



# USAccess Blue Top Newsletter

October 27, 2016

Volume 9, Issue 20

- [Upcoming Meetings and Trainings](#)
- [USAccess Software Release v10.0](#)
- [Mandatory PIV card login for roleholder portals](#)
- [Construction to Sacramento, CA DOI USAccess site parking lot](#)
- [Service Enhancements](#)
- [Security Tip](#)

---

## Upcoming Meetings and Trainings

### User Group Meeting

- **Tuesday, November 15, 2016, 10:00am - 12:00pm**
- Location: GSA Central Office 1800 F Street, NW, Room: 3042
- Conference Line: [1-888-455-1864](tel:1-888-455-1864), Passcode: 5887966

### Customer Advisory Board (CAB)

- **Tuesday, November 15, 2016, 1:00pm - 2:00pm**
- Location: GSA Central Office 1800 F Street, NW, Room: 3042

### Registrar Refresher Training

- **Thursday, November 10, 2016, 2:30pm - 3:30pm**
- Location: <https://meet.gsa.gov/r1njwtxf41/>, [888-455-1864](tel:888-455-1864) passcode: 3611044

### Registrar Classroom Training

- **November 16-17, December 7-8**
- Location: HPE, Chantilly
- Contact [Jim Schoening](#) for information

---

## USAccess Software Release v10.0

The USAccess Software Release v10.0 is now scheduled for November 19, 2016. This release launches the PIV-I pilot with the Department of Justice, Department of Commerce, and the Department of Interior, as well as some changes that are visible to all customers.

## PIV-I related changes visible to all USAccess role holders

- **PIV-I search criteria in applicant status report (ASR):** All agency role holders running the ASR will see PIV-I as a value to filter against. However, only agencies participating in the pilot will be able to use it.
- **New credential option indicator in adjudication:** A new field will appear on the Record Background Check Results tab in the Adjudication Portal that indicates they type of credential the Applicant will receive.
- **PIV-I activation portal/pilot desktop icon:** All Activators working on Light Activation, Light Credentialing Solution or Fixed Activation workstations will see a PIV-I pilot activation icon on their desktops. However, it will not work unless their Agency is a pilot customer.

## PIV-I changes visible only to PIV-I pilot agency role holders

- **Sponsorship Changes:** Within the same agency, Applicants can only be sponsored for one type of credential, either a PIV or a PIV-I, but not both.
- **Adjudication Changes:** With PIV-I, background check are not considered when running the pre-issuance validation rules, unless an Agency opts in to record PIV-I Agency Specific Adjudication (PIV-I ASC) results.
- **SIP/Bulk upload changes:** The SIP Service and bulk upload will be updated so the new value of PIV-I will be accepted.
- **Card differences:** Physical and on card
- **Activation changes for PIV-I:** There will be a new Pilot PIV-I desktop icon that appears on the desktops of fixed and light systems that needs be used to activate PIV-I credentials.

## Other Release v10.0 Changes

- **Remove lock on sponsorship record when record is set to print:** The applicant's sponsorship record will no longer be locked for editing while the Applicant's card is in an "issuance request" (IRQ) status or during the printing or shipping process.
- **Combine ASR and Supplemental ASR Reports in to a single report and add issuance sub-status:** The ASR and ASR Supplemental reports will be combined into a single report.
- **Auto terminate cards that are delivered but not activated after 1 year**
- **Remove required field validators in document validators in document validation screen of Security Officer Portal**
- **Correct OPM submission issue when no flat prints exists:** The adjudicator portal will be updated to indicate that the fingerprint package cannot be sent to OPM as it does not contain the same amount of roll and slap fingerprint images.
- **Correct SIP so Country of Citizenship (COC) value is returned**

## System Changes

- **Apply changes to improve system workflow**

For more details on PIV-I and Release v10.0 please read the Updated Release Notes posted to the Agency Lead Portal on October 27, 2016.

## Mandatory PIV card login for roleholder portals

Currently, roleholders have a choice to use their username and password or their PIV card to get into some of the USAccess roleholder portals. **However, effective January 7-9, 2017, all USAccess roleholder portals will require a PIV login.** This date coincides with scheduled mandatory maintenance.

### The following portals already require a PIV login:

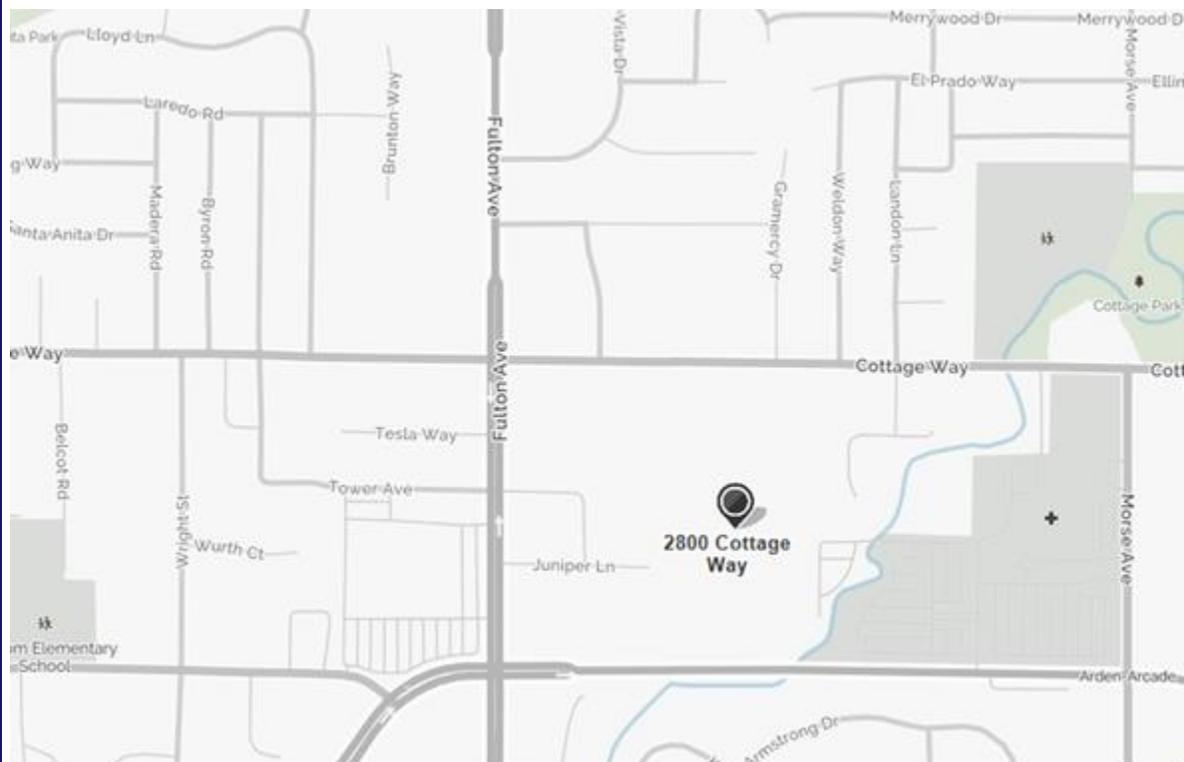
- Assured Identity (Enrollment and Attended/Unattended Activation)
- PCA (Activation and Local Print)
- Credential Inventory Tool
- Site Manager

### The following portals will be affected by the change:

- Assured Identity (Sponsorship, Security Officer, Adjudication)
- Report Viewer
- TRACKS
- Role Administration
- Self Service Password Reset

MSO will continue to publicize this requirement in the time leading up to this change.

## Construction to Sacramento, CA DOI USAccess site parking lot



The Sacramento, California Department of Interior facility parking lot will be undergoing construction over the next several weeks. **Between the weeks of September 6, 2016 to November 21, 2016 there will not be any onsite parking available for the employees of the Department of Interior or applicants attending the USAccess Center.**

Due to the parking situation, individuals with USAccess Center appointments are asked to arrive 45 minutes to 1 hour ahead of your scheduled appointment time to allow you to find alternate parking. **Please note, the only entrance to the USAccess Center will be from the Cottage Way Entrance - no one will be able to access the Alta Arden Entrance.**

The new hours of operations are: Monday and Tuesday only from 7:00am - 11:45am and 12:45pm - 4:00pm.

---

## Service Enhancements

### Changes/updates since last Blue Top

- Added OPAC Combination for American Battle Monuments (ABM)
- Provide SIP Client support of HHS OIG

### Planned changes

For any maintenance downtime periods, please schedule some buffer time to resume enrollment and activation appointments to account for any unanticipated delays in service.

- Maintenance is planned for the USAccess service on Saturday, November 5. The USAccess service will be unavailable for most of the day.
- USAccess Software Release 10.0 has been rescheduled for November 19. Please see the updated draft release notice posted on the Agency Lead Portal for more information on what is included in this release. This release will enable the PIV-I pilot for our participating agencies among other changes.
- Maintenance is planned for the USAccess service on Saturday, December 3. The USAccess service will be unavailable for most of the day.

---

## Security Tip

### USB Devices Best Practices

**According to USAccess policy, plugging any unknown or unauthorized USB device in to the USAccess computers is not permitted.** Unknown USB devices are those not provided and approved by your agency or those not exclusively used by you. USB devices shared with colleagues may fall into this category. Unknown USBs and other external devices can pose a significant threat to your agency's system and data as well as your personal data. It is important that you use caution when plugging in any external unknown device. If you are not the only person that used the device you

cannot be absolutely sure that it is not infected with viruses or malware without it being scanned. Most virus tools or the helpdesk can be used to scan the device. In extreme cases, plugging in an unknown device can destroy your system. The only foolproof way to assure that your system cannot be affected by a USB device is not to use a USB device on your computer.

A good practice is to keep personal and government USB devices separate. Mixing personal and government storage devices not only violates agency security policies it can potentially pass along viruses and malicious software. Introducing a virus into the agency network can lead to the theft of proprietary data. Conversely, if the network security tools employed by your agency successfully stops a threat from an infected USB device your personal system may be unable to eliminate it, introduce the malicious code into your less protected environment, and place your personal system and information at risk.

A few quick tips to help protect your data and systems:

- **Do not plug in any unauthorized USB devices into your USAccess Stations**
- Use encryption with passwords to protect all sensitive data. (Your agency and your personal data).
- Keep software up to date.
- Disable the autorun function.

If you suspect that you have received a suspicious or unknown USB device report it to your agency helpdesk.

---

To subscribe to this newsletter click the green envelope in the "Stay Connected" section of the footer below.

Contact Sharon Meng ([Sharon.Meng@gsa.gov](mailto:Sharon.Meng@gsa.gov)) to be added to USAccess distribution lists.

STAY CONNECTED:

