



Blue Top Newsletter

Upcoming Meetings and Training

Meeting/Training	Date & Time (EST)	Location	Dial-In Info
Workshop on SPs Supporting FIPS 201-2	Wed and Thurs Mar 3-4	NIST, Administration Building, Portrait Room, 100 Bureau Drive, Gaithersburg, MD 20899	Registration info: http://www.nist.gov/itl/csd/fips201-2_workshop_2015.cfm
Registrar Classroom Training	Wed and Thurs Mar 18-19 Apr 8-9	HP Chantilly, VA	Contact Jim Schoening for information or to Register
CAB	Thurs, Mar 5 9:30 to 12:00	Grant Thornton 333 John Carlyle Dr., Alexandria, VA 4th Fl. Conf. Rm	No Telecon Provided
User Group	Tue, Mar 17 9:00-12:00	GSA Central Office 1800F St. NW Conference Rm. 3046	888-455-1864 Passcode: USER GROUP

SSP IV Award Update

The USAccess Managed Service Office (MSO) announced the award of SSP IV to XTec, Inc. on Friday, February 20, 2015. A Government Accountability Office (GAO) protest has been initiated by HP Enterprise Services, and a stay of performance was been requested. GSA Contracting issued a work stoppage on Friday, February 27. Once it has completed its review, GAO will issue a recommendation to GSA for resolution of the protest. No further transition activities can take place by the award winner, XTec, until the protest has been resolved. It is not GSA’s intent to vacate the award, as was done in the Fall of 2014 during the initial protest, but to allow GAO to fully examine the acquisition and make a recommendation ruling.

This action will not have any effect on the current service. GSA has strongly committed itself to continued support for the USAccess service, and will not permit any contract issues to interfere with or interrupt the service.

Special Points of Note:

Now found on
www.fedidcard.gov:

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

Inside this issue:

Training Calendar	1
Spotlight Articles	1-3
Service Enhancements	5/6
Security Tip	7

SSP IV continued

Transition activities will begin as soon as cleared by GSA's Contracting and General Counsel. The full implementation timeline will be pushed to the right, but the net result will be uninterrupted services for our agency customers. Our transition plan includes stringent requirements for technical and program interchanges with customer leads, and the discovery process will assure that the eventual transition will be seamless and uninterrupted.

We will update you as we have more information and appreciate your patience as the protest is resolved.

Change to Photo Capture Screen

There is a New Custom Camera Exposure checkbox on Photo capture page in Enrollment application. Here are the details:

- This new checkbox allows the Registrar to adjust the exposure setting of the camera to lighten or darken a photo.
 - Please note that Registrars should still follow the recommendations in their Registrar Quick Reference Guide on setting up the kit with adequate natural lighting as this is the primary way to achieve the best photo.
- This new custom setting should ONLY be used if the photos do not appear correctly after following the guidelines included in this guide for setting up the LCS kit to utilize natural lighting.
- To use the feature, Registrars should first leave the checkbox unchecked, and take a picture.
 - If the photo lighting is acceptable, then proceed with enrollments and do not check the Custom Camera Exposure checkbox.
 - If the photo appears too light or dark, check the Custom Camera Exposure checkbox, then slide the bar to a lighter setting (to the left) or darker setting (to the right), depending on the need. Then take another picture.
- Registrars can adjust the slide bar as needed and retake photos until desired lighting is achieved. Once achieved, the Registrar can proceed with the enrollment.

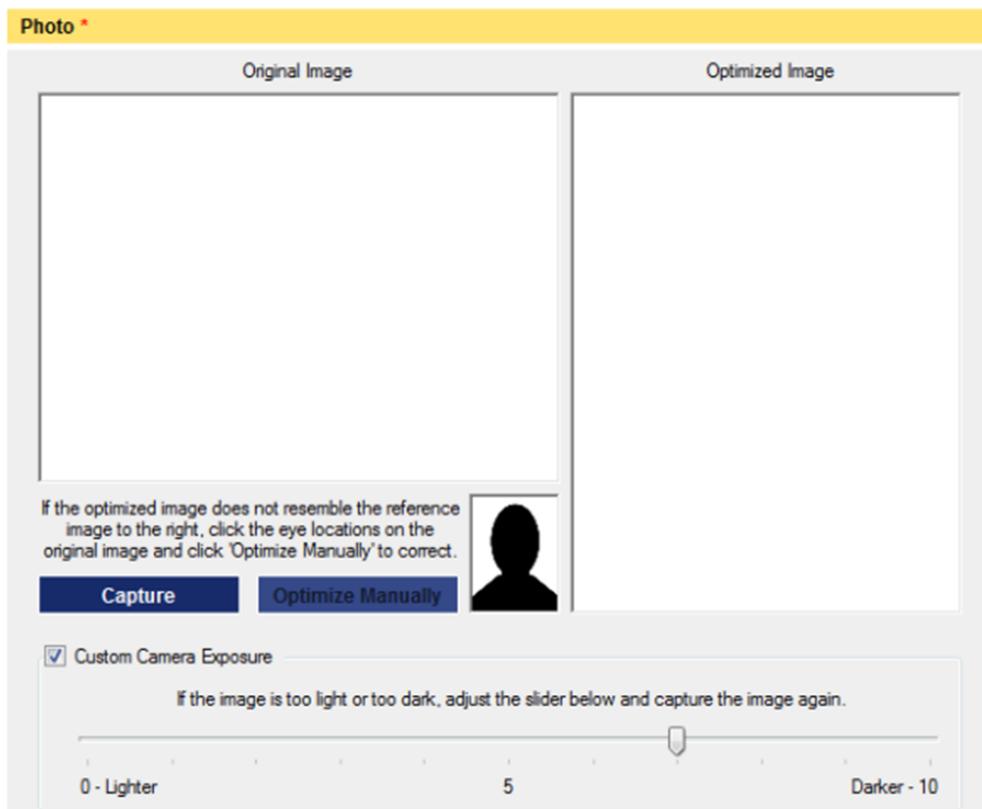
Photo Capture Screen continued

- The Enrollment application has now set the default camera exposure setting to this new custom level, so Registrars do not need to reset for future enrollments.

NOTE: Registrars that use an LCS kit that contains a Canon Rebel T3 or T5 camera may find that using the custom setting may not lighten or darken the photo to the same degree as when not using the custom feature.

For example, when using the custom setting, a photo that needs darkening may actually appear lighter when using the custom feature. This is because the custom exposure range is not as wide as the exposure range provided by the T3 or T5 camera when used in auto mode (i.e.; not checking the Custom Camera Exposure box.)

If using a Canon T3 or T5 camera, Registrars should attempt to re-adjust the position of the kit and camera to make best use of natural light.



New Photo Capture Screen

Windows 7 Fixed Workstation Update

An email has been sent out to Agency Leads asking for information to help the MSO develop a schedule for replacing the workstations. The email includes a list of Agency sites, and asks Leads to confirm or provide Site, IT and Registrar POC information for each site. Agencies were also asked to indicate any scheduling preferences the MSO should take into consideration when prioritizing the installation schedule. Please respond to the USAccess Help Desk by Friday, February 27. **If the help desk does not receive information from you, your sites will not be scheduled for upgrade. Any sites that are not upgraded by mid-June will not be allowed to operate within the USAccess infrastructure as the MSO ATO is scheduled for this summer.**

Once we have the schedule finalized, it will be distributed so Agencies can review and request any last minute changes before we begin sending out Prep Call emails.

Registrar/Activator Training Calls and Customer Calls to be repurposed to Win7 Upgrade Calls

The USAccess Program will soon be commencing a Windows 7 Upgrade process. During this time there will be weekly Prep Calls with pending upgrade sites. As a result, the timeslots currently being used for Refresher/Activation Refresher Training and Customer Calls will be repurposed for Windows 7 Prep Calls. The Upgrade process is scheduled to complete in June. At this point the Refresher/Activation Refresher Training calls will be reinstated.

USAccess Agency Lead Portal Reminder

On November 2, 2014, the USAccess Agency Lead Portal transitioned from the SharePoint platform to the Salesforce platform. This was a GSA-wide initiative. The Salesforce admin team sent all current ALP users their new usernames and directions to set up a password at that time.

As a reminder, we'd like to share the URL for the site fas.my.salesforce.com. All users of the ALP have a username that is your federal agency email address with the suffix *.gsacomunity*. For example, *john.doe@xyz.gov.gsamcommunity*. If you've forgotten your password simply click on 'Reset Password' on the Salesforce login page.

If login issues persist, please contact Fassfsupport@gsa.gov.

[Connect.gov Program Seeking Volunteers](#)

Do you have a PIV card or CAC? The [Connect.Gov](#) program is seeking volunteers to participate in a short 10 minutes testing of the Connect.Gov solution. Your participation and assistance is extremely valuable to the program!

Please respond to Angela (Angela.M.Lagneaux@usps.gov) and Ashrab (ashahmed@deloitte.com) with the following information and a member of the USPS team will provide you specific instructions to perform the testing, which can be executed remotely at your convenience.

- Whether you have a PIV card or CAC
- The issuing agency

About Connect.Gov: The Connect.Gov service enables citizens to access online Federal Government Services in a convenient, privacy enhancing, and secure manner without having to create a new login. To learn more about Connect.Gov, please click [here](#).

[Service Enhancements](#)

[System Changes Since Last Blue Top](#)

New Light Credentialing Solution (LCS) and Light Activation (LA) installers now posted on SFTP server

The installers were posted on Tuesday, February 17. Release notes are available for the LCS and LA v3.4 installers on the Agency Lead Portal.

The LCS upgrade is a MANDATORY update, as it renews a certificate required for enrollments that is set to expire March 12. If LCS kits are not updated to v3.4 by March 12, they will receive an error message when attempting to launch the enrollment application.

The LA installer is a RECOMMENDED update that includes updates for Java and ActivClient (same versions as those included with LCS v3.4). LA machines are not affected by the enrollment certificate that expires on March 12, 2015. While LA systems with v3.2 software will still function in the USAccess infrastructure after March 12, the MSO highly recommends that Agencies update their machines to v3.4 to deploy the latest version of Java and receive the ActivClient hotfix.

Service Enhancements continued

Agencies can update LA and LCS machines right now as v3.4 works within the existing USAccess infrastructure.

Fixed enrollment workstations must also have the updated enrollment certificate by March 12. Fixed workstations will be updated using our automated update distribution method, therefore no action is needed by Agencies.

NOTE: Some agencies have experienced issues accessing the SFTP server using Internet Explorer recently. If you receive an “Internet Explorer cannot display the webpage” message when attempting to access the SFTP server, please check the TLS configuration in your IE settings. From the Tools>Internet Options>Advanced tab, verify the User TLS 1.0 and TLS 1.1 boxes are checked.

Also, after logging in, a user may be prompted to install an Upload/Download Wizard. This wizard is not necessary to download the files. A user can choose to install it, or choose to disable the wizard. Either option will still allow the installer files to be downloaded.

Planned Changes

SIP service certificates expiring in Mid-March 2015

SIP customers also need to update their SIP interfaces with a new service by mid-March. An email was sent to SIP customers the week of February 2 informing them of the need update the certificates and provided ETAs on when they will be available for each environment (Test, Staging and Production.)

Routine Maintenance Planned for February 28

Routine maintenance is planned for February 28. Please plan for the USAccess service and role holder portals to be unavailable for much of the day.

Security Tip

Security Incident Responses

This week's security tip covers how to respond to security incidents involving USAccess. Please follow these steps to report an incident:

1. Contact your System ISSO or Agency ISSM within one (1) hour of the incident.
2. Your Agency ISSO or ISSM should contact the MSO Program Office
3. At a minimum, GSA will need the following information:
 - A brief description of the incident
 - A description of the types of Personally Identifiable Information (PII) involved (e.g. full name, Social Security Number, date of birth, home address, account number, etc.);
 - Date(s) of the breach
 - How it was discovered
 - Encryption or protected status of the PII if known
 - The name of the person(s) that the GSA MSO should contact for more information (contact information should include a telephone number, e-mail address, and street address if available.)
4. The GSA Security Team will work with your Agency Security Office to:
 - Determine what steps the Agency and individual should take to protect himself/herself from potential harm;
 - Determine what steps GSA will take to investigate the breach, mitigate losses, and to protect against any further breaches; and
 - Assign an Impact Level for the incident and determine the potential impact on GSA, the Agency or the potential for identity theft of the individual Three levels may be assigned.

The impact level assigned by GSA to the information breached will determine when and how the incident will be addressed. Higher Impact Levels may require additional information from you and your Security office. GSA Impact Levels are defined as:

Low - the loss of confidentiality, integrity, or availability is expected to have a limited adverse effect on organization operations, organizational assets or to individuals.

Moderate - the loss of confidentiality, integrity, or availability is expected to have a serious adverse effect on organizational operations or to individuals.

High - the loss of confidentiality, integrity, or availability is expected to have a severe or catastrophic effect on organizational operations, organizational assets, or to individuals.