From: SM Communications
Sent: Tuesday, August 25, 2015 10:00 AM
Subject: USPS re:supply Issue 22 August 25, 2015

usps | re:supply
news our suppliers can use

Issue 22

August 25, 2015

CONTENTS

U.S. Postal Service Suppliers,

You are receiving this newsletter as you have registered your interest to do business with the U.S. Postal Service (USPS) or your e-mail is on file as a point of contact for a current or past contract. Please share this newsletter with your colleagues within your company as it contains important supplier related information about the Postal Service.

The Postal Service has launched the **CyberSafe at USPS** initiative focused on increasing awareness of cybersecurity threats and procedures USPS employees can follow to help protect systems and data. We are extending that message to our suppliers, and in particular, those suppliers' employees who have access to USPS systems.

We want you and your employees that have USPS ACE (Advanced Computing Environment) Active Directory access to be aware of two web based training courses that are now available to supplier personnel which are recommended to be completed by September 30, 2015 as mentioned in the article below. These two courses are *recommended* for contractors to increase awareness about information security at USPS and are *not* mandatory.

This issue is simultaneously being sent to USPS Supply Management employees for their information.

Thank you!

Cybersecurity Courses Now Available to Suppliers with Access to USPS Systems

Suppliers Share in Responsibility to Protect USPS Information and Networks

CyberSafe™
at USPS

The U.S. Postal Service is taking additional steps to increase the awareness of our supplier community regarding USPS information security. Each supplier employee with ACE Active Directory access now has access to two USPS Learning Management System (LMS) courses on information security. We recommend these courses be completed by **September 30, 2015.**

- 10024251: CyberSafe 101: Passwords and Phishing – 15 minutes
- 10021144: Our Shared Responsibility – 45 minutes

The instructions for supplier personnel with ACE IDs to access these courses are included below, starting on page 4.

For questions related to the IT: Security – Our Shared Responsibility course and the IT: Security – CyberSafe 101 course, please contact Gerri Wallace at *gerri.wallace@usps.gov* or Rose Tutera via e-mail at *rose.a.tutera@usps.gov*. If you need help with the Learning Management System (LMS), please contact *ELMS@usps.gov*.

Cybercriminals are hard at work 24/7, 365 days a year attempting to steal government, corporate, and personal information and it takes everyone's support to defend against them. We have increased our security posture and will continue to make improvements. We are relying upon our employees and the employees of our suppliers to play a key role in the protection of our network and information.

The Postal Service recently launched CyberSafe at USPS, an initiative to educate employees and the employees of our suppliers on critical cybersecurity topics. One of the first steps is to focus on increasing the information security awareness of our suppliers' employees who have active access to USPS networks.

Please help us spread the word to members of your team who have access to the USPS CyberSafe blue page, a central resource for important USPS cybersecurity information. The site is available at *CyberSafe at USPS*. Additionally, please share with your team the following tips:

- If you have a log-in credential (username/password) for any USPS system(s):
  - Never share this information with anyone or write it down.
  - Never use the same credential in other systems.

- If you are issued a USPS e-mail address:
  - Never auto-forward e-mails from another account to your USPS e-mail account.
  - Watch out for phishing e-mails that try to convince you to click on links or attachments, or enter information into a suspicious site.

- Information security incidents (including suspected or actual phishing scams) must be immediately reported to the USPS Computer Incident Response Team (CIRT) via telephone at 1-866-USPS-CIR(T) or 1-866-877-7247 or via an e-mail to *cybersafe@usps.gov* or *uspscirt@usps.gov*. Do not dismiss a suspected incident or discount its seriousness.

- For more information on USPS Information Security policies, please go to http://about.usps.com/handbooks/as805/welcome.htm.

- Additional cybersecurity resources focused on increasing the understanding of cyber threats and empowering the American public to be safer and more secure online are available through the U.S Department of Homeland Security (DHS) *Stop.Think.Connect.* national public awareness campaign. For more information please go to http://www.dhs.gov/stopthinkconnect.

We want to thank you for your continued support in helping the Postal Service deliver on its mission while protecting its network and information.

RETURN TO TOP

The Postal Service receives no tax dollars for operating expenses and relies on the sale of postage, products, and services to fund its operations.

ARE YOU REGISTERED TO DO BUSINESS WITH THE U.S. POSTAL SERVICE?

More than 14,700 suppliers have registered since our launch of the Supplier Registration site in July 2009.

All suppliers interested in doing business with the U.S. Postal Service should register their company in the Postal Service Supplier Registration system.

For more information, please go to *http://about.usps.com/suppliers/becoming/registration.htm*.

CONTACT US!

We value your questions and feedback to this newsletter. Please feel free to reply to this message with your feedback or mail to:

U.S. Postal Service
Supply Management Communications
475 L'Enfant Plaza, SW, Room 1100
Washington, DC 20260-6201

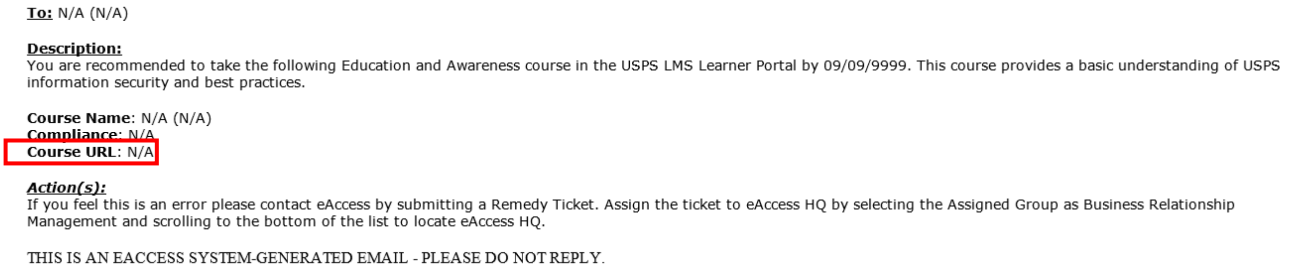
If you prefer not to receive future issues of *re:supply* from the U.S. Postal Service, click *SMCommunications@usps.gov* and type **Unsubscribe** in the Subject line.

To be added to our *re:supply* e-mail list, click *SMCommunications@usps.gov* and type **Subscribe** in the Subject line.

DID YOU KNOW ?
The CyberSafe at USPS site has tips and information to avoid phishing attacks.
CyberSafe

Instructions for Accessing Courses in LMS

Once you have been loaded to the **IT: Security – Our Shared Responsibility** course and the **IT: Security – CyberSafe 101** course, you will receive notification via email. The below is a sample image of that communication.



To: N/A (N/A)

Description:
You are recommended to take the following Education and Awareness course in the USPS LMS Learner Portal by 09/09/9999. This course provides a basic understanding of USPS information security and best practices.

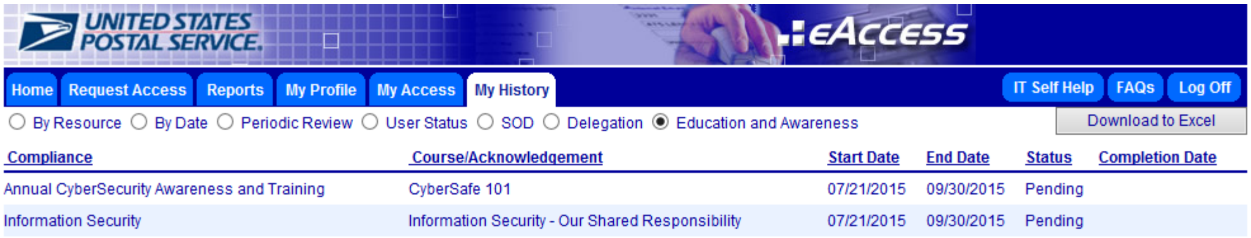
Course Name: N/A (N/A)
Compliance: N/A
Course URL: N/A

Action(s):
If you feel this is an error please contact eAccess by submitting a Remedy Ticket. Assign the ticket to eAccess HQ by selecting the Assigned Group as Business Relationship Management and scrolling to the bottom of the list to locate eAccess HQ.

THIS IS AN EACCESS SYSTEM-GENERATED EMAIL - PLEASE DO NOT REPLY.

> *Note:* the email will contain a direct link for the Learning Portal in the LMS on Blue (https://blue.usps.gov/wps/myportal/LMS). Click on the link in the email to access the courses.

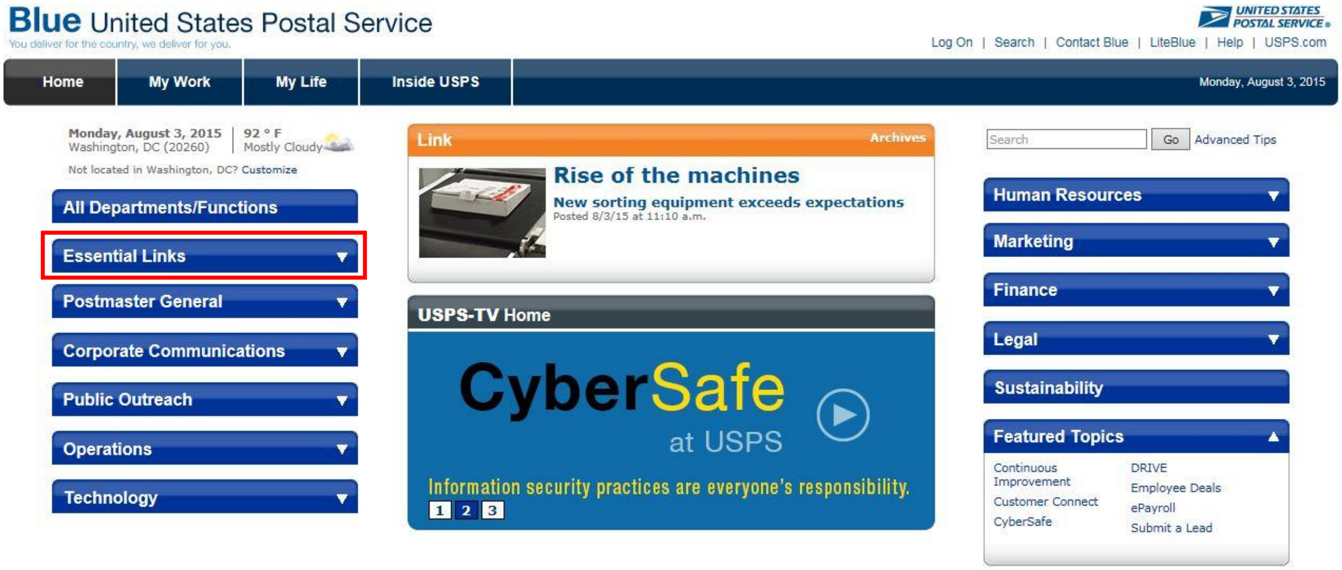
You can confirm that you have been given access to the courses via eAccess. Log onto eAccess and click on the "My History" tab. Click the "Education and Awareness" button. The courses will be listed there with a Pending status until you complete them.



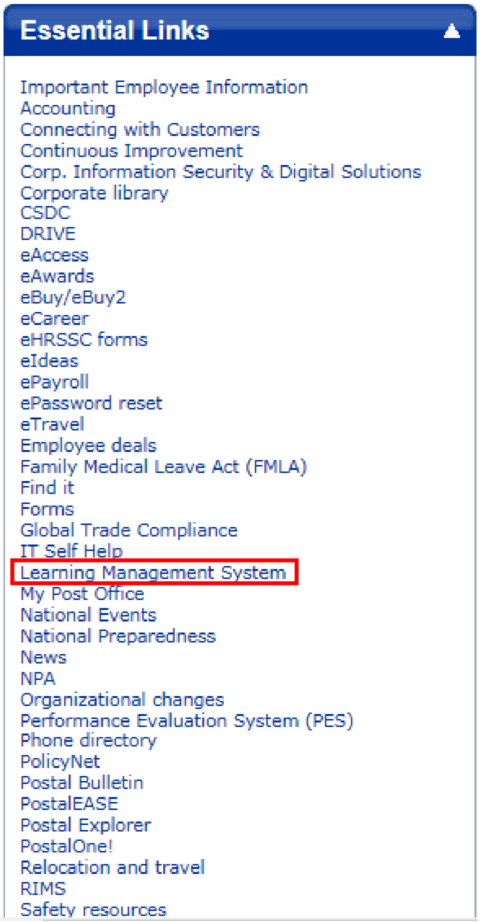
○ By Resource ○ By Date ○ Periodic Review ○ User Status ○ SOD ○ Delegation ● Education and Awareness

Compliance	Course/Acknowledgement	Start Date	End Date	Status	Completion Date
Annual CyberSecurity Awareness and Training	CyberSafe 101	07/21/2015	09/30/2015	Pending	
Information Security	Information Security - Our Shared Responsibility	07/21/2015	09/30/2015	Pending	

If you are unable to access the course via the link in the email, you can access the courses via the Learning Portal on Blue. Go to the Blue homepage. Click on "Essential Links."



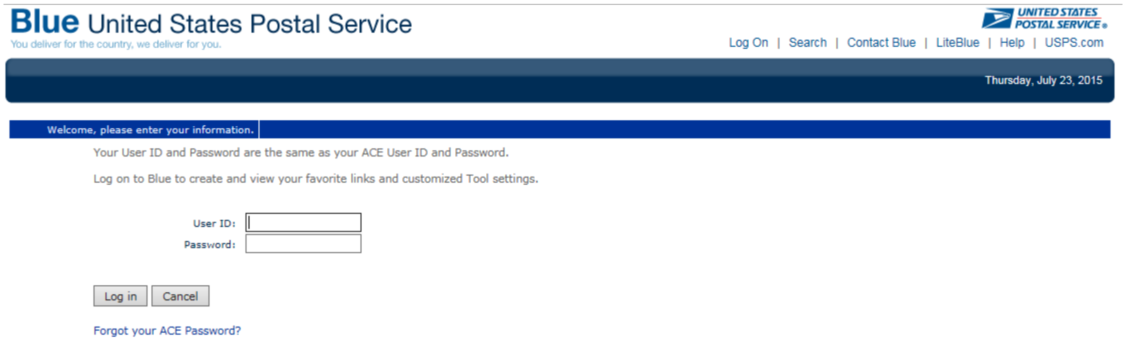
Click on "Learning Management System" in the Essential Links tab.



Essential Links

Important Employee Information
Accounting
Connecting with Customers
Continuous Improvement
Corp. Information Security & Digital Solutions
Corporate library
CSDC
DRIVE
eAccess
eAwards
eBuy/eBuy2
eCareer
eHRSSC forms
eIdeas
ePayroll
ePassword reset
eTravel
Employee deals
Family Medical Leave Act (FMLA)
Find it
Forms
Global Trade Compliance
IT Self Help
Learning Management System
My Post Office
National Events
National Preparedness
News
NPA
Organizational changes
Performance Evaluation System (PES)
Phone directory
PolicyNet
Postal Bulletin
PostalEASE
Postal Explorer
PostalOne!
Relocation and travel
RIMS
Safety resources

Log in using your ACE ID and password.



Blue United States Postal Service
You deliver for the country, we deliver for you.
UNITED STATES POSTAL SERVICE
Log On | Search | Contact Blue | LiteBlue | Help | USPS.com
Thursday, July 23, 2015

Welcome, please enter your information.

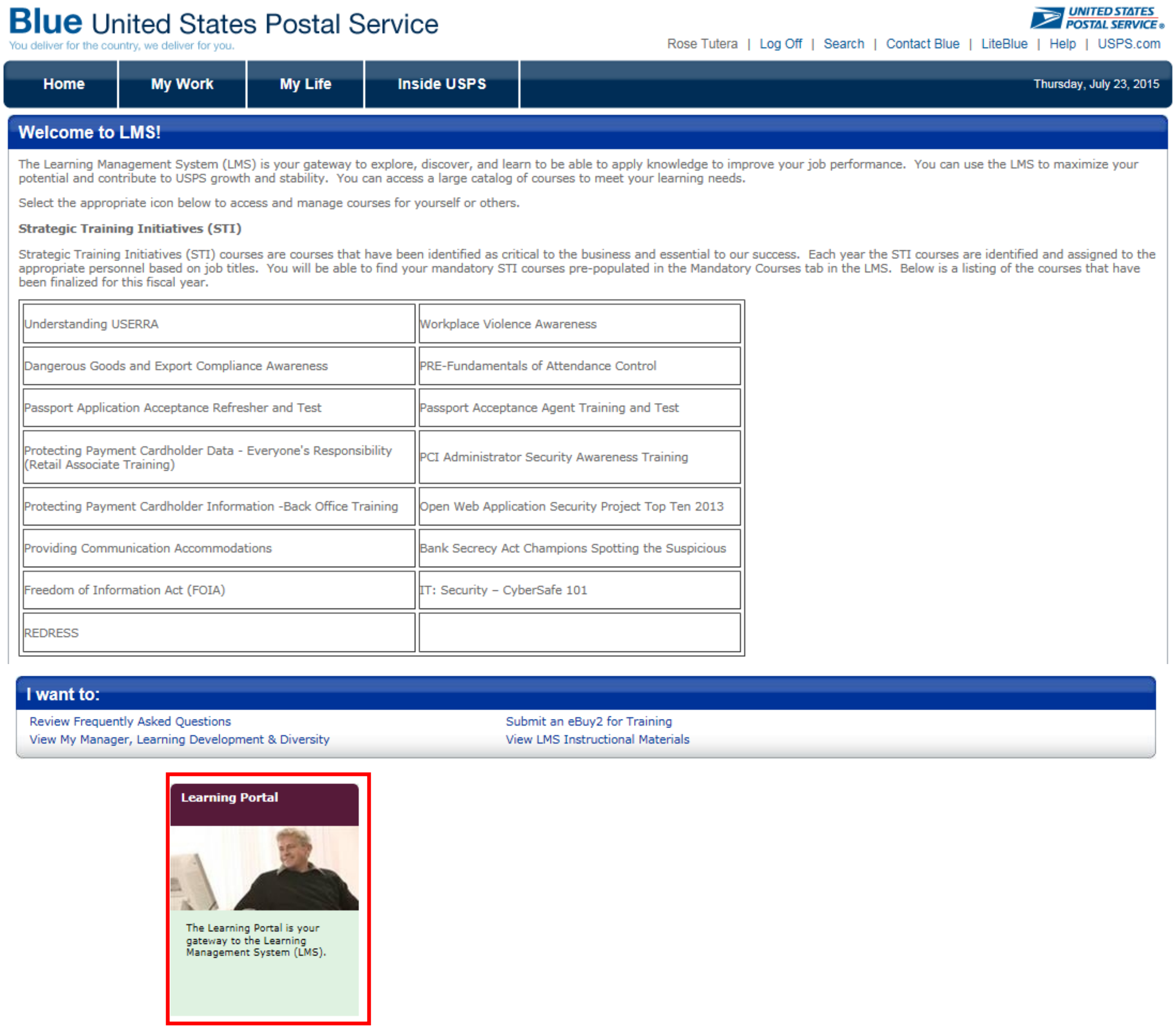
Your User ID and Password are the same as your ACE User ID and Password.

Log on to Blue to create and view your favorite links and customized Tool settings.

User ID:
Password:

Log in
Cancel
Forgot your ACE Password?

This will take you to the Learning Management System (LMS). Scroll down on the page to the Learning Portal icon. Click “Learning Portal.”



Blue United States Postal Service
You deliver for the country, we deliver for you.
UNITED STATES POSTAL SERVICE
Rose Tutera | Log Off | Search | Contact Blue | LiteBlue | Help | USPS.com
Home
My Work
My Life
Inside USPS
Thursday, July 23, 2015

Welcome to LMS!

The Learning Management System (LMS) is your gateway to explore, discover, and learn to be able to apply knowledge to improve your job performance. You can use the LMS to maximize your potential and contribute to USPS growth and stability. You can access a large catalog of courses to meet your learning needs.

Select the appropriate icon below to access and manage courses for yourself or others.

Strategic Training Initiatives (STI)

Strategic Training Initiatives (STI) courses are courses that have been identified as critical to the business and essential to our success. Each year the STI courses are identified and assigned to the appropriate personnel based on job titles. You will be able to find your mandatory STI courses pre-populated in the Mandatory Courses tab in the LMS. Below is a listing of the courses that have been finalized for this fiscal year.

Understanding USERRA	Workplace Violence Awareness
Dangerous Goods and Export Compliance Awareness	PRE-Fundamentals of Attendance Control
Passport Application Acceptance Refresher and Test	Passport Acceptance Agent Training and Test
Protecting Payment Cardholder Data - Everyone's Responsibility (Retail Associate Training)	PCI Administrator Security Awareness Training
Protecting Payment Cardholder Information -Back Office Training	Open Web Application Security Project Top Ten 2013
Providing Communication Accommodations	Bank Secrecy Act Champions Spotting the Suspicious
Freedom of Information Act (FOIA)	IT: Security – CyberSafe 101
REDRESS	

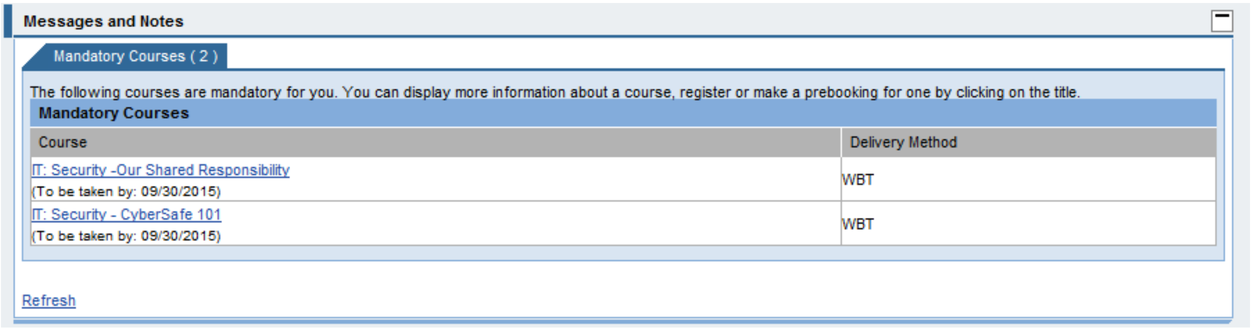
I want to:

Review Frequently Asked Questions
View My Manager, Learning Development & Diversity
Submit an eBuy2 for Training
View LMS Instructional Materials

The Learning Portal is your gateway to the Learning Management System (LMS).

The Learning Portal will display a list of courses to which you have been given access. The list should include the **IT: Security – Our Shared Responsibility** course and the **IT: Security – CyberSafe 101** course. Click on the hyperlink to display the course title page.

> *Note:* The Mandatory Courses tab lists all courses to which you have been given access. The Our Shared Responsibility and CyberSafe 101 courses are *recommended* for contractors to increase awareness about information security at USPS and are *not* mandatory.

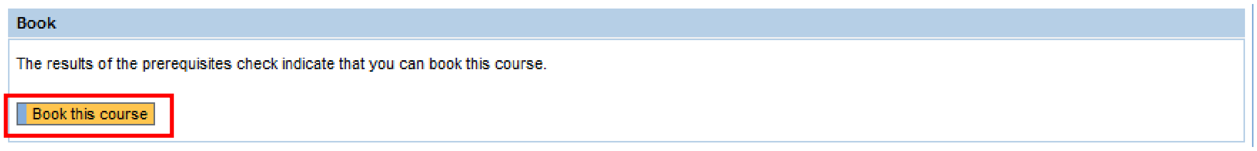


The following courses are mandatory for you. You can display more information about a course, register or make a prebooking for one by clicking on the title.

Mandatory Courses

Course	Delivery Method
IT: Security -Our Shared Responsibility (To be taken by: 09/30/2015)	WBT
IT: Security - CyberSafe 101 (To be taken by: 09/30/2015)	WBT

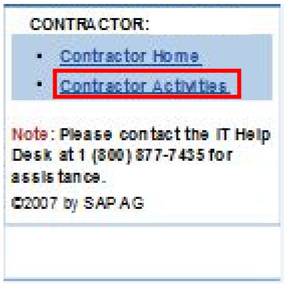
Scroll to the bottom of the description page to find the option to Book the course. Click the yellow “Book this course” button to add the WBT course to your listing.



Book

The results of the prerequisites check indicate that you can book this course.

The course will then appear in your Contractor Activities and will be available for you to take.



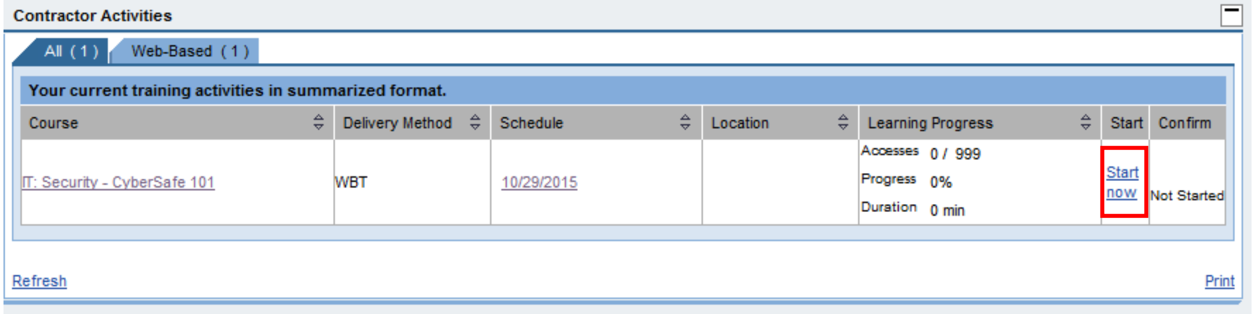
CONTRACTOR:

- Contractor Home
- Contractor Activities

Note: Please contact the IT Help Desk at 1 (800) 877-7435 for assistance.

©2007 by SAP AG

Click “Start now” to take the course.

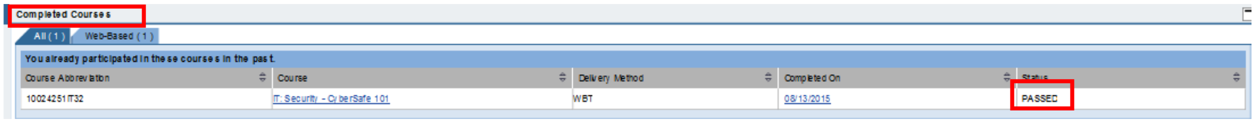


Contractor Activities

Your current training activities in summarized format.

Course	Delivery Method	Schedule	Location	Learning Progress	Start	Confirm
IT: Security - CyberSafe 101	WBT	10/29/2015		Accesses 0 / 999 Progress 0% Duration 0 min	Start now	Not Started

Upon completion of the course, you can click on the Contractor’s Activities link again and see that the page indicates you have successfully passed the course in the Completed courses tab.

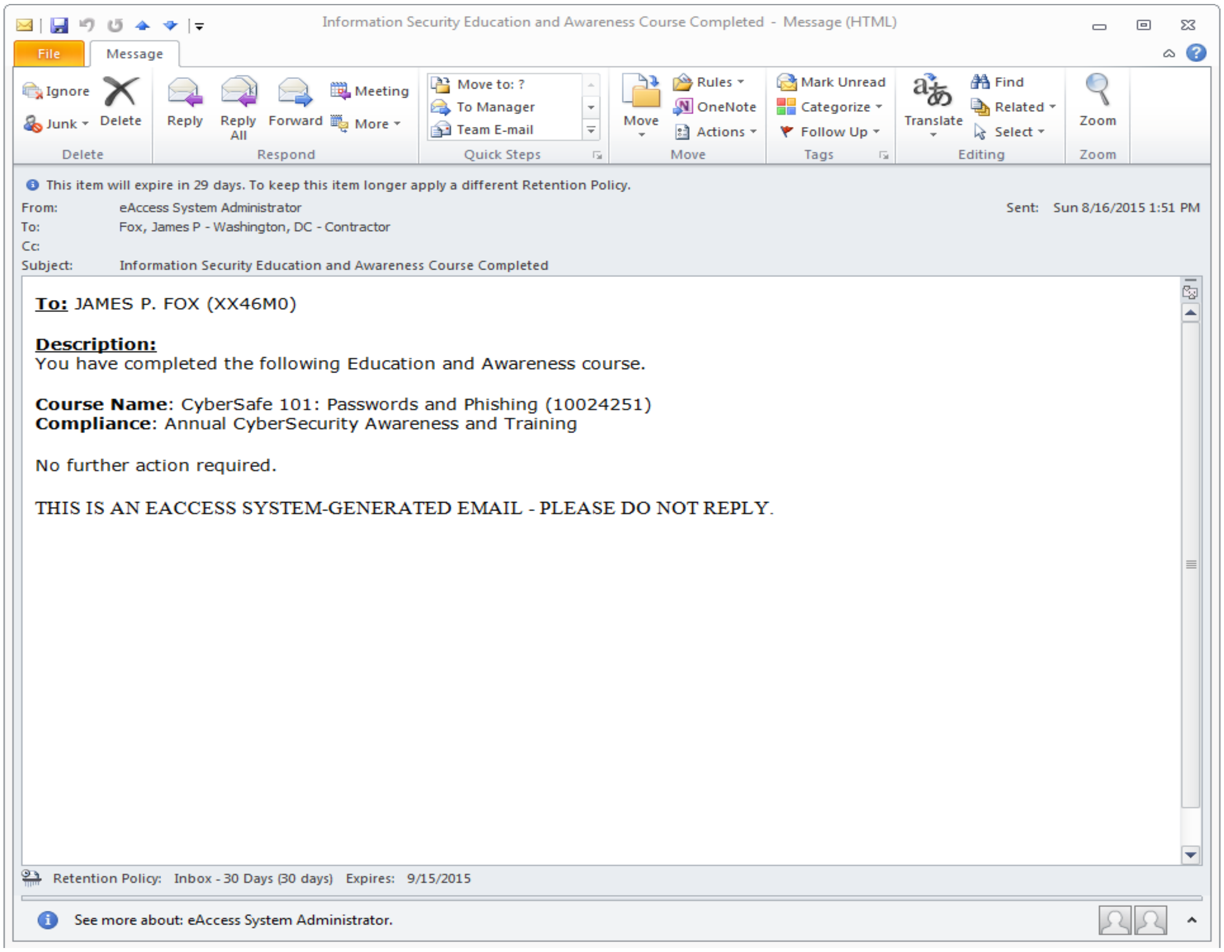


Completed Courses

You already participated in these courses in the past.

Course Abbreviation	Course	Delivery Method	Completed On	Status
10024251IT32	IT: Security - CyberSafe 101	WBT	08/13/2015	PASSED

You will also receive an email from the eAccess administrator notifying you that you have successfully completed the course within 2-3 days after LMS has refreshed course completion data within eAccess.



This item will expire in 29 days. To keep this item longer apply a different Retention Policy.

From: eAccess System Administrator
Sent: Sun 8/16/2015 1:51 PM
To: Fox, James P - Washington, DC - Contractor
Cc:
Subject: Information Security Education and Awareness Course Completed

To: JAMES P. FOX (XX46M0)

Description:
You have completed the following Education and Awareness course.

Course Name: CyberSafe 101: Passwords and Phishing (10024251)
Compliance: Annual CyberSecurity Awareness and Training

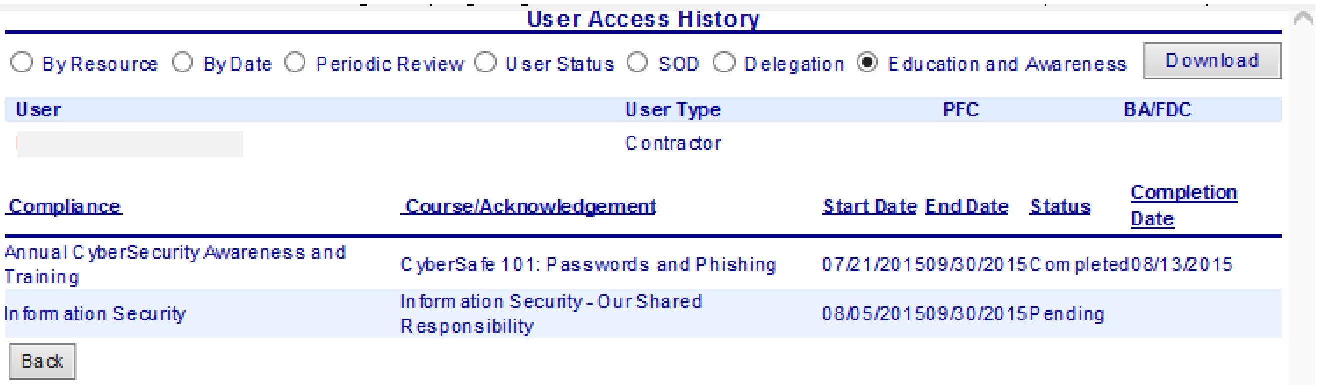
No further action required.

THIS IS AN EACCESS SYSTEM-GENERATED EMAIL - PLEASE DO NOT REPLY.

Retention Policy: Inbox - 30 Days (30 days) Expires: 9/15/2015

See more about: eAccess System Administrator.

You can also see the status update in eAccess under User Access History – Education and Awareness.



User Access History

○ By Resource ○ By Date ○ Periodic Review ○ User Status ○ SOD ○ Delegation ● Education and Awareness

User	User Type	PFC	BA/FDC
[redacted]	Contractor		

Compliance	Course/Acknowledgement	Start Date	End Date	Status	Completion Date
Annual CyberSecurity Awareness and Training	CyberSafe 101: Passwords and Phishing	07/21/2015	09/30/2015	Completed	08/13/2015
Information Security	Information Security - Our Shared Responsibility	08/05/2015	09/30/2015	Pending	

For questions related to the **IT: Security – Our Shared Responsibility** course and the **IT: Security – CyberSafe 101** course, please reach out to Gerri Wallace at gerri.wallace@usps.gov or Rose Tutera via email at rose.a.tutera@usps.gov.

For more information about the CyberSafe campaign at USPS, visit the CyberSafe website at http://blue.usps.gov/cyber. Remember to report all incidents and suspicious activity when on the USPS network or USPS ACE machine to cybersafe@usps.gov or via phone at 866-USPS-CIRT (866-877-7247).