



NOVEMBER 3 ,2021

ISOAG MEETING



AGENDA

- **WELCOME / INTRODUCTION: MIKE WATSON**
- **ROY LOGAN/NASA**
- **MEREDITH WARD/NASCIO**
- **STEVEN SEIBERT/SAIC**
- **UPCOMING EVENTS**
- **ADJOURN**



VITA Briefing Innovation - NASA Remote PIV Issuance Process



**Special Agent Roy Logan
Center Chief of Protective Services
Langley Research Center
Hampton, Virginia**

Nov 3, 2021



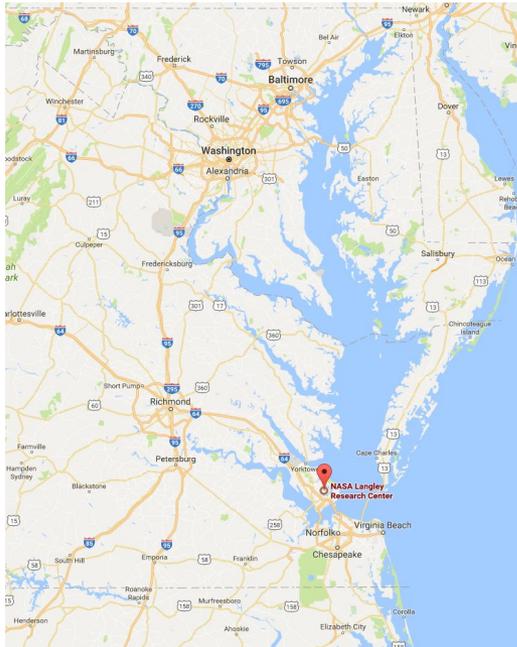


Overview of Topics

- **Background/Necessity**
- **Issues**
- **Process**
- **Questions**



Langley Research Center Overview



The First NASA Center.

Specializing in Aeronautics Research

Wind Tunnel Test Facilities
Laboratories for Acoustic,
Atmospheric Science, Structures and
Materials, Laser, Lidar and Remote
Sensing research

750 acres

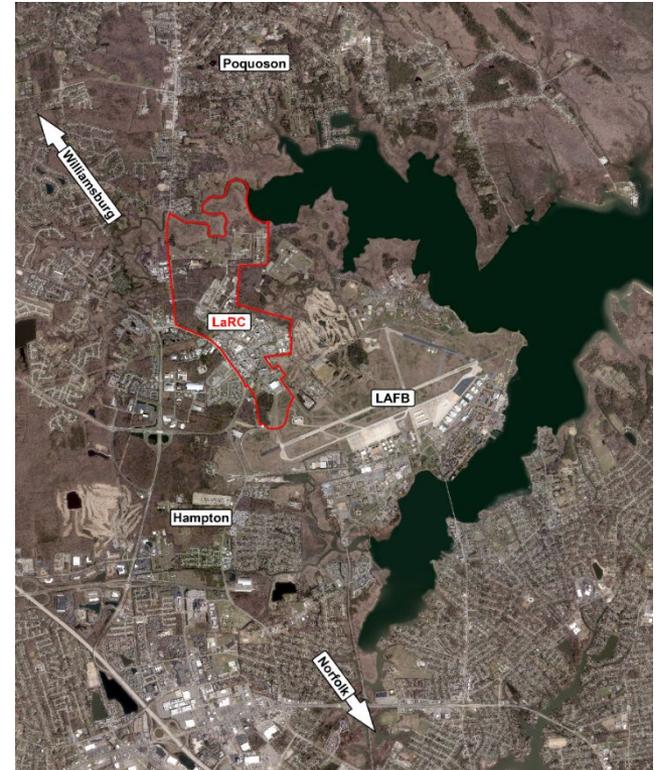
198 buildings

6338 rooms

Approx. 3.4M gross sq ft

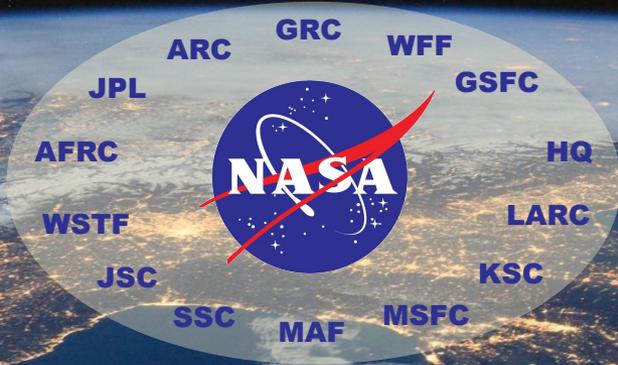
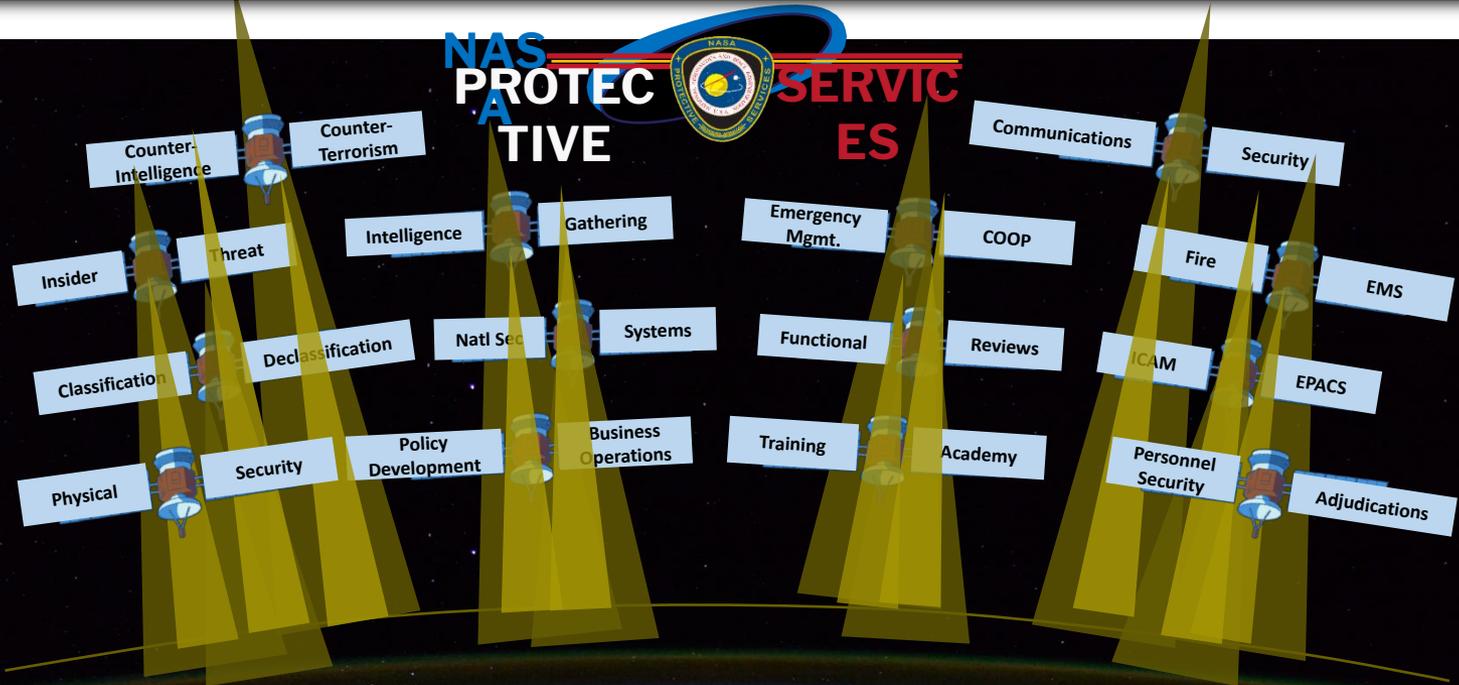
Replacement value of \$3.6B

5069 Civil Servant and Contractor
Employees divided into 19 managerial
organizations





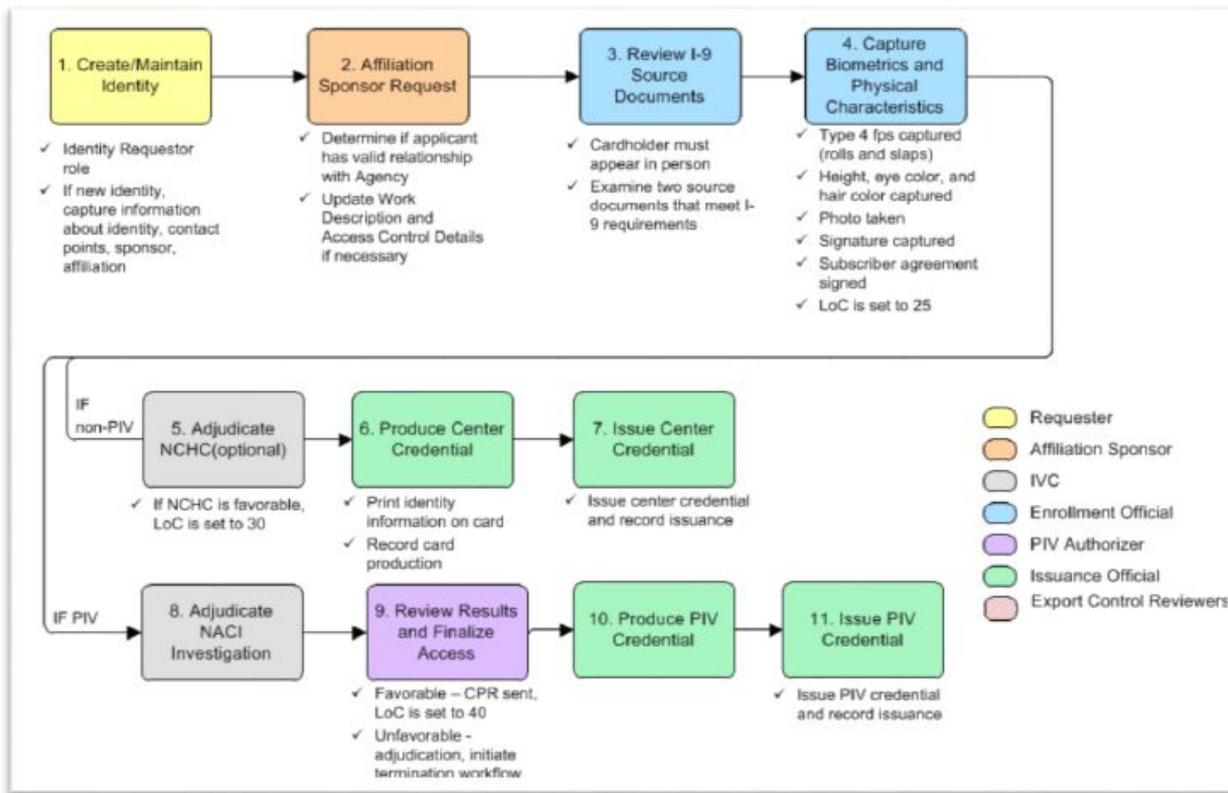
NASA Protective Services Enterprise





Identity, Position Risk, and Credentialing

IDENTITY ONBOARDING WORKFLOW





ISSUE

Center closed during COVID (Stage 4)

- New employees unable to obtain IT assets or physical access to HR personnel.
- Once onboarded, PIV required for accessing IT infrastructure
- Any employee (CS or Kr) unable to perform telework without PIV/IT platform.
- BPO staff traumatized.



Remote Process

What you should do first

- 1. If you do not have a PIV or ASB Smartcard, contact the ESD @ 1-877-677-2123 so they can facilitate your access without a PIV.
 - a. They will assign an Emergency RSA Soft Token
 - b. They will assign a PIV Exemption allowing you to log in using Username/Password
- 2. Verify you can access Microsoft Teams
- 3. Verify your camera, microphone and speaker are working properly on your computer a. If your microphone does not work, the Badging official may call you directly
- 4. A Badging Official will contact you via Microsoft TEAMS to complete the PIV card process.



Remote Process

What to expect during your Teams meeting

- The Badging Official is required to complete a visual facial verification which means the meeting between you and the Badging Official will be conducted using the camera from your laptop. During this meeting the Badging Official will share their screen with you so that you can see what steps they are completing during the process. The Steps you will complete are as follows:
 - 1. Badging Official will complete a visual facial verification
 - 2. Badging Official will encode your badge
 - 3. Badging Official will *Give Control* of their screen to you
 - 4. You will be required to Enter a Pin
 - 5. You will be required to Confirm the Pin



Remote Process

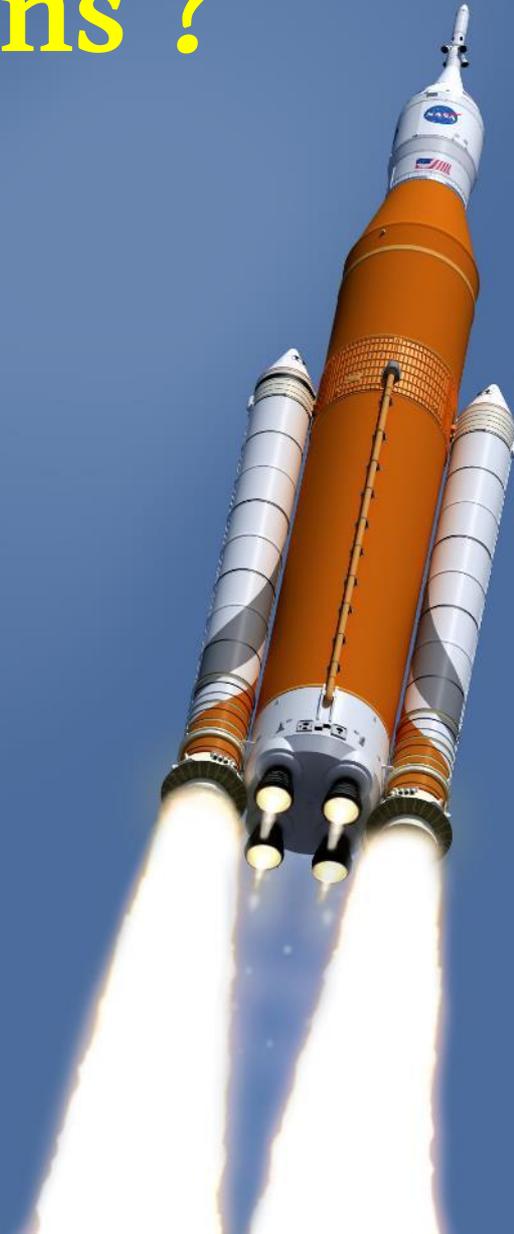
Pros:

- Allows systems access up to LOC 30 (email, WebTADS, SATERN, etc.). Higher level requires fingerprints.
- Facilitates ability to work remotely until fully vetted.

Cons:

- Requires acceptance of additional risk.
- Requires physical presence at some point in time – additional work.

Questions ?



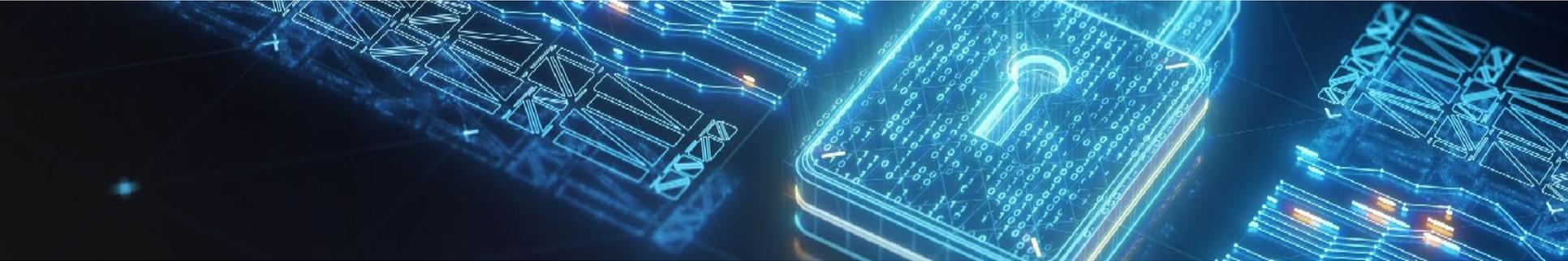


State Cyber Trends

Commonwealth of Virginia
VITA ISOAG Meeting
November 3, 2021

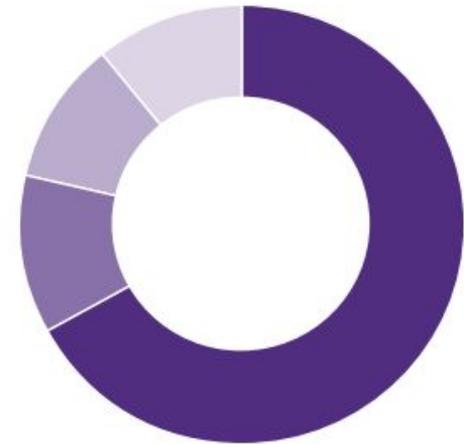
Meredith Ward
Director, Policy & Research
NASCIO





Concerning the continuity of government, what is your top cybersecurity risk today?

- Ransomware attack **57%**
- Compromises to the software supply chain **10%**
- Agency use of shadow IT solutions or products **8%**
- Stolen identities/fraudulent claims for benefits (UI, SNAP, etc.) **8%**



Based on the impact of the COVID-19 pandemic, what cybersecurity initiatives will receive more attention in the next 2-3 years? (select all that apply)



Adoption/expansion of enterprise identity and access management solutions



Continuous enterprise cybersecurity assessment



Endpoint detection



Introducing or expanding a zero trust framework



Increased due diligence with vendors and third-party providers



Improved anti-fraud capabilities and services



Cybersecurity awareness training



Increased use of behavioral analytics

Which automation solutions and emerging technologies adopted in response to the COVID-19 pandemic do you believe are here to stay?



1
Chatbots (virtual agents) for online citizen service inquiries



2
Automated fraud detection using predictive analytics



3
Voicebots to support call center interactions



4
Robotic process automation (RPA) to streamline business processes

What emerging IT area will be most impactful in the next 3-5 years?



Low-code/no-code



Artificial intelligence (AI)/Machine learning



Mass personalization /citizen personas



Robotic process automation (RPA)



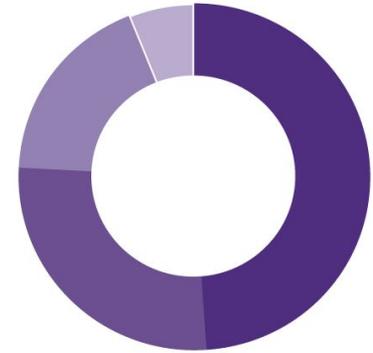
Internet of things (IoT)



Remote work technology

Please characterize the status of your citizen digital identity initiative.

- Partially implemented **49%**
- Planned **27%**
- No plans to implement **18%**
- Fully implemented **6%**



- Please characterize the status of your enterprise-wide IAM solution (covering all agencies under governor's jurisdiction).

- Partially implemented **60%**
- Planned **21%**
- Fully implemented **13%**
- No plans to implement **6%**



What are your top three priorities in driving your cloud strategy forward?



78%

Scalability/Flexibility



57%

Security



43%

Investment optimization

41%

Disaster recovery/Risk management

27%

Application rationalization

20%

Staff training

10%

Mobility

10%

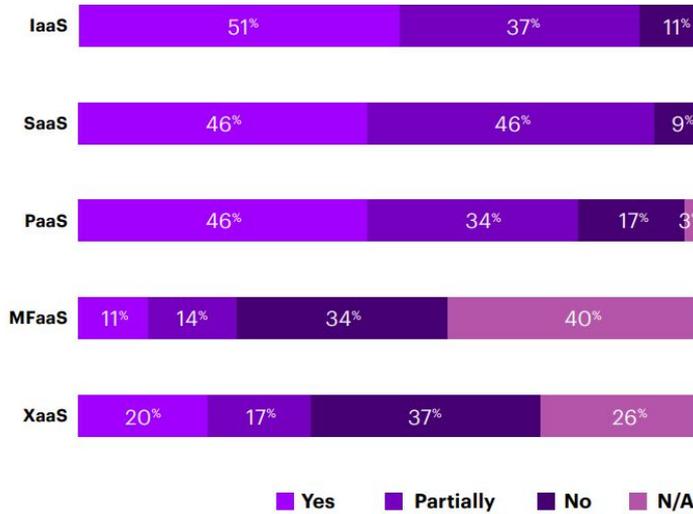
Extending catalog of cloud services

4%

Procurement reform
to terms and conditions



Is your state using multi-factor authentication for cloud services?





Possible Actions:

Incorporate state identity, credentialing and access management (SICAM) into cloud strategy. **(Maturity level 2)**



Incorporate end user cloud awareness education such as phishing, spearfishing, smishing and other threat profiles that can occur as a distributed workforce accesses cloud computing from non-centrally secured locations. **(Maturity level 2)**

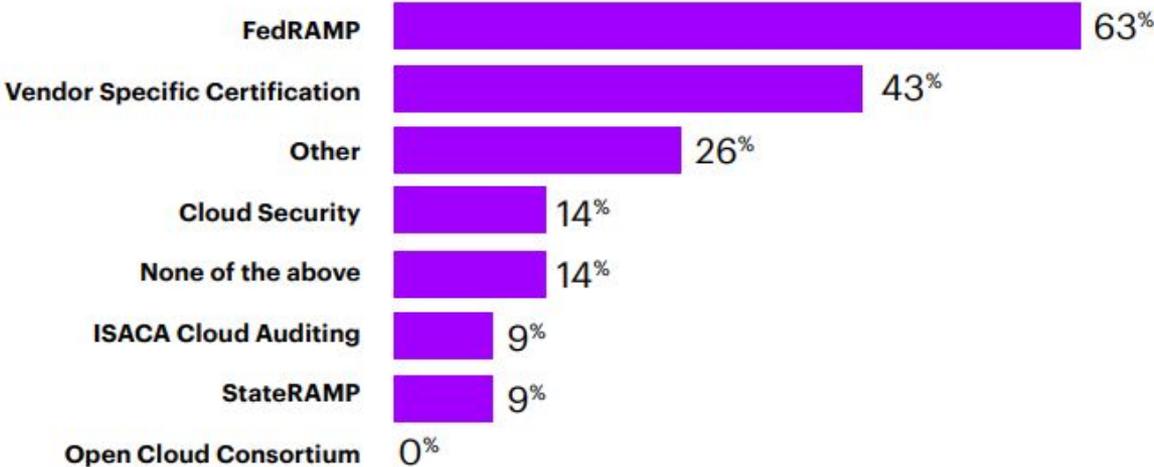


Explore cloud native security offerings and meet with current security product owners to understand how their products align with cloud service providers. This could influence the selection of cloud partners and should be included as a necessary process step in cloud procurement operating discipline. **(Maturity level 2)**



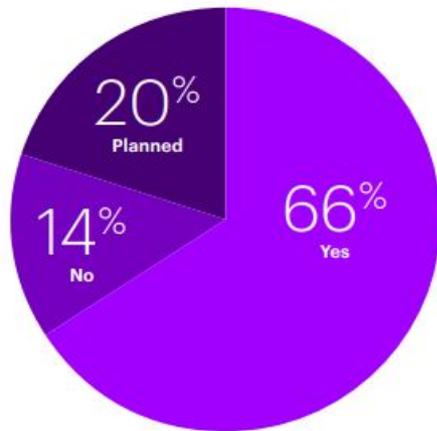


Which of the following cloud certification/standards programs does your state require?

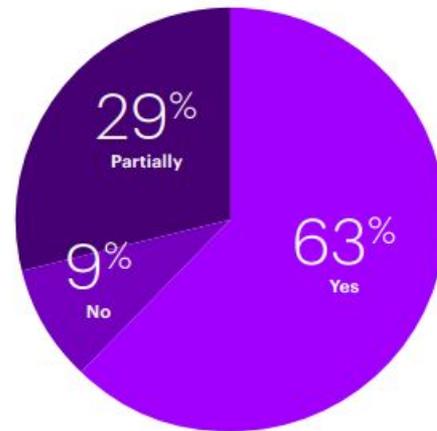




Does your state have a process for managing cloud-related privileged permissions?



Are cloud-related logins and access activities monitored?



State Cyber Trends to Watch



Sustaining and securing the remote work environment

No-code/low-code

Identity and Access Management

Zero-trust

Securing digital government services; .GOV adoption

Whole-of-state cybersecurity collaboration



Third party contractors; supply chain compromises

mward@nascio.org



★ LET'S BE FRIENDS
FOLLOW US

 NASCIO

 NASCIOmedia

 NASCIO

www.nascio.org/resource-center

Patching Methods

Steven Seibert, Natalie Murdock, Thaddeus Gibson
November 3, 2021

SAIC



Table of Contents

1. What software is patched?
2. Server patching
3. EUC patching



What the ITISP patches ...

There is a defined list of Software patched by the ITISP. It is the Enterprise Security Software Patching list. (ESSP)

.

The list can be found on the Patching SharePoint site located here:

<https://center.share.virginia.gov/ITP/patching/SitePages/Home.aspx>



Queries in Tenable

There are queries setup in Tenable that show the vulnerabilities the ITISP will patch.

Please log a ticket with ENT-MSS-SECURITY-GRC for training on how to use the query

Software included	Software not included
Adobe Reader	Java (non-JRE versions)
Microsoft Office	Adobe professional products
Operating systems (server and workstation)	Licensed products not available on standard image
Antivirus	



Server Patching

Natalie Murdock
Unisys

Sharepoint site

<https://center.share.virginia.gov/ITP/patching/SitePages/Home.aspx>

- Patching Event Calendar
- Server List
- Monthly Patch Announcement
- Server Patching Schedule

Contact Natalie Murdock
Natalie.Murdock@Unisys.com
 for access

SharePoint Murdock, Natalie (ITP)

CENTER Search Center COVID-19 Public Collaboration COVID-19 MSI Continual Improvement (CSI) VITA STS Transition Assistance Program

Server Patching Management Site

Patching Home

Recent

Patching event calendar

EDIT LINKS

Site Contents

Patching event calendar

October 2021

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
26 Patch Day B	27	28 Patch Day C	29 Patch Day D	30	1	2
3 Patch Day E	4	5 Patch Day X	6 Patch Day F	7	8	9
10 Server Remed	11	12 Patch Tuesday	13	14 Pilot Desktops	15	16
17 Patch Day A	18	19	20	21 Production De	22	23
24 Patch Day B	25	26 Patch Day C	27 Patch Day D	28 DBHDS Deskto	29	30
31 Patch Day E	1	2 Patch Day X	3 Patch Day F	4	5	6

Announcements

new announcement or edit this list

Title	Modified
Change Suspensions	March 12, 2020
Patch hold procedures	March 12, 2019

Server List

Name	Modified	Modified By
September 2021 Enterprise Windows Server Patching Remediation	A few seconds ago	Murdock, Natalie (ITP)
Archive Device List	August 28, 2018	Spurlock-Tupponce, Shelia (ITP)
September 2021 Linux Server Patching Day A	September 16	Murdock, Natalie (ITP)
September 2021 Linux Server Patching	Monday at 12:50 PM	Ghanta, Rajkiran (VDH)



Patch Tuesday is the 2nd Tuesday of each Month

Server Patching Schedule

[+ new item](#) or [edit this list](#)

✓	Title	Description	Time
	Day A	... 1st Sunday after Patch Tuesday	3 AM - 9 AM
	Day B	... 2nd Sunday after Patch Tuesday	3 AM - 9 AM
	Day C	... 2nd Tuesday after Patch Tuesday	10 AM - 3 PM
	Day D	... 2nd Wednesday after Patch Tuesday	7 PM - Midnight
	Day E	... 3rd Sunday after Patch Tuesday	3 AM - 9 AM
	Day X	... 3rd Tuesday after Patch Tuesday	10 AM - 3 PM
	Day F	... 3rd Wednesday after Patch Tuesday	7 PM - Midnight
	Remediation	... 4th Sunday after Patch Tuesday	3 AM - 9 AM



Distribution lists

DL Server Maintenance Day A DLmaintenanceDayA@vita.virginia.gov

DL Server Maintenance Day B DLServerMaintenanceDayB@vita.virginia.gov

DL Server Maintenance Day C DLMaintenanceDayC@vita.virginia.gov

DL Server Maintenance Day D DLServerMaintenanceDayD@vita.virginia.gov

DL Server Maintenance Day E DLServerMaintenanceDayE@vita.virginia.gov

DL Server Maintenance Day F DLServerMaintenanceDayF@vita.virginia.gov

Use the VITA Service portal to request being added or removed from any of the distribution lists.



Patch holds

If a patching hold/delay is required, the agency ISO must request a Maintenance Hold Waiver via the VITA Customer Care Center (VCCC) at vccc@vita.virginia.gov.

The request must identify the server(s) along with the start and end dates of the hold.

The VCCC will route it to VITA CSRM for approval and notify both the Patch and Service Asset and Configuration Management (SACM) Team.



EUC Patching

Thad Gibson

Ironbow

Schedule:

Patch Tuesday is the 2nd Tuesday

Pilot is the Thursday following Patch Tuesday beginning at 6PM

Production Deployments all begin at 6PM

- Thursday (1 week after Pilot) – All Windows 8 and 20H2 systems, 200 Windows 7, 200 10/1809 and 1500 10/1607, 10/1909 systems
- The following Monday – to all remaining Windows 7, 500 10/1809 and 3500 10/1607, 10/1909 Systems
- The next day (Tuesday) – to all remaining Windows 10/1809 and 5000 10/1607, 10/1909 Systems
- The next day (Wednesday) – All remaining Systems
- The next day (Thursday) - for DBHDS



Update Pilot Workstation list

Navigate to the Service Catalog and select [Desktop Pilot Group Update](#) and complete the form.

The screenshot shows the Virginia IT Agency Service Catalog interface. The header includes the agency logo, navigation links for Service Catalog, Knowledge, Request Assistance, My Items (3), System Status, Contact Us, and a Cart (1). The breadcrumb trail is Home > Service Catalog > Personal Computing > Desktop Pilot Group Update. A search bar is present on the right. The main content area features a dark blue sidebar on the left and a white content panel. The content panel is titled 'Desktop Pilot Group Update' and includes a sub-header: 'Use this form to add and/or remove users from your agency's pilot deployment group.' Below this is an icon of a computer monitor and keyboard. The main text explains that the form is used to update an agency's Pilot List for patching and software deployments, and that changes submitted will result in an update to the list of pilot devices used by the endpoint management tool, SCCM. A note specifies that the form is only in effect after Production and Patch Tuesday. The average fulfillment time is listed as 5 business days. On the right side of the content panel, there is a dropdown menu with '1' selected, an 'Add to Cart' button, and an 'Order Now' button. Below these is a 'Required information' section with a red 'Action Requested' button.



Sharepoint site

<https://center.share.virginia.gov/ITP/patching/SitePages/Home.aspx>

Patching Event Calendar Monthly Patch Announcement

The screenshot displays a SharePoint site titled "Server Patching Management Site". The main content area features a "Patching event calendar" for October 2021. The calendar is a grid with days of the week as columns and dates as rows. Events are represented by colored boxes with text labels.

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
26 Patch Day B	27	28 Patch Day C	29 Patch Day D	30	1	2
3 Patch Day E	4	5 Patch Day X	6 Patch Day F	7	8	9
10 Server Remed	11	12 Patch Tuesday	13	14 Pilot Desktops	15	16
17 Patch Day A	18	19	20	21 Production De	22	23
24 Patch Day B	25	26 Patch Day C	27 Patch Day D	28 DBHDS Deskto	29	30
31 Patch Day E	1	2 Patch Day X	3 Patch Day F	4	5	6

On the right side of the page, there are two panels: "Announcements" and "Server List". The "Announcements" panel shows a "new announcement" button and two items: "Change Suspensions" (modified March 12, 2020) and "Patch hold procedures" (modified March 12, 2019). The "Server List" panel shows a table with columns for Name, Modified, and Modified By. It lists several servers, including "September 2021 Enterprise Windows Server Patching Remediation", "Archive Device List", "September 2021 Linux Server Patching Day A", and "September 2021 Linux Server Patching".



Patching Distribution List

Each monthly security update is communicated by CSRM using a distribution list maintained by Ed Miller.



Patching Holds

If a patching hold/delay is required, the agency ISO must request a change freeze to include security patching. The request must identify the start and end dates of the freeze. Change freezes exceeding 89 days require a CSRM Security exception.



Questions?



Upcoming events



DECEMBER ISOAG

Dec. 1, from 1 to 4 p.m.

Presenters:

Douglas Streit/ Old Dominion University

Steve Aiello/AHead

Tim Gawne/ AHead

Patrick Robinson /ATT

Bindu Sundaresan/ ATT

IS ORIENTATION

FINAL IS ORIENTATION 2021

Dec. 8, 2021 1 – 3 p.m.

Presenter: Marlon Cole

Registration Link :

<https://covaconf.webex.com/covaconf/onstage/g.php?MTID=e6299241bfefde9a4e45b6e1b8a81e7cb>



**THANK YOU FOR
ATTENDING!**

