Pennsylvania
Department of Public Welfare

Bureau of Information Systems

FTP Problem Reporting and Resolution Procedures

Version 2.0

February 26, 2016

Table of Contents

FTP Problem Reporting and Resolution Procedures

Introduction

This section lends support to the inbound and outbound files and the users that use the FTP process and renders procedures in the event that a file has not reached its intended destination.

Purpose

The purpose of this document is to give instructions in the event that files sent via the Managed File Transfer process did not reach its intended destination.

Files Sent from DHS – Business Partner did not receive

Any Business Partner that encounters problems with the Managed Data Transfer process. (**Files we send them**) must call their respective program area during normal business hours. SeGOV has no knowledge of the content of the file. SeGOV only transfers data. It does not manipulate data. After hours, for files labeled as critical (business process will halt if data is NOT received and processed) business partners should contact DHS Operations and Scheduling at 717-772-7155.

1. The caller will indicate that a critical file has not been received. Caller must supply the following information
   a. Business Partner Name
   b. Business Partner Contact name
   c. Business Partner Contact phone
   d. Business Partner Contact email address
   e. Environment (TEST or PROD)
   f. File name
   g. Approximate time file was to be sent

2. DHS Operations and Scheduling will contact key individual and relay nature of problem.

3. SeGOV personnel will research failure and provide response to DHS Operations and Scheduling. If more information is required key contact may contact business partner directly.

4. If file has not been received from Source application – key contact personnel will notify DHS Operations and Scheduling who will in turn notify the application that file has not been received in SeGOV-Staging directory.

5. If connectivity is broken –

   a. DHS Failure – Enter a Trouble Ticket with Vendor mark as PRODUCTION FAILURE -
   b. Business Partner Failure – provide appropriate error message – file will be resent once connectivity is re-established

6. If file in question is not critical, business partner must contact either WMAdmins (ra-wmadmins@pa.gov) or the program area. This account is monitored during normal business hours (07:30am – 04:00pm). SeGOV key personnel will research next business day.

7. Files in TEST environment are not considered critical and will be researched next business day.

Files Sent by Business Partner – not processed

Business Partner encounters problems with the managed file transfer process **from** the Business Partner (**files they send us**) to DHS. The technical analyst should contact WMAdmins (ra-wmadmins@pa.gov) or the program area. This account is monitored during normal business hours (07:30am – 04:00pm). SeGOV key personnel will research next business day.

1. If the Business Partner encounters issues connecting to SeGOV DMZ using SeGOV secure Browser.
   a. Has the user entered the correct URL
      i. TEST – https://missl-s.dhs.state.pa.us
      ii. PROD – https://missl.dhs.state.pa.us
   b. Can user reach the URL
      i. NO – have user verify IP address to the Internet – must be static and routable. Contact local ISP or IT department to verify.
      ii. YES – have user change password – passwords expired every 120 days.

2. If the Business Partner encounters issues connecting to SeGOV via SFTP:
   a. Review log for transmission – what is error message
   b. Has source IP address to Internet changed?
   c. Is SSH2 public key being sent? This key is associated with the Private Key on the business partner server. It will not change until a new server is brought on line.
   d. Has the password expired – ALL passwords must be changed every 120 days

3. If the Business Partner encounters issues connecting to SeGOV via FTPS
   a. Review log for transmission – what is error message
   b. Has Source IP address to the Internet changed?
   c. Has Business Partner digital certificate expired? Certificate must be trusted on DHS DMZ servers.
   d. Has the password expired – ALL passwords must be changed every 120 days

4. If file has been posted to the DMZ but has not moved in 24 hours, something is wrong. Please contact
   a. Program Office contact – review file naming convention
   b. Ra-wmadmins@pa.gov – please include the following in your communication
      i. Business Partner Name
      ii. Business Partner Contact name
      iii. Business Partner Contact phone
      iv. Business Partner Contact email address
      v. Environment (TEST or PROD)

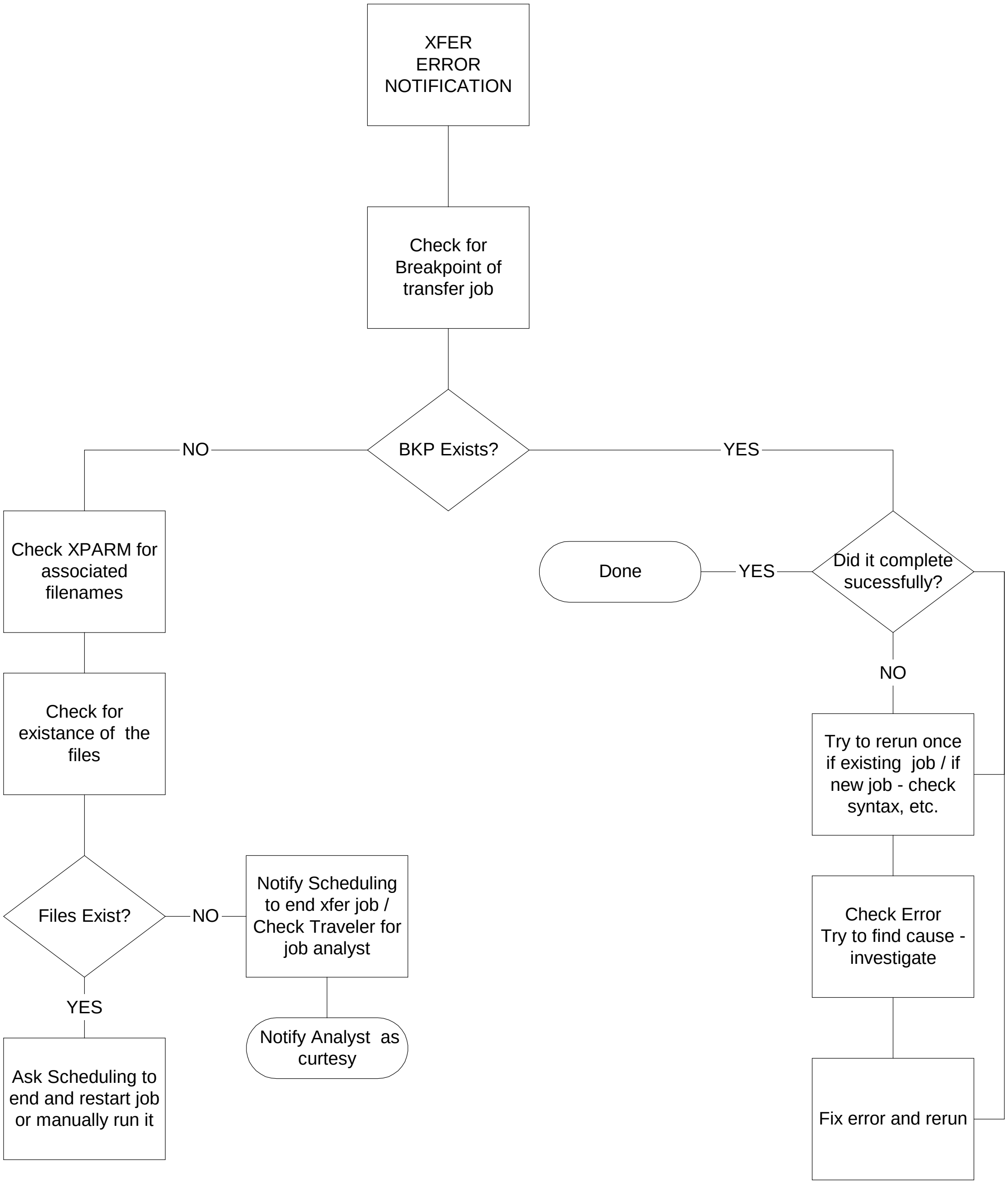
vi. File name
vii. Approximate time file was to be sent
viii. Directory where file is to be placed

Files Sent From Mainframe – Not Received

To troubleshoot data transfer failures from the mainframe, the business partner must contact the Program Office, or DHS Operations and Scheduling and provide information as described below. The application developer may need to be contacted to work with Middleware Services Unit.

1. Program Office contact
    a. Business Partner Name
    b. Business Partner Contact name
    c. Business Partner Contact phone
    d. Business Partner Contact email address
    e. Environment (TEST or PROD)
    f. File name expected (Server Side)
    g. Date/Time file was expected
2. DHS Middleware Services Unit provide
    a. Business Partner Name
    b. Business Partner Contact name
    c. Business Partner Contact phone
    d. Business Partner Contact email address
    e. Mainframe HOST were job was to run
    f. Mainframe Environment (IMD, PLT, SAT etc.)
    g. Mainframe File name
    h. Mainframe Job that was to run
    i. Mainframe Transfer Job that was to run
        a. Access the proper HOST MF Demand mode
        b. Access BUOPS*BOPWK4.XPARM
        c. Find Filename – Transfer job name will be on the extreme left
    j. Approximate time file was to be sent
    k. Directory where file is to be placed
3. Please provide breakpoint if available

TROUBLESHOOTING DECISION TREE for Transfers FROM Mainframe


XFER ERROR NOTIFICATION
Check for Breakpoint of transfer job
BKP Exists?
NO
YES
Check XPARM for associated filenames
Check for existance of the files
Files Exist?
NO
Notify Scheduling to end xfer job / Check Traveler for job analyst
Notify Analyst as curtesy
YES
Ask Scheduling to end and restart job or manually run it
Done
YES
Did it complete sucessfully?
NO
Try to rerun once if existing job / if new job - check syntax, etc.
Check Error Try to find cause - investigate
Fix error and rerun

Files Sent To Mainframe – Not Processed

Managed File Transfer software is used to send files to the mainframe. Questions concerning execution of jobs and schedules on the mainframe should be directed to DHS Operations and Scheduling and Middleware Services Unit. The application developer will need to be involved.

1. Business Partner Contact name
2. Business Partner Contact phone
3. Business Partner Contact email address
4. Environment (TEST or PROD)
5. File name (Server Side)
6. Business Partner Name
7. Date/Time file was expected
8. Task must be set up in Managed File Transfer software
9. Trigger, if used, must be sent to staging directory where DHS OPCONS (batch scheduling software) can pick up
10. Based on existence of trigger in OCT staging directory on the DHS FTP server, OPCONS will add file to the appropriate schedule
11. Job-to-run on the mainframe must be set up with scheduling.
12. File on the mainframe may be assigned to fixed or temporary storage. If the application developer has not taken steps to keep the file (by placing in on a mainframe removable disk pack), it may be deleted after midnight.
13. Is the file large – if yes, were enough tracks available on the HOST to process the file?

Change Password

Commonwealth Policy states that ALL passwords must expire. These passwords must be changed every 120 days. DHS security has provided the ability for users to create hint questions and change the password without assistance from the Help Desk.

SeGOV staff does not have the ability to change passwords. Please take the time to create HINT questions.

Passwords for the SeGOV system expire every 120 days.
Have you created your HINT questions?

Yes –
Please go to login screen for Keystone Key

https://www.humanservices.state.pa.us/selfservice.html

Click on **Forgot Password**
Enter UserID

Answer 2 HINT Questions
Change Password as per on-screen instructions
Upon receipt of success message close current window
Close all Internet sessions
Open login screen and login
PROD - https://missl.dhs.state.pa.us or
TEST -- https://missl-s.dhs.state.pa.us
Password has been changed and is good for 120 Days

Note – If you receive message “Not enough information to complete HINT questions” – then your HINT questions are not complete. Follow instructions below

No –
Complete HINT questions – we expect all users to complete HINT questions and be able to change their password without assistance.

If your password has expired and you DID NOT create HINT questions, please contact OIS Account Administration at 1-800-281-5340 and request managed password reset – you will need to provide your b-UserID

Please go to login screen for Keystone Key

https://www.humanservices.state.pa.us/selfservice.html

Enter Username and Password on Keystone Key
Click Login
Accept 205.34 Agreement (this is MANDATORY)
Click Next
Confirm information is correct
Follow onscreen instructions
Change password
Confirm password
Enter email (as registered)
Confirm email (as registered)
Answer three (3) HINT questions
Enter phone number (10 digits, no dashes)
Click submit
Upon receipt of success message close current window
Close all Internet sessions
Open login screen and login
PROD - https://missl.dhs.state.pa.us or
TEST -- https://missl-s.dhs.state.pa.us

Security Agreement, HINT questions and Password have been changed. Password is good for 120 Days.

Good news – Once HINT questions have been created, users are able to change their password even if it has expired. ***PLEASE NOTE – if user contacts OIS Account Admin and requests password reset, existing HINT Questions will be cleared and HINT Questions will need to be re-established.***

Key Contacts –

Each Program Office should maintain a list of key contacts. Please refer to Program Office communications to define list of contacts.

DHS Operations and Scheduling maintain a list of key contacts in the event a critical file has not been received or processed. SeGOV team will research and advise if file has been received or sent. In the event the file has not been received, DHS Operations and Scheduling will move to that area on the contact list.

The Program Office will define a list of critical files (operations and business will come to a halt if not received and processed).

TEST files are not considered critical.

Maintenance Windows

DHS application releases and updates may affect success and timing of data transfer. The Program Office is responsible for communicating these outages to users and business partners.

In addition there are several standing maintenance windows. They include:

- Tuesday – 09:00PM – Wednesday 01:00AM
- Thursday – 09:00PM – Friday 01:00AM
- Sunday – 06:00PM – Monday 06:00AM

While these outages are generally intermittent in nature, they are predicated by the work that needs to be accomplished. Files may need to be resent (inbound or outbound) as needed.

While these are standing maintenance windows, the Office of Administration (OA) may need to schedule emergency maintenance outside of this window. This will be communicated to DHS Operations and Scheduling area as well as to the Program Offices.

Document Change Log

Change Date	Version	Change Description	Author and Organization
01/24/03	1.0	Initial creation.	Charles H. Strange OIS/Enterprise Administration Section
05/11/04	1.0	Reviewed for content – No change necessary	Charles H. Strange
02/18/2005	1.0	Reviewed content – No change necessary	Dave Shevenock
10/7/2013	2.0	Revised Content	DTE – B Wadlinger
02/26/16	2.0	Revised Content	DTE – B Wadlinger