



# Blue Top Newsletter

## Upcoming Meetings and Training

Meeting/Training	Date & Time (EST)	Location	Dial-In Info
User Group	Tue, May 19 9:00-12:00	GSA Central Office 1800F St. NW Conference Rm. 3046	888-455-1864 Passcode: 5887966
Derived Credential Working Group	Wed, May 20 10:00-12:00	GSA Central Office 1800F St. NW Conference Rm. G143	866-556-0154, Passcode: 2132069
CAB	Thu, Jun 4 9:30 to 12:00	Grant Thornton 333 John Carlyle Dr., Alexandria, VA 4th Fl. Conf. Rm	No Telecon Provided
Registrar Classroom Training	Wed and Thu Jun 10-11 Jul 15-16 Aug 12-13	HP Chantilly, VA	Contact Jim Schoening for information or to Register

Special Points of Note:

Now found on  
[www.fedidcard.gov](http://www.fedidcard.gov):

- > Service Order Requests and Test Card Orders
- > Role Holder Web Based Training Registration
- > Deployment Activities and USAccess Center Status Alerts
- > Contact Steve Sill ([Stephen.sill@gsa.gov](mailto:Stephen.sill@gsa.gov)) to be added to User Group (UG) distribution list.
- > Contact Jim Schoening ([jim.schoening@gsa.gov](mailto:jim.schoening@gsa.gov)) for Registrar Classroom Training sign up

## USAccess Derived PIV Credential Industry Day Summary

The USAccess Derived PIV Credential Industry Day was held on April 27 at GSA Headquarters. Industry Day provided the opportunity for the MSO and its Customer Agencies to see various vendor solutions that currently exist to help inform our decision on incorporating a derived PIV credential solution into our core service offering.

The Industry Day presentations included:

- *An Overview and Status of Derived PIV Credentials And Associated Test Guidelines*, provided by Hildegard Ferraiolo, PIV Program Lead, NIST
- *Derived PIV Application and Data Model Test Guidelines (NIST SP 800-166 Draft) - Status Update*, provided by Hildegard Ferraiolo, PIV Program Lead, NIST
- *FIPS 201 Evaluation Program*, provided by Chi Hickey, Identity Assurance and Trusted Access Division, GSA

### Inside this issue:

Training Calendar	1
Spotlight Articles	1-3
Service Enhancements	4
Security Tip	4

## **Industry Day Continued**

The Industry Day vendor demonstrations included:

- Entrust
- Intercede, TriVir, Symantec, NetIQ, Census
- HP, CyberArmed
- XTec

Presentations and notes with all questions asked in each demonstration were distributed to attendees on May 6. Please contact the MSO if you were not able to attend the event but would like to review the notes.

There were 143 total participants from 21 agencies in attendance. The majority of feedback has been positive and indicates that Industry Day has helped the Derived Credential Working Group move forward in the derived PIV credential decision making process.

## **Fixed Infrastructure Windows 7 Workstation Replacement Update**

The schedule for fixed workstation replacement is posted on the Agency Lead Portal (ALP). This schedule includes the planned timeframes for fixed site Prep Calls, Windows 7 equipment shipments and Install Calls.

### **Prep Calls Completed for Waves 1-9**

Prep calls are complete for Waves 1-9. Our last set of prep calls for Wave 10 will be completed by Friday, May 22. We appreciate all of you who have kept to your schedules and attended the calls. Sites that attended a prep call are now eligible for equipment shipping. **If a site does not attend a call, equipment will not be shipped.** If your site did not attend their scheduled call, please contact the MSO immediately to have them attend these last few prep calls.

### **Windows 7 Equipment Shipping**

Equipment has shipped for Waves 1-7. Wave 8 should complete shipping by end of this week.

Emails were sent to site POCs with shipment tracking information and instructions for preparing for the install call. Please look for the shipment email and be sure to follow the steps to prepare for and schedule the install call within 2 weeks of equipment arrival on site.

## **Fixed Infrastructure Windows 7 Workstation Replacement Update Continued**

### **Install Calls/Site Recertifications**

As of Friday, May 8, we've certified/held install calls for 120 sites and are more than halfway to our goal of upgrading all fixed centers to Windows 7.

**As a reminder, please prepare for your Install Calls.** When a site completes the following steps before the call, we can complete an install in about an hour. When they are not completed, **they can take up to 3 hours.**

**Please complete the following before your install call:**

- Registrars/Activators know UPN/Password (refer to USAccess Windows 7 Workstation Replacement Guide)
- Set up Windows 7 machines 1 hour prior to install call (refer to USAccess Win 7 Quick Install Guide)
- Line up Applicant to activate or update card during install call (needed to recertify site)
- Have Site POC, Local IT and Registrars/Activators on call

### **Weekly Reports—Please reach out to MSO if you have not received them**

Reports are sent to the MSO on a weekly basis (on Mondays) that show Agency Leads the schedule for their fixed sites, as well as their progress in meeting all of their milestones. If you have not received a report, please reach out to the MSO.

## **Finance Reminder**

As a reminder to all of our customer agencies, please be sure to maintain sufficient funding for your HSPD-12 services. The IA addendum form used to obligate additional funding and instructions for completing it can be found on the FedIDCard.gov website under the Customer Agencies tab in the Onboarding Process section. Please feel free to contact Spiro Papagjika ([spiro.papagjika@gsa.gov](mailto:spiro.papagjika@gsa.gov)) or Meredith Rose ([Meredith.rose@gsa.gov](mailto:Meredith.rose@gsa.gov)) with any funding-related questions.

## **Service Enhancements**

### **System changes since last Blue Top**

- Maintenance was completed as scheduled on Saturday, April 25, Saturday, May 2 and Saturday, May 9.

### **Planned changes**

- Maintenance is scheduled for Saturday, May 30 for most of the day. Please plan for the USAccess Service and role holder portals to be unavailable for most of the day.

## **Security Tip**

### **Protecting Your Government Owned Equipment and Personally Identifiable Information**

Agency workplaces and telework provide great flexibility in how we accomplish our jobs, that flexibility requires each of us to be diligent in how we properly handle and secure our Government owned equipment and Personally Identifiable Information (PII).

Below are some tips that each of you should make part of your daily routine whether you are physically in the office or working remotely. Please take a moment to review them carefully.

Top Tips for Keeping PII and Government Owned Equipment Secure in a Flexible Workplace:

- Lock your computer when you step away
- Secure your agency issued laptop and other mobile devices
- Protect and secure documents when you send them to the printer
- Don't leave documents that have PII out on your desk when you're not there
- Lock all PII documents in a secure storage unit when you're not actively working with them
- Encrypt all PII being sent outside of your agency network.

Every federal employee has a responsibility to make sure their Government owned equipment and sensitive or Personally Identifiable Information is secured.