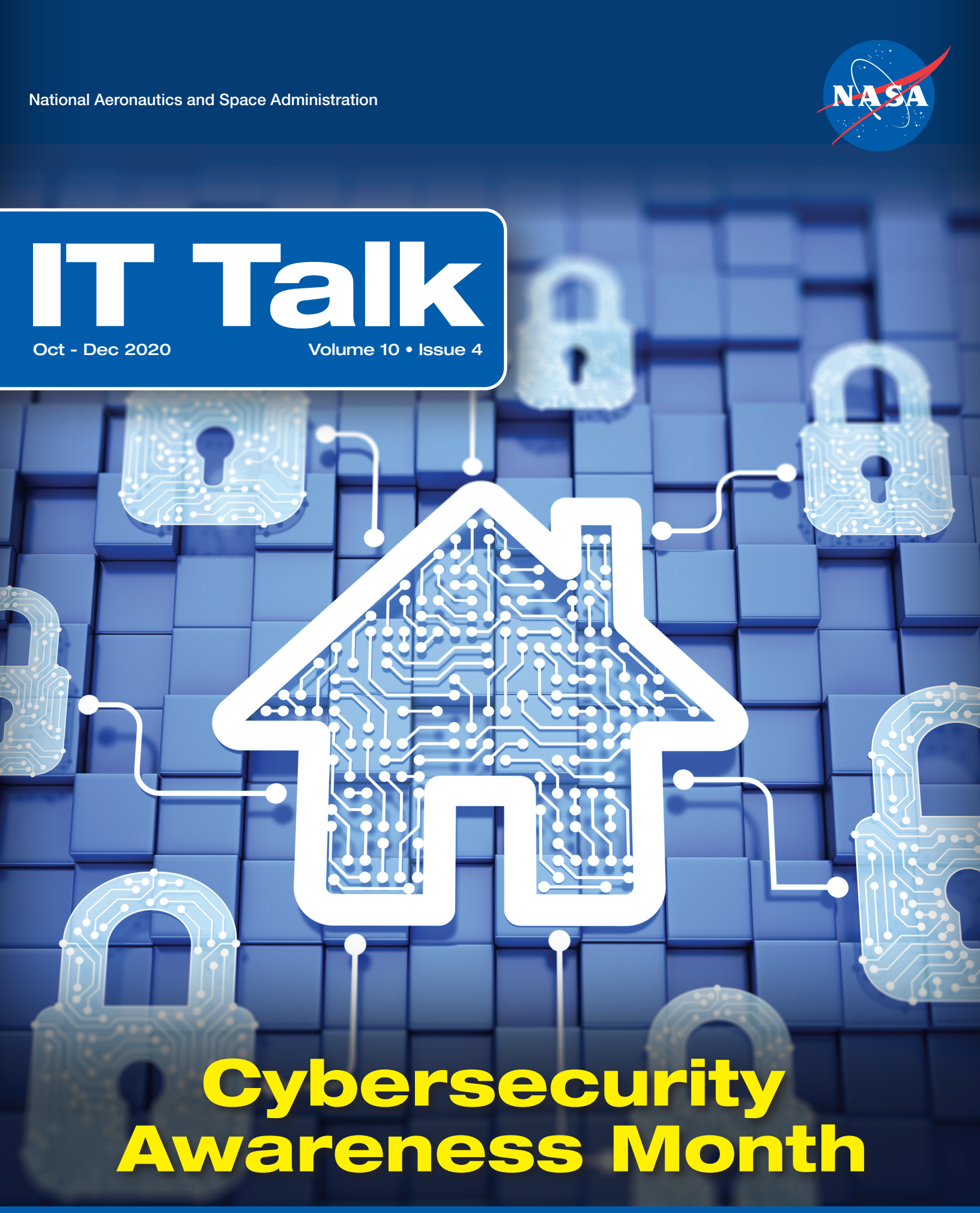
National Aeronautics and Space Administration

IT Talk

Oct - Dec 2020 Volume 10 • Issue 4



Cybersecurity Awareness Month

IT Talk

Oct - Dec 2020 Volume 10 • Issue 4

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

Chief Information Officer
Jeff Seaton (Acting)

Editor & Publication Manager
Eldora Valentine

Graphic & Web Designer
Michael Porterfield

Copy Editor
Meredith Isaacs

IT Talk is an official publication of the Office of the Chief Information Officer of the National Aeronautics and Space Administration, Headquarters, Washington, D.C. It is published by the OCIO office for all NASA employees and external audiences.

For distribution questions or to suggest a story idea, email:
eldora.valentine-1@nasa.gov

To read *IT Talk* online visit:
www.nasa.gov/offices/ocio/ittalk

For more info on the OCIO:
- *www.nasa.gov/offices/ocio*
- *inside.nasa.gov/ocio*
  (Internal NASA network only)
- *www.nasa.gov/open/*

www.facebook.com/NASAcio

In this Issue

Message from the NASA CIO

Now more than ever, many of us are working from home due to the COVID-19 pandemic. From the kitchen table to the classroom, from business transactions to essential Government operations and services, we are all relying on technology to get things done and this means cybersecurity is more important today than ever.

With so many of us working remotely, there is an even greater risk that sensitive data can be exposed to unauthorized individuals. It is critical that we remain vigilant and cyber smart! Each of us has a role to play in protecting NASA's data and systems, as well as our own personal information and home networks.

In recent years, threats and attacks on NASA systems have increased significantly. There are many types of cyber-attacks—unauthorized access, denial or disruption of service, malware, phishing, ransomware, cyber espionage, and viruses to name a few, with the threats getting more sophisticated and harder to detect every day.

October is National Cybersecurity Awareness Month and here at NASA we want to engage and educate, raising awareness about cybersecurity and increasing our resiliency to prevent and address cyber incidents. This issue is dedicated to exploring some common-sense rules to protect yourself, your organization, and your family against cyber threats. We'll also share some general dos and don'ts of teleworking.

None of us is immune to cyber threats. We all need to do our part to ensure that our online personal and work lives are kept safe and secure.

Jeff Seaton

NASA Chief Information Officer (Acting)

JPL Selects New CISO, Deputy CISO

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

Jet Propulsion Laboratory (JPL) Chief Information Officer (CIO) Randi Levin announced the appointment of Preston Miller and Elizabeth "Liz" Rodgers as JPL's new Chief Information Security Officer (CISO) and Deputy Chief Information Security Officer, respectively. The appointments were part of an organizational restructuring that includes a new name, the Information and Technology Solutions Directorate (ITSD).

Miller arrived at JPL from NASA's Ames Research Center in 2019 to be Manager of the Networking and Cybersecurity Division, bringing with him more than 15 years of experience and expertise in cybersecurity. His leadership and management of the NASA Implementation Impact Analysis and Implementation Planning have strengthened JPL's bond with NASA.

Rodgers was Deputy Manager of the Information and Engineering Technology Planning and Development Division. Her 22 years of experience managing cybersecurity programs, as well as her expertise in program management, organizational change management, and strategic planning, earned Rodgers positions of increasing responsibility at JPL, Booz Allen Hamilton, the NTT Innovation Institute, and the RAND Corporation.

Wes Gavins, the previous CISO, has been named Senior Cybersecurity Systems Engineer, a critical new role for ITSD.

Richard Van Why, the previous Deputy CISO, has been appointed as the Manager of Operations in the Networking and Cybersecurity Division.

Preston Miller

Elizabeth Rodgers

IoT Attacks

What is the Internet of Things (IoT)?

The 'Internet of Things' refers to 'smart devices' like refrigerators that will tell us when we're out of milk. IoT includes other smart objects such as thermostats, coffee machines and cars. These gadgets are embedded with electronics, software, sensors and network connectivity so that they can connect to the Internet.

What are IoT threat actors after?

Information

The IoT holds an abundance of information that can be critical, private, or sensitive.

Monetary Gain

IoT attacks can prove profitable for threat actors, who can choose to sell stolen data or seek payment to relinquish control of compromised assets.

Attack Base

Hackers can weaponize IoT devices for attacks that can spread outward or deeper into the main infrastructure.

How to prevent an IoT Attack

- Look at IoT devices like any other computer.
- Immediately change the default password, check regularly for security patches, and always use HTTPS when possible.
- When you're not using the device, turn it off. If the device has other connection protocols that are not in use, disable them.

The Same Office You've Used for Years, Plus All the Benefits of the Cloud

By Shaina Strom, Communication Strategist, End User Services Program Office, Marshall Space Flight Center

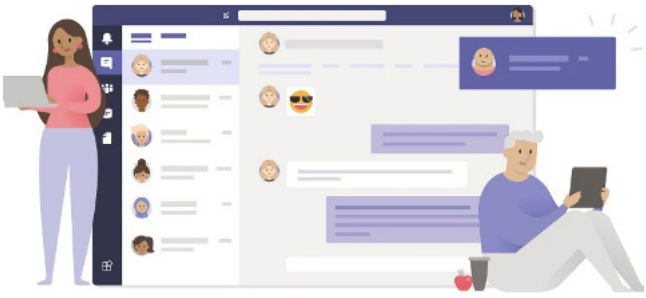
Almost overnight, the way we work and live changed dramatically. Kitchen tables became desks; dogs became colleagues; and vacations became sleeping on the other side of the room. Managing change has always been a taxing process, and the coronavirus pandemic required coordinated efforts at every level—affecting where we live, work, and play. Fortunately, NASA's adoption of cloud-based technical solutions empowered a secure, remote workforce.

Across the board, Federal organizations are adopting cloud solutions to outpace looming security risks and cultivate a productive workforce. With customers like NASA and the House of Representatives, Microsoft is one of only two companies to receive Impact Level 6 Department of Defense clearance. They've dedicated software and services specifically to serve the public sector, separate from what is offered commercially. Microsoft O365 Government Community Cloud (GCC) incorporates security at every level, from application development to physical data centers to end-user access.

In creating the secure, unified tools we use today, Microsoft attacked its own product. By designing threat models based on a range of possibilities, Microsoft tested every feature and function against worst possible scenarios. Improvements were built into both the coding process and implementation practices.

O365 GCC only houses data in centers physically located in the United States. While Office 365 supports integration with third-party service providers, these applications might move data through third-party systems outside of the O365 infrastructure. If you have an application you'd like to investigate, submit a Change Request to initiate a Risk Assessment for review.

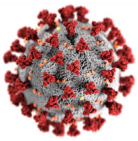
The New Adage Is to Trust Nothing and Verify Everything



Through all the threat models, security protocols, and risk assessments, the end user remains one of the top security vulnerabilities any organization faces. NASA's End User Services Program Office (EUSO) and Communications Program (CP) work to make our virtual workspaces as safe as possible through firewalls, encryption, Bitlocker, Data at Rest (DAR), Virtual Private Network (VPN), and software upgrades.

Of course, it's impossible to design against all unknown security threats, and there's no way to predict what will appear in the wild. However, because Microsoft product development embraced secure design principles from the start, O365 GCC incorporates security technologies as a fundamental part of its architecture.

This modern workspace enables secure collaboration—even from your kitchen table.



Do Your Part. #BeCyberSmart.
Be Wary of Coronavirus Scams

By Tammy Ashraf, Senior Systems Engineer, Goddard Space Flight Center

Since the onset of the COVID-19 pandemic, many people are now finding themselves in situations where they must work from home, homeschool their children, and care for family members. Hackers have used this unprecedented time as an opportunity to prey on heightened levels of anxiety and stress by sophisticated social engineering and phishing scams. According to recent data from the Federal Trade Commission (FTC), there has been a substantial rise in coronavirus-related fraud in which over $100 million has been stolen from people in the United States.

One such scam involves contact tracing. A contact tracer is a person affiliated with a government health department who identifies which people may have come in contact with a person who has an infectious disease, and asks those who are infected, or potentially infected, to quarantine until it is clear that they are no longer sick. Hackers have used this opportunity to scam people by pretending to be contact tracers and asking for financial information and money. A true contact tracer will not ask for financial information or payment.

Furthermore, scammers are targeting people by posing as employees of the Centers for Disease Control and Prevention (CDC) or World Health Organization (WHO) offering bogus vaccinations and home testing kits. Be wary of these types of offers as many aren't accurate or approved by the Food and Drug Administration (FDA).

Another scam to be wary of is coronavirus stimulus payments. Scammers will send unsolicited e-mails, texts, or phone calls asking for personal financial information to deposit stimulus payment funds. Additionally, they may ask you to pay a fee in order to receive funds or ask you to pay back money that was "accidentally over-allocated." In order to verify the status of your stimulus payment or submit financial information, always refer to https://www.irs.gov/coronavirus-tax-relief-and-economic-impact-payments.

Robocalls are also a method that scammers are using to target people with offers for cheap health insurance or work-at-home jobs. Many of these calls appear to be from a legitimate organization as they use a method called spoofing to mask their actual caller ID. They will likely ask for your financial information over the phone. The best course of action is to hang up on robocalls and report them to https://www.donotcall.gov/.

Finally, scammers are using this time as an opportunity to conduct coronavirus donation fraud. They will pose as a legitimate organization and ask you to donate money to support coronavirus relief efforts. Research and verify the charity to ensure that it is legitimate before you donate, especially via online portals.

Be sure to maintain vigilance and be wary of these types of scams. To get the latest and most accurate information regarding COVID-19, refer to https://www.coronavirus.gov/; for more tips on consumer protection, refer to https://www.ftc.gov/coronavirus.

CYBER SAFETY STARTS AT HOME!

Help make your home a safe digital haven by protecting networks, devices, and online lives with these tips:

KEEP A CLEAN MACHINE

Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats. Remember mobile phones, tablets, gaming systems, and other web-enabled devices need updating too!

PROTECT YOUR PERSONAL INFORMATION

Secure your accounts: Usernames and passwords are not enough to protect key accounts like email, bank, and social media. Improve account security by enabling strong authentication tools such as biometrics and two-factor authentication as an extra layer of protection when available.

CONNECT WITH CARE

When in doubt, throw it out: Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete or, if appropriate, mark as junk email.

BE WEB WISE

Think before you act: Be wary of communications that implore you to act immediately, offers something that sounds too good to be true, or asks for personal information.

BE A GOOD ONLINE CITIZEN

Help the authorities fight cybercrime: Report stolen finances or identities and other cybercrime to the Internet Crime Complaint Center (https://www.ic3.gov), the Federal Trade Commission (https://www.ftccomplaintassistant.gov/Information#crnt&panel1-1), and to your local law enforcement or state attorney general as appropriate.

CP Transforms Network Automation and Security with Software-Defined Networking (SDN)

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

The Communications Program (CP) is deploying an innovative approach to network security across the NASA network known as Software-Defined Networking (SDN).

What is SDN?

SDN is based on the principles of Intent-Based Networking (IBN), which will transform NASA's current network based on rigid hardware and manual configuration toward an automated network that can capture and anticipate the needs of NASA personnel and missions.

What are the benefits of SDN? A more secure, efficient, and effective enterprise network.

Currently, a wide spectrum of NASA devices, including enterprise-managed laptops, mobile devices, badge readers, HVAC systems, and lighting controllers, all require specialized and labor-intensive network configuration, authentication, and security policies. SDN provides the software-based network capabilities to deliver a standardized approach for the network control, security policies, and automation of devices connected to the NASA network.

Deploying SDN across the enterprise will provide NASA with a far more secure network while reducing operational costs and increasing the ease of deploying more specialized networks in support of NASA partners and missions. The SDN foundation will enhance network control, automation, and security to allow the Agency to be more efficient and effective in supporting its missions.

One of the tenets of SDN is Intent-Based Networking (IBN), which provides identity-based connectivity to resources only as needed. With this capability, SDN enables "just in time" provisioning of network access for any credentialed user or device and keeps out intruders and unauthorized personnel. This moves NASA toward a "zero-trust" network architecture, which has been proven to prevent data breaches.

SDN streamlines and automates the decisions and manual configurations needed for network traffic and security policies, enables the use of artificial intelligence and machine learning to protect the NASA network, and reduces the time to generate and provision specialized and partner networks from months to minutes.

Using SDN policies standardizes local networks across the Agency so an enterprise network engineer will now be able to quickly troubleshoot issues at any Center.

How is SDN being delivered? Quickly and securely.

CP is leveraging Agile and DevSecOps to deploy SDN across the enterprise network.

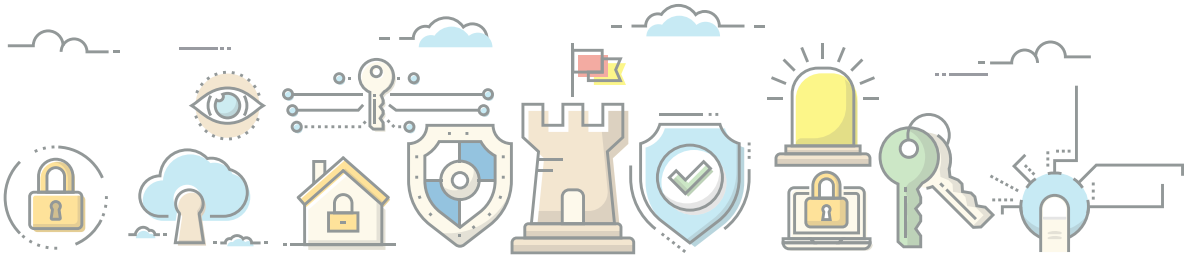
- Agile is a delivery methodology that utilizes self-organizing, cross-functional, collaborative teams to encourage nimble responses and continual improvement. The Agile approach emphasizes adaptive planning, iterative and incremental development, and early delivery.
- DevSecOps provides a framework focused on security by combining development, engineering, IT security, and operations teams to develop and deploy changes.

How does SDN affect NASA missions? It provides secure, specialized networks at the speed of light.

With automated network configuration and management, SDN will enable NASA's network to operate much more quickly and responsively within the Agency's new operating model of close collaboration with commercial partners for key missions. SDN will reduce the time needed to provision specialized networks for commercial partners, allowing faster access to NASA resources and collaboration across mission teams, all while enhancing NASA's security posture with reduced opportunities for network vulnerabilities.

The SDN model reduces the time needed to deliver patch updates and the number of vulnerabilities as increased automation eliminates mistakes and reduces downtime from network attacks. The DevSecOps concept integrates security into engineering and deployments at a much earlier stage, which reduces the need for reactionary patching and updates.

Mission customers across NASA will benefit from highly secure, responsive, and reliable networks, delivered on demand to only the personnel who need it—instantly at the time they need it—with SDN.



Why NAC? Why Now? Why ME?

By Jeremy Breeden, NICS Project Manager for the Communications Program (CP) Network Access Control (NAC) Enforcement Support Team, Marshall Space Flight Center

A plague affecting countless individuals is spreading like the latest viral video trend, and no, this is not the recent respiratory illness known as COVID-19; this plague takes the form of threats to cybersecurity. In the past decade, we've witnessed some of the largest breaches to personal and financial data across a variety of sectors and industries affecting both government and retail institutions. And the worst part is that this is likely a small taste of what lies ahead as cybercriminals become more resourceful at exploiting vulnerable technology. However, there are means to help strengthen our digital "immune system" to combat these future attacks, and one of those means is through identifying and preventing unauthorized devices from gaining access to NASA's networks.

Over the past several years, Federal requirements have forced stricter cybersecurity compliance standards for all organizations in efforts to safeguard information and reduce the chances for device compromise and exploitation. In response to these requirements, NASA has embarked on the path to "zero-trust" for its network infrastructure. A principal tenet of zero-trust is granting need-based access rather than default access. Network Access Control (NAC) is one of the steps along the journey to zero-trust. So, what is NAC, why are we doing it, and what does it mean for me?

Network Access Control enables the enterprise to control access to the NASA network; it's an approach to network management and security that enforces access controls to the NASA network by enabling only compliant, authenticated, and authorized endpoint devices to access network resources and infrastructure. As we improve the security posture of NASA's corporate networks and implement the tools and capabilities the Agency requires to enable access controls to corporate networks across Centers, it is critical for us to understand who and what are authorized to access our network infrastructure and how. The desired end state is to have 100 percent of the endpoints on the NASA corporate network with "closed mode" enforced. To get to this desired end state, NAC

enforcement teams were established at the Centers to identify, analyze, and categorize all relevant endpoints across the corporate ports; determine the appropriate authorization method for an endpoint; and convert the port to perform an authentication check prior to allowing access to the network. A simple analogy would be that NAC enforcement is like a gate guard who checks your NASA badge prior to allowing you into a NASA facility.

If you, the reader, made it this far in the article, you may be thinking, "That's cool, but what does this have to do with me?" or "What do I need to do?" The answer to those questions is multifold. Ideally, with proper testing and advanced communications, there will be minimal to no impact to the end users at the Centers during the NAC Enforcement (NAC-E) activities. Great care is being taken to coordinate support during the conversion activities to minimize the risk of downtime; however, with any large implementation across an organization with as many endpoints as NASA, it's inevitable that some edge-cases will arise. That leads to the second question about what, if anything, you need to do. Check for notifications of upcoming NAC conversions in your area, respond to requests from your local NAC team about your endpoints, and contact the Enterprise Service Desk (ESD) if you are experiencing issues connecting your approved device to the NASA network after a NAC activity.

For additional information, the NAC Enforcement Support Team created a SharePoint site accessible to all with a valid NASA account: *https://sharepoint.msfc.nasa.gov/sites/cso/internalnac/SitePages/Home.aspx*.

While the pandemic continues to challenge all of us in new ways and shape the way we are working, the absence of most individuals from the Center provided a unique opportunity to analyze thousands of static devices remaining and performing the necessary preparation work required. In the coming weeks and months, multiple activities will be scheduled and executed to convert NASA's corporate-network switches to meet Agency goals. While every effort is being made to limit impacts to all end users during these conversions, anomalies happen. Please remain patient and report any loss of connection or degradation of service promptly to the Enterprise Service Desk (ESD).

Keeping Your Software and Operating System up to Date

By Daniel Horton, EUSO Communications, Marshall Space Flight Center

On either your personal or work computer, you've probably seen the notifications or e-mails. Periodically, you may get a message informing you that it's time for an update to your software or to your entire operating system.

These kinds of updates can supply useful new features and often include critical security patches. Ensuring that your machine is up to date can be a crucial part of keeping it running smoothly.

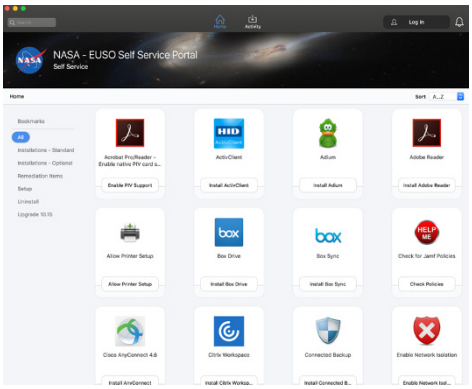
Updates Keep Your Device Secure

Out-of-date devices can sometimes contain a security hole or weakness that a bad actor or hacker can exploit. Taking advantage of this can allow them to potentially gain access to sensitive documents or information. Developers managing operating systems and software packages continually stay on top of any vulnerabilities and include fixes to these issues in patches and updates.

The End User Services Program Office's (EUSO's) Security Manager, Kirk Johnson, mentions that "quality improvements, bug fixes, and known exploits" are typically some of the biggest fixes included in patches and operating system updates.

Check Self-Service for Updates

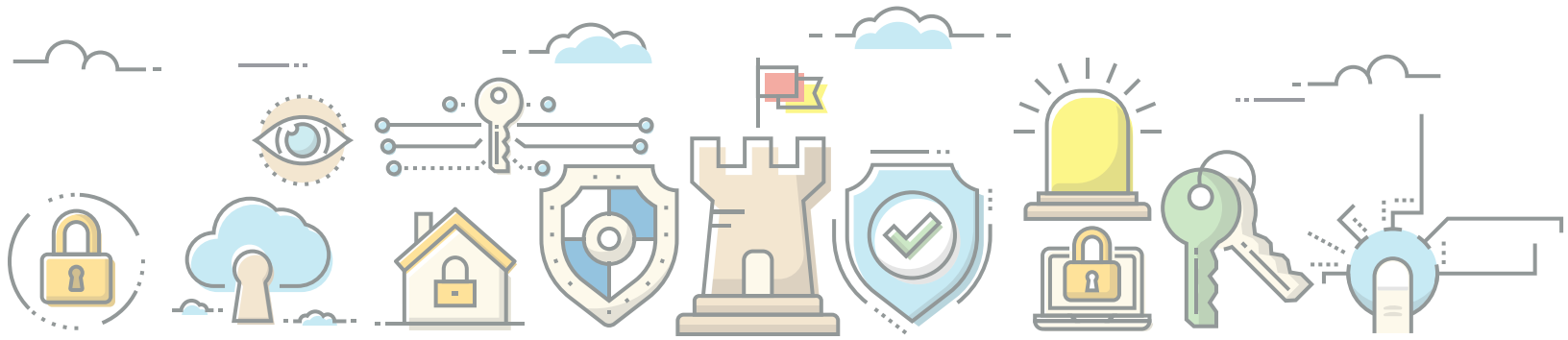
If your machine is due for a critical update, you will be notified by e-mail ahead of time.



This e-mail will contain instructions on how you can self-install any required updates. Remember that if you have not self-installed by a specified deadline, a forced installation could occur at a time scheduled for you.

- **NASA Self-Service Portal—**To look for required and optional self-install updates, check the self-service app on your machine. Here, you can see critical software or operating system updates.
- **Standard Installations—**In this tab, you can find updated browsers, office packages, and security patches.
- **Optional Installations—**Check this tab for other elective and useful software that can be downloaded.
- **Operating System Upgrades—**If you're due for an operating system update such as MacOS 10.15, a tab will appear containing this upgrade. From here, you should be able to begin the upgrade process.

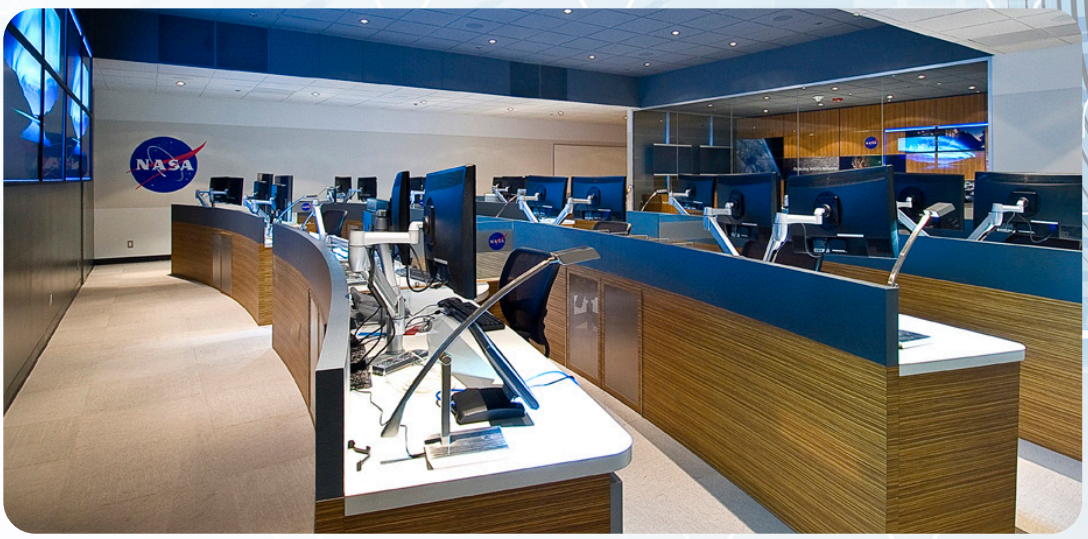
As many of us at NASA continue to work remotely, our laptops and other machines have become our lifeline to our work. At EUSO, we're continuing to keep your machine running smoothly and securely so you can continue your work in pursuit of the mission.



24 x 7 NASA's Security Operations Center

By Penny Hubbard, NASA SOC Communications, Ames Research Center

On October 1, NASA's Security Operations Center (SOC) realigned with the Office of CyberSecurity Services (OCSS). The NASA SOC functions as the only authorized single, agencywide cybersecurity operational entity whose mission is to provide proactive prevention, detection, and response to computer security incidents targeting NASA's networks and systems. This includes all NASA networks and systems across the corporate, mission and operational technology domains. The NASA SOC is the nerve center for 24/7 cybersecurity incident monitoring, reporting, detection, prevention, response, mitigation, and cyber threat analysis for the Agency. NASA SOC provides robust distributed security operations hosted at Ames Research Center and Johnson Space Center maintaining sound around the clock services. The new alignment with OCSS further enables consistent, efficient, and effective service delivery of the SOC's core functions. NASA's SOC is online with informative resources including Cybersecurity tips, Cyber-threat Awareness Bulletins, and links to Agency resources. Check us out online: *https://nasa.sharepoint.com/sites/soc*



IT Talk

National Aeronautics and Space Administration

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

www.nasa.gov

NASA CIO