VIRGINIA
IT AGENCY

NOVEMBER 3 ,2021

ISOAG MEETING

VIRGINIA
IT AGENCY

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

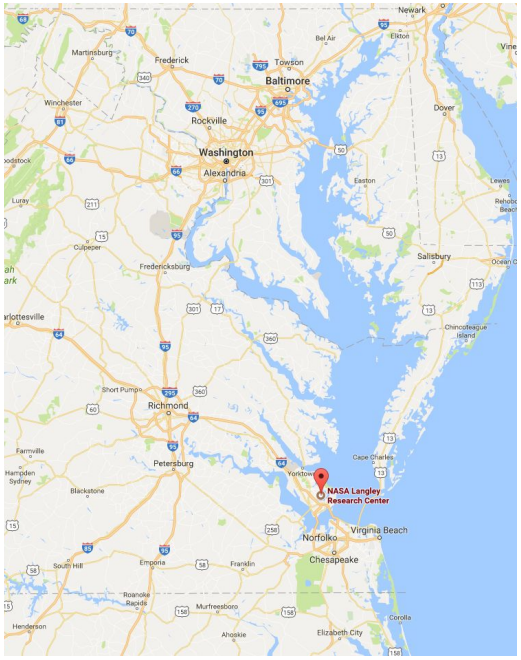
Special Agent Roy Logan
Center Chief of Protective Services
Langley Research Center
Hampton, Virginia

Nov 3, 2021

Overview of Topics

- Background/Necessity
- Issues
- Process
- Questions

Langley Research Center Overview



The First NASA Center.

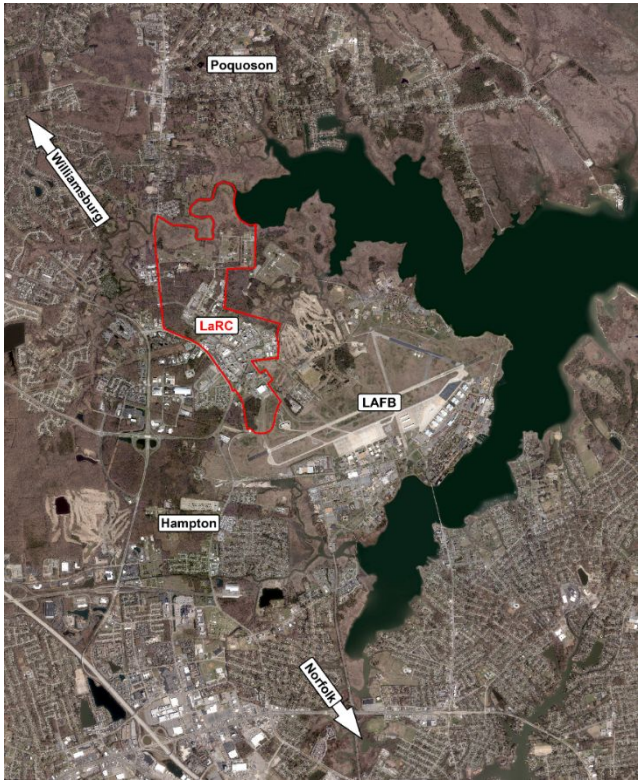
Specializing in Aeronautics Research

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

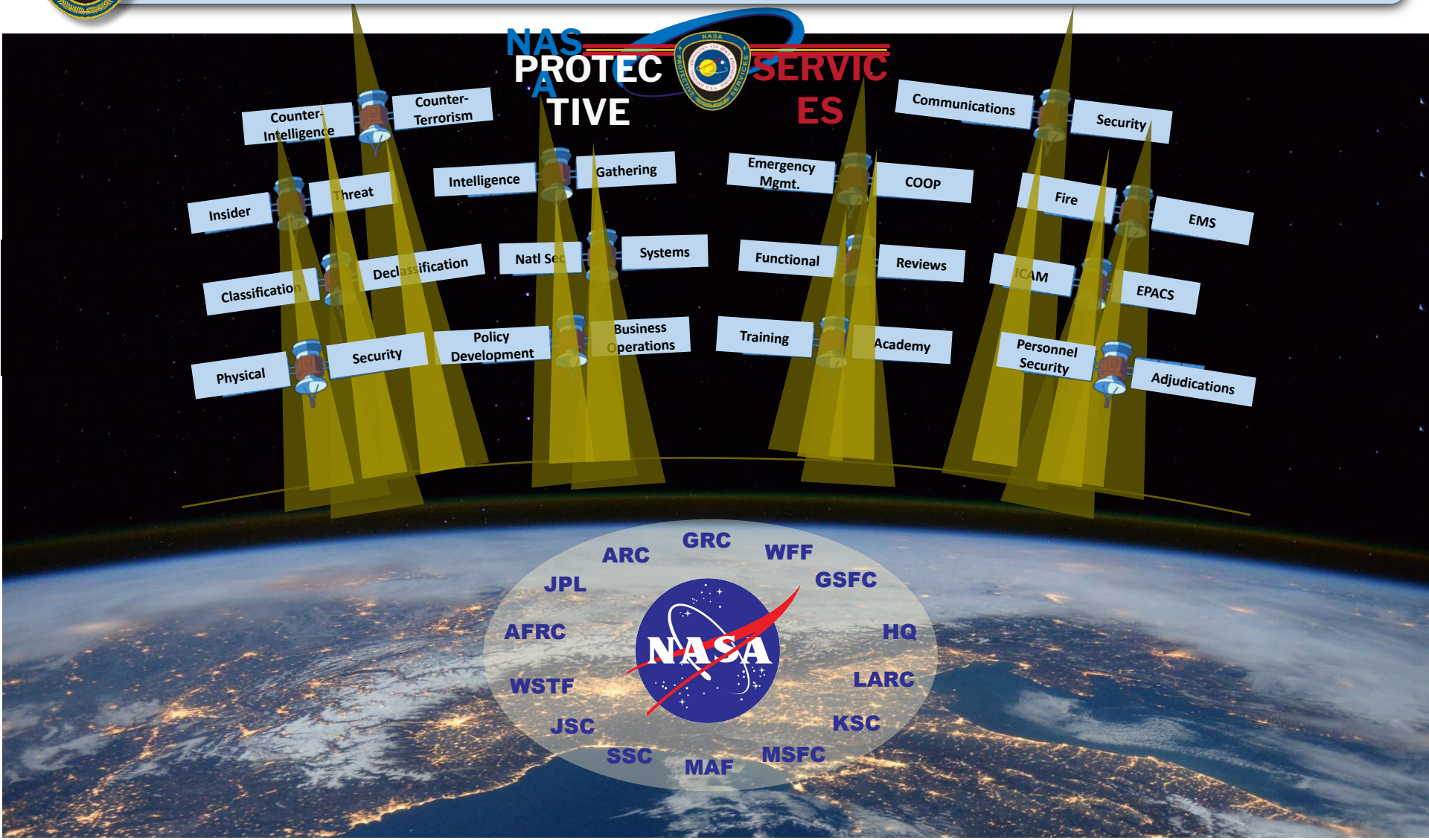
750 acres
198 buildings
- 6338 rooms
- Approx. 3.4M gross sq ft

Replacement value of $3.6B

5069 Civil Servant and Contractor Employees divided into 19 managerial organizations

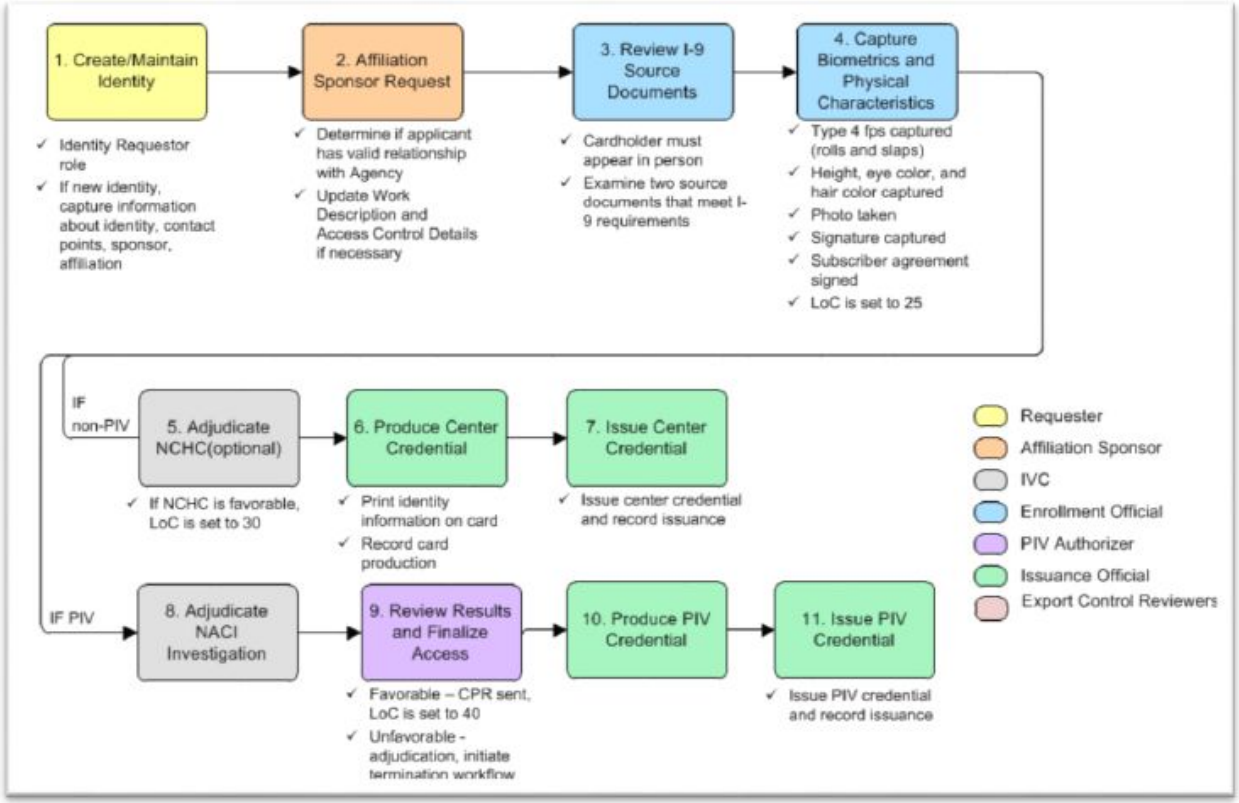


NASA Protective Services Enterprise



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:

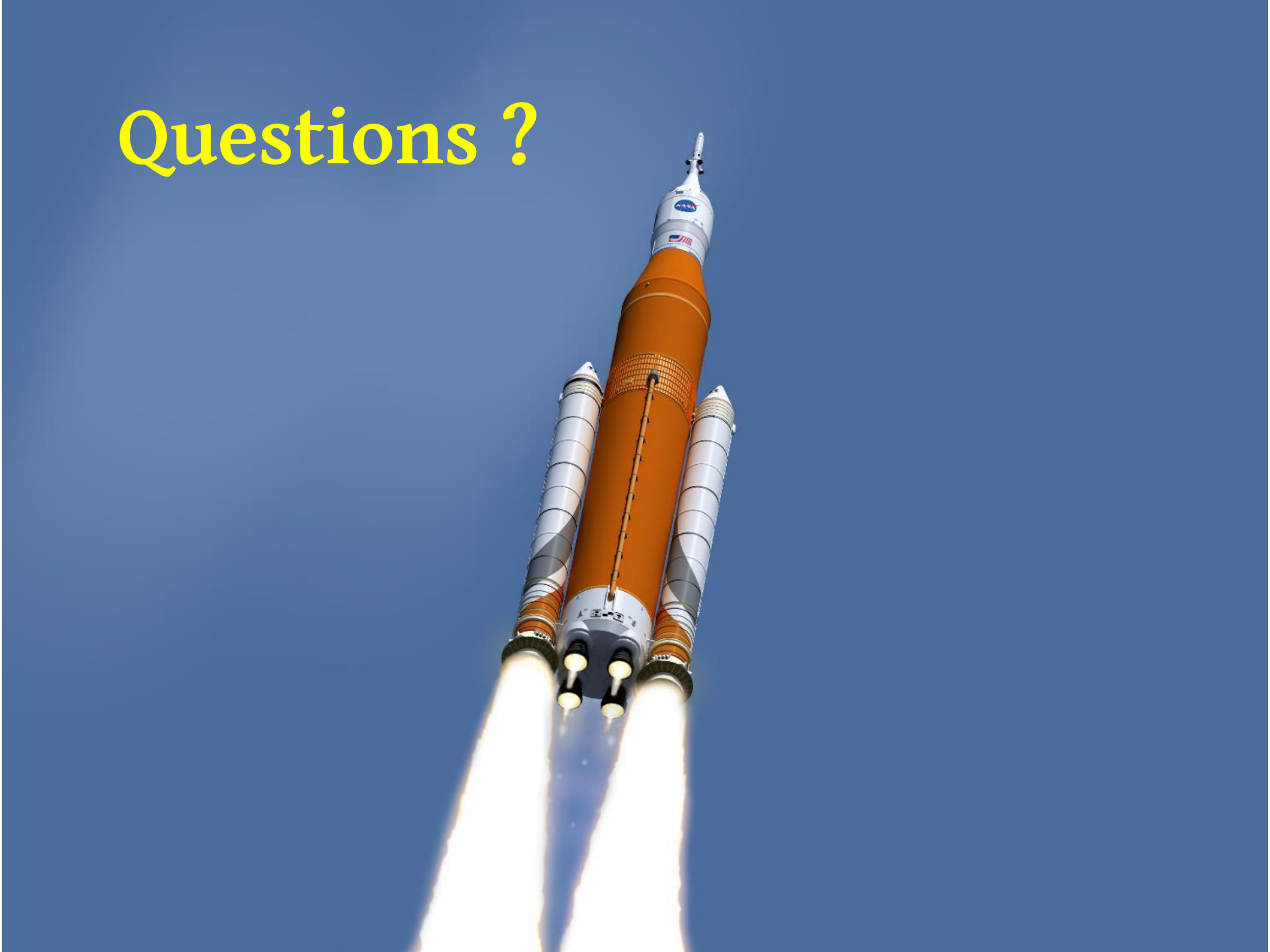
- Allows systems access up to LOC 30 (email, WebTADS, SATERN, etc.). Higher level requires fingerprints.

- 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


NEW

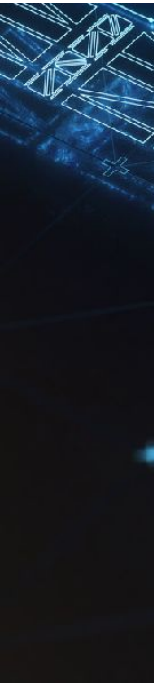

NASCIO | GrantThornton | CompTIA
Driving digital acceleration
The 2021 State CIO Survey


NASCIO
A fresh look: Capitals in the Clouds
2021 Accenture and NASCIO Cloud Study

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)



83%	69%	67%	67%
Adoption/expansion of enterprise identity and access management solutions	Continuous enterprise cybersecurity assessment	Endpoint detection	Introducing or expanding a zero trust framework
63%	60%	56%	50%
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

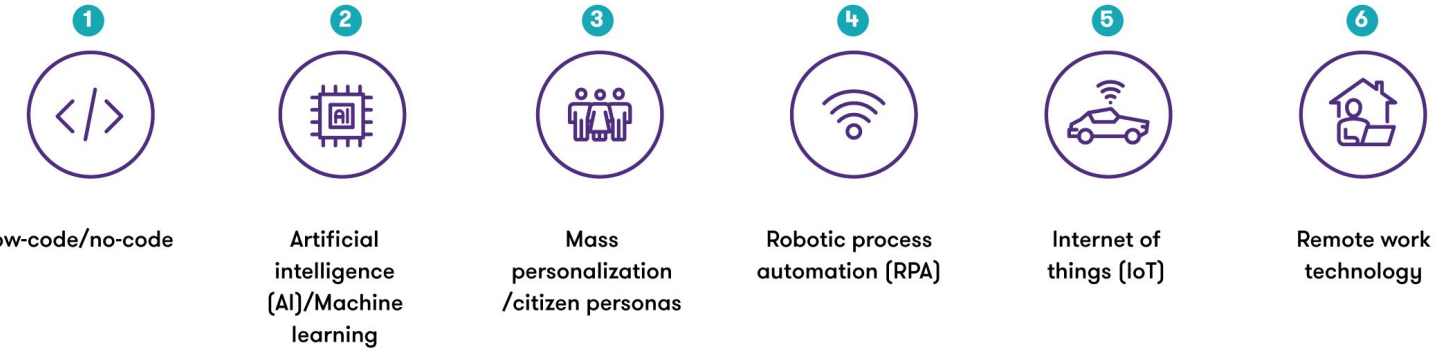
3. 

Voicebots to support call center interactions

4. 

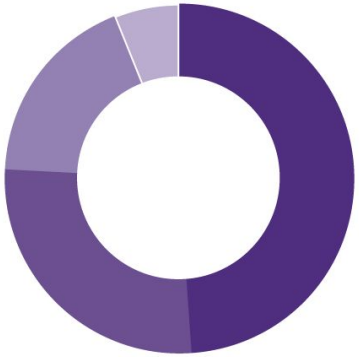
Robotic process automation (RPA) to streamline business processes

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



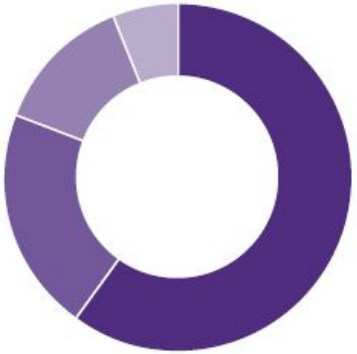
Please characterize the status of your citizen digital identity initiative.

- 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%

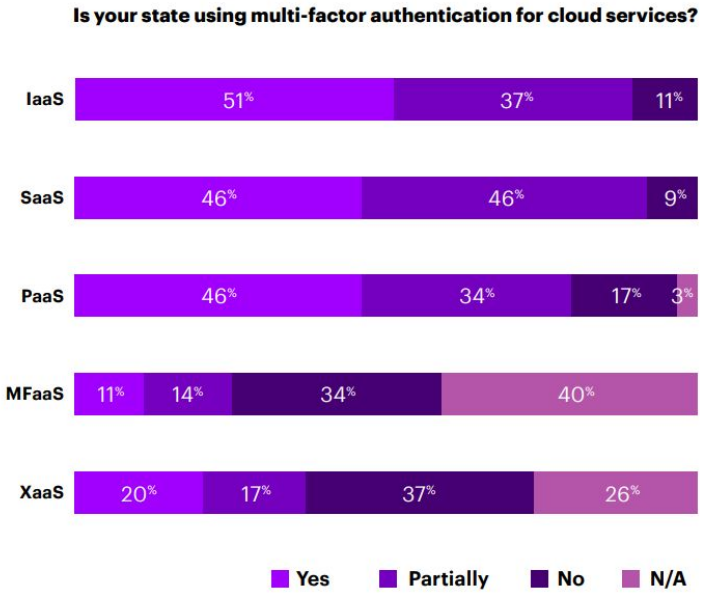
Investment optimization

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

NASCIO

Grant Thornton

CompTIA


Is your state using multi-factor authentication for cloud services?
IaaS
51%
37%
11%
SaaS
46%
46%
9%
PaaS
46%
34%
17%
3%
MFaaS
11%
14%
34%
40%
XaaS
20%
17%
37%
26%
Yes
Partially
No
N/A

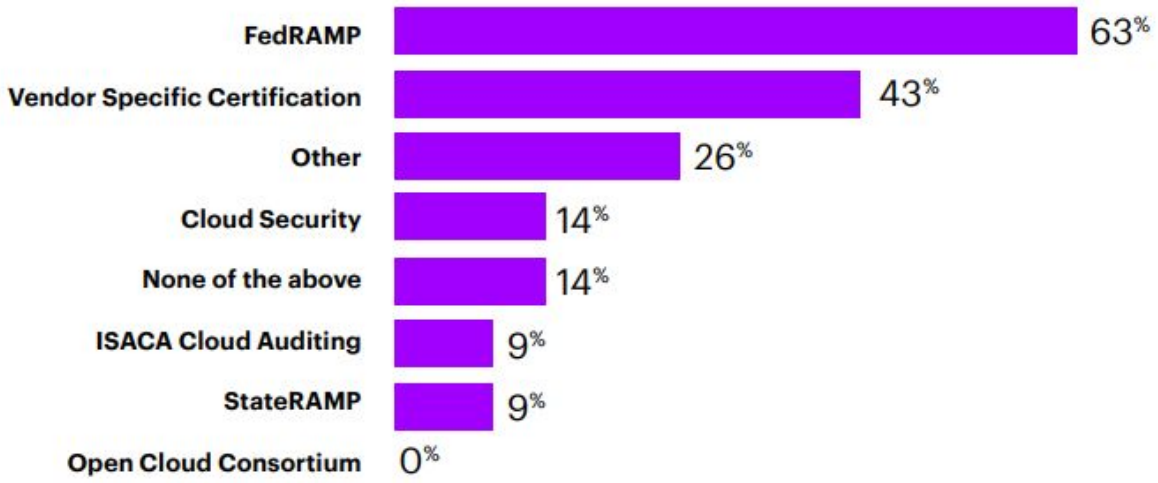
Possible Actions:

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

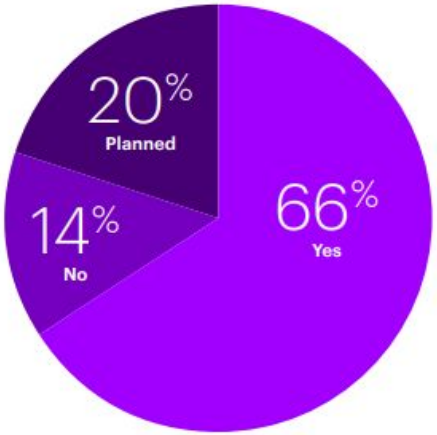
Incorporate end user cloud awareness education such as phishing, spearfishing, smishing and other threat profiles that can occur as a distributed workforce accesses cloud computing from non-centrally secured locations. (**Maturity level 2**)

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**)

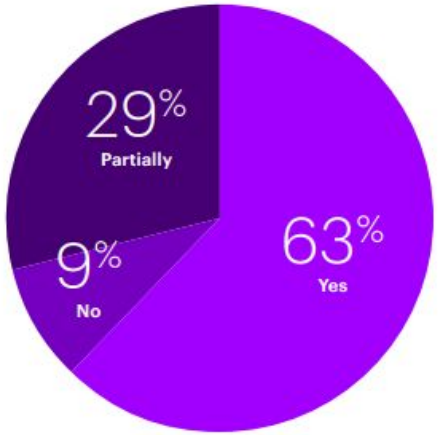
Which of the following cloud certification/standards programs does your state require?



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

www.nascio.org/resource-center

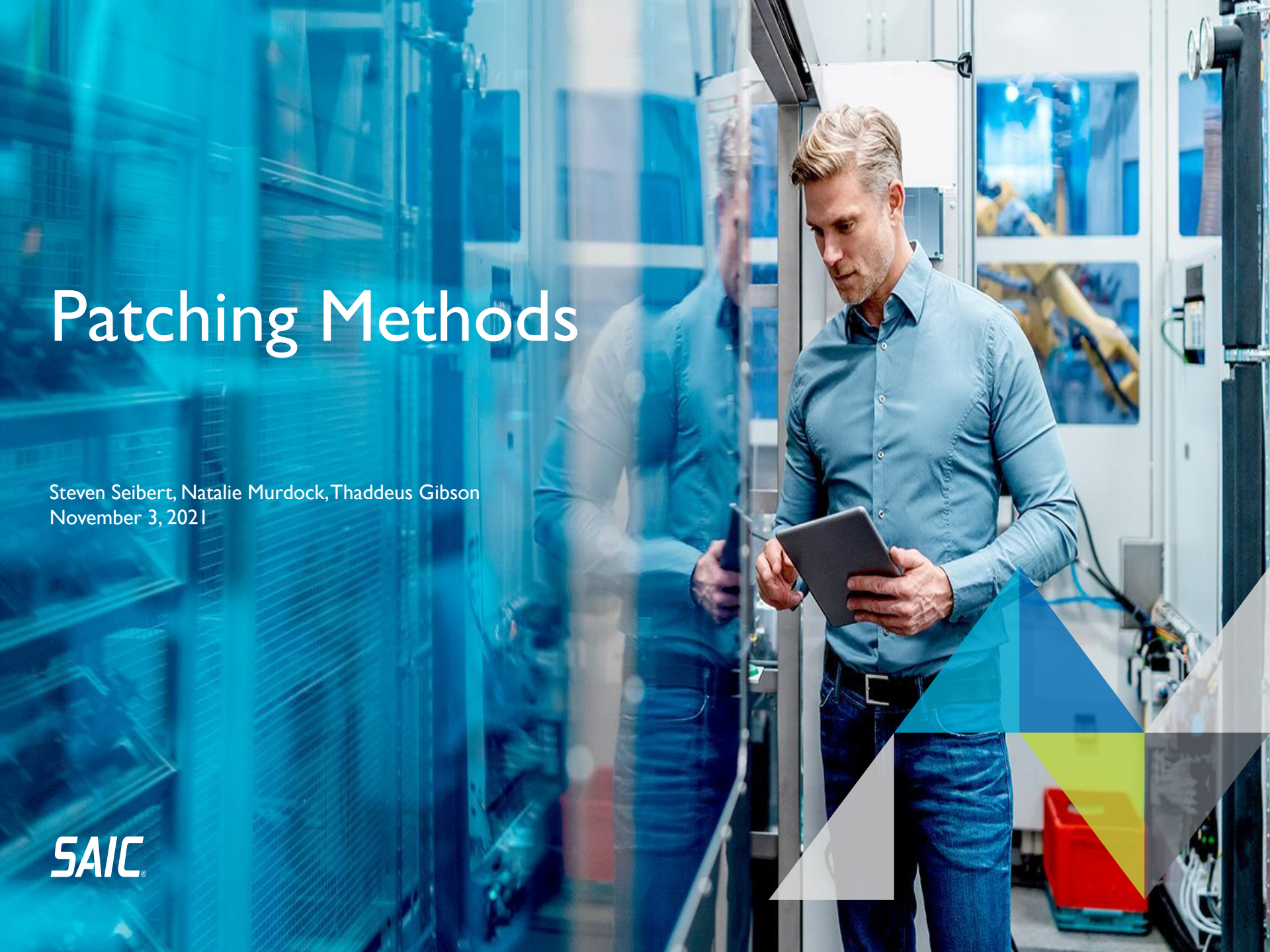
mward@nascio.org

LET'S BE FRIENDS
FOLLOW US

NASCIO
NASCIOmedia
NASCIO

Patching Methods

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



SAIC

Table of Contents

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

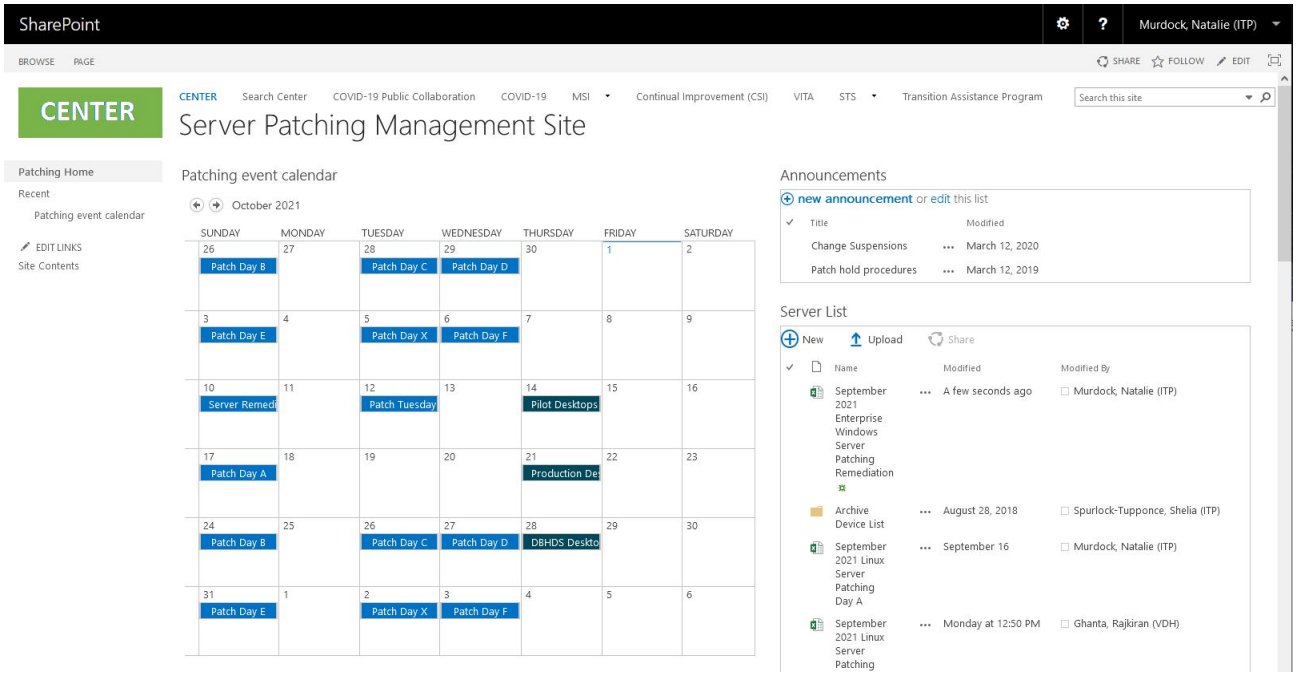
SAIC

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



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

SAIC

Schedule:

Patch Tuesday is the 2nd Tuesday

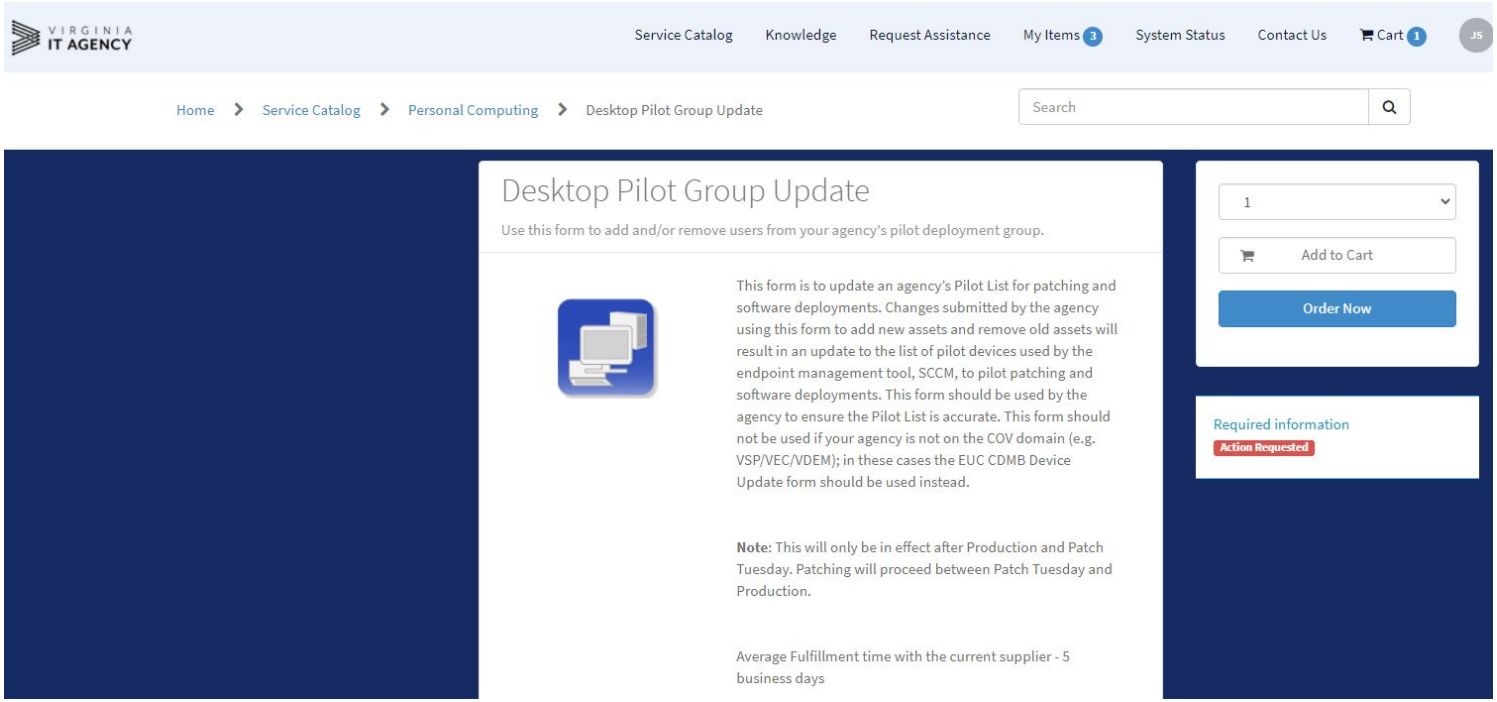
Pilot is the Thursday following Patch Tuesday beginning at 6PM

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

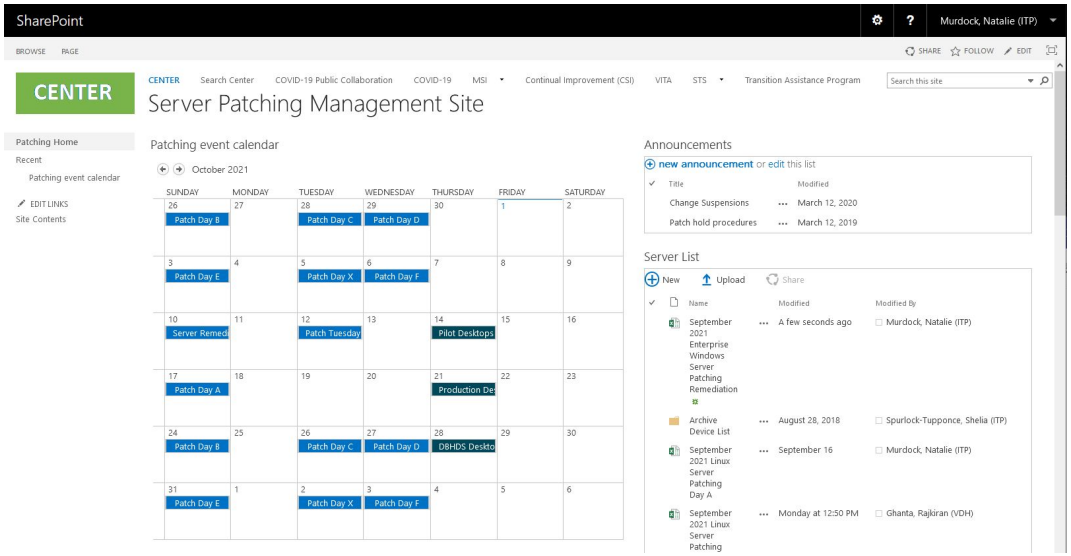
Navigate to the Service Catalog and select Desktop Pilot Group Update and complete complete the form.



Sharepoint site

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

Patching Event Calendar
Monthly Patch Announcement



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?

VIRGINIA
IT AGENCY

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

VIRGINIA
IT AGENCY

THANK YOU FOR ATTENDING!