



Blue Top Newsletter

Upcoming Meetings and Training

Meeting/Training	Date & Time (EST)	Location	Dial-In Info
CAB	Wed, June 1 9:30 to 12:00	GSA Central Office 1800 F St. NW Room 3042	No telecon provided
User Group	Wed, June 8 9:00 to 12:00	GSA Central Office 1800 F St NW Room 3334	888-455-1864 Passcode: 5887966
Registrar Refresher Training	Thu, June 9 2:30 to 3:30	Telecon/Webinar	888-455-1864 Passcode: 3611044
Registrar Classroom Training	Wed and Thu May 18-19 May 25-26 Jun 1-2 Jun 15-16 Jul 20-21	HPE Chantilly, VA	Contact Jim Schoening for information or to Register

FedIDCard.gov outage planned between May 27 through May 29

The FedIDCard.gov website will be down during Memorial Day weekend from Friday, May 27 at 8:45am through Sunday, May 29 at 1:00pm.

This outage will be due to a data center move that will impact FAS Production servers and the applications that run on them. Despite the fact that FedIDCard.gov will be unavailable, applicants will still be able to access the Scheduler using the direct link: <http://app3.timetrade.com/login.do?url=usaccess>

At this time we have not been made aware of any other planned outages following the one at the end of this month. This outage will not effect any of our other sites including roleholder portals, activations, or enrollments.

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 Alerts
- > Contact Sharon Meng (Sharon.Meng@gsa.gov) to be added to USAccess distribution lists.
- > Contact Jim Schoening (jim.schoening@gsa.gov) for Registrar Classroom Training sign up

Inside this issue:

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

LCS kits MUST have v.4.0 or v.4.0.1 installed in order to complete enrollments

The USAccess team upgraded the USAccess F5 Edge server on May 7. This was originally scheduled for April 23, but by Agency request, we delayed this update to allow Agencies to update their systems. An email was sent to Agency Leads on Wednesday, April 20 to inform them of the new date.

The F5 Edge server is used by LCS kits to connect to the USAccess service and complete enrollments. The new F5 configuration allows enrollment connections to use TLS 1.2 protocol. Before, it only supported TLS 1.0 and TLS 1.1. Now that the upgrade work is complete all LCS kits will need the new F5 desktop client included in Light Installers v4.0.0 or v4.0.1 in order to complete enrollments.

NOTE: Light Installers v4.0 that was released in early February 2016 includes the new F5 desktop client needed to complete enrollments following the May 7 upgrade. If agencies have already updated their LCS systems to v4.0, they will continue to work. However, we strongly encourage agencies to upgrade to v4.0.1 even if they are already on v4.0, as 4.0.1 includes fixes to known issues with v4.0, as well as the updated TLS protocol capability.

You know you have v.4.0 or higher if you have PCA on the desktop.

New Platform and URL for Refresher Training Web Conference

The MSO will now be using Adobe Connect as the platform used to present Registrar and Activator Refresher Training. This change results in a new URL to access the web conference. The old URL is no longer operational. Agency Leads should notify their Registrars and Activators of the new URL, provided below. As always, the presentation slides will be posted to TRACKS and the ALP prior to the training for those who choose to follow along offline.

New URL for Refresher Training: <https://meet.gsa.gov/r1njwttxf41/>

Adobe Connect is the same platform used successfully for the recent PCA and Sponsor Training sessions. Our findings have shown a higher success rate of connecting to a web conference using Adobe Connect than the previous platform.

An added benefit of using Adobe Connect is that the recordings of the Refresher Trainings can be viewed online. Links to the Registrar Refresher Training recordings will be posted on TRACKS, enabling Registrars and Activators to access the training directly. Previously, the recording files were too large to post to TRACKS. The May Refresher Training recording link will be posted to TRACKS and the ALP.

Role Holders can test connectivity to Adobe Connect using the following link:
https://meet.gsa.gov/common/help/en/support/meeting_test.htm

Mandatory PIV card login for roleholder portals

At this time some role holders have a choice to use their username and password or their PIV card to get into the USAccess roleholder portals. However, as an effort to enhance security, as of January 1, 2017, all USAccess roleholder portals will require PIV login. A list of the portals affected are as follows:

- Sponsorship
- Enrollment
- Adjudication
- Attended and Unattended Activation
- Report Viewer
- Credential Inventory Tool
- Site Manager
- Security Officer
- Print Operator
- TRACKS

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

Service Enhancements

Changes/updates since last Blue Top

- Completed maintenance as scheduled on April 27, April 30 and May 7th.
NOTE: The May 7th maintenance involved a change to the F5 to allow TLS 1.2 connections. Prior to this change, the F5 only supported TLS 1.0 and TLS 1.1. All LCS kits need the new F5 desktop client included in Light Installers v4.0.0 or v4.0.1 in order to complete enrollments. If your LCS kit is experiencing issues with enrollments following May 7, please verify the version of Light software you are running and upgrade to either v4.0 or v4.0.1. We strongly encourage agencies to upgrade to v4.0.1 even if they are already on v4.0, as 4.0.1 includes fixes to known issues with v4.0, as well as the updated TLS protocol capability.

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.

- **May 21.** Maintenance is scheduled for Saturday, May 21. The USAccess service and portals will be unavailable for most of the day. This release (Release 9.10) will apply several hotfixes to the CMS that are behind the scenes and do not have changes that are visible to users of the system or will impact how the system operates. This release also an update where the fingerprint templates located on the PIV card will be populated with the appropriate values per NIST SP 800-76-2 policy in the case of whether an Applicant has no fingerprints in the system or they are of poor quality. Currently in the system, the templates do not have a value in these cases. A draft release notice is posted on the Agency Lead Portal.
- **June 4-5.** Maintenance is scheduled for Saturday, June 4, and routine security scans on Sunday, June 5. The USAccess service and portals will be unavailable for most of Saturday, June 4, and roleholders *may* see slowness in the system on Sunday, June 5 while the scans are conducted. These dates are tentative and will be confirmed in the next Blue Top.

Security Tip

Just a reminder: no matter how much expertise and money your agency puts into securing its network and data assets—firewalls, security appliances, encryption, etc.—the human component of the security system is the most critical and quite often the most vulnerable. Social Engineering and Phishing are two techniques employed to attack the human component.

Social Engineering

Social Engineering is the manipulation of words and/or actions that are intended to establish a false sense of trust and confidence. Once trust is established, the attacker's objective is to ultimately induce a desirable response. When an unsolicited contact is asking for information, consider whether the person you're talking to deserves the information they're requesting and how the information may be employed by an attacker.

Social engineers have repeatedly shown that those who focus on technology alone to solve the problem of protecting an IT system and its data are addressing only part of the problem. They discount or ignore the evidence that the human component will always be the weakest link. Technology is important but minimizing the vulnerability of this weak link is the system user's responsibility.

Successful social engineering often depends on pressuring the target and not allowing time to think about their decision. If you find yourself dealing with someone and suddenly you feel pressured to make a decision, or to take some immediate action, you should stop and ask yourself; where is this pressure coming from - internal or external - and why am I being pressured? Unwarranted pressure is a big red flag and it should set off your alarm bells. Be wary if the contact does not match the person or message.

Phishing

Phishing attacks are closely related to social engineering and refer to the process where someone posing as a legitimate contact contacts you by email, telephone or in person. The purpose is to lure you into providing sensitive information. The information requested may then be used to access your user account, another user's account or agency assets.

Email phishing attacks will often include eye-catching or attention-grabbing statements. These attacks are designed to immediately get your attention. Phishing scams are wide and varied and typically include information request from someone claiming to have a legitimate authority. Communications that unexpectedly appear in you inbox from a senior agency manager that you do not typically deal with directly is a red flag. You may recognize the source - your agency's CIO office or IT Security Office, but the name is one that you do not recognize. Unless you are sure, you should not respond. If you are not sure, report it.

Many people will fall prey to social engineering or phishing attacks because the attackers understand human nature. These are sophisticated people that leverage this understanding to exploit human nature and our desire to be helpful and accommodating. Remember, attackers are skilled at establishing trust and then inducing a desired response.

Our defense begins with the understanding that we are all targets. A good personal policy is that when something doesn't seem right it isn't. Trust your gut instincts. If there is any doubt STOP and contact your ISSO or agency help desk and report it.