Helping our members work together to keep the lights on... today and in the future
EFT Server

April 21, 2011

Kevin B. Perry
Director, Critical Infrastructure Protection
kperry@spp.org · 501.614.3251
Agenda

- Overview of Data Confidentiality
- Overview of the EFT Server
- Demonstration

This webinar is being recorded
The presentation slides will be posted to the SPP RE page on the SPP website.
Data Confidentiality

- Certain information collected during an audit or enforcement activity is highly sensitive and must be protected from inadvertent disclosure.

- Examples include:
  - Critical Energy Infrastructure Information (CEII)
  - CIP-protected information
  - Self-report/self certification supporting evidence
  - Mitigation plans and supporting evidence
  - Personnel or personally identifying information
Identification of Confidential Information

• The submitting entity shall mark as confidential any information that it submits to NERC or a regional entity that it reasonably believes contains confidential information as defined by the NERC Rules of Procedure.
  
  – Indicate the category or categories defined in Section 1501 of the NERC Rules of Procedure
  
  – If the information is subject to a prohibition on public disclosure, indicate as such and provide supporting references and details.
Protection of Confidential Information

• NERC Rules of Procedure, Section 1502. Protection of Confidential Information

2. Confidentiality — Except as provided herein, a receiving entity shall keep in confidence and not copy, disclose, or distribute any confidential information or any part thereof without the permission of the submitting entity, except as otherwise legally required.
Submitting Sensitive Information

• Confidential, sensitive information, such as CIP-protected information should only be submitted via the SPP EFT Server
  – Secure HTTP/S connection.
  – Automatically PGP-encrypted (AES-256) upon upload to the EFT Server.
  – Access to encrypted information files limited to SPP RE staff.
  – Submitter does not have to have PGP installed.
EFT SERVER OVERVIEW
Advantages of the EFT Server

- Uploaded files are immediately PGP-encrypted upon receipt
- No information protection steps required of the sender
- No cost to the registered entity
- Maximum efficiency
System Requirements

• Supported Browser
  – Internet Explorer 7
  – Internet Explorer 8
  – Current Mozilla Firefox

• Configure browser to support TLS 1.0

• Java Runtime Environment
  – Requires JRE6
TLS 1.0 Required
JRE6 Required
User Account Required

- Access to the EFT Server is via a username and password.
  - Individual user accounts required
  - PCC or AO requests the user account via an e-mail message to Kevin Perry (kperry@spp.org) or Leesa Oakes (loakes@spp.org)
  - Provide name, e-mail address, and phone number of each user
- Username and password will be e-mailed from the EFT Server (eftadmin@spp.org)
Password Complexity Rules

• The password must meet certain complexity rules:
  – The password must be at least eight characters in length
  – The password must contain a combination of at least four characters of the following:
    ▪ Lower case alphabetic (a – z)
    ▪ Upper case alphabetic (A – Z)
    ▪ Numeric digits (0 – 9)
  – Cannot use 3+ character sequence from user name
  – Cannot use any of the previous ten passwords
  – Must be changed at least every 90 days
To connect to the SPP EFT Server, launch your browser and navigate to: https://eft.spp.org/. 
You are now logged out.
Directory listings and other screens may be retained by your browser’s history. We recommend you delete temporary files if extremely sensitive data is involved.

Password security reminder:
Please treat your password as confidential. As a security reminder, we recommend that you periodically change your password (if this policy is enabled by the server administrator).

Security notice:
When logging on to this server, we will never ask for any personal information other than your account login name and password.

If you are ever prompted for additional personal information upon attempting to log in, please contact the server administrator.
EFT SERVER DEMONSTRATION
Questions?
Q&A FROM WEBINAR PARTICIPANTS

Q: The file size on the submitter’s PC (shown in the upper-left pane) is larger than the same file’s size on the EFT Server (shown in the upper-right pane). Is this something we need to be concerned about?

A: The file size will change and most often is smaller when the file is encrypted. Encrypting the file also compresses the file somewhat in most instances. As long as the file name includes the “.pgp” extension on the EFT Server side and the progress status in the lower pane shows COMPLETED, the file transferred properly.

Q: Will PGP encryption or the use of the EFT server affect the hash verification?

A: No. The SHA-2(256) hash is basically an electronic signature on the file created by applying a mathematical formula to the content of the file. The hash is created before the file is uploaded to the EFT server. The hash is verified after the PGP-encrypted file has been retrieved by the SPP RE staff and decrypted. Decrypting the file returns it to the same state as it was prior to uploading it to the EFT Server and the hash value will be the same.

Q: Can we submit test files to make sure we are comfortable with the system before we have to use it for real?

A: Yes. We ask you do one of two things. Either let us know you will be submitting test files so that we know to ignore them, or better yet, name the files and folders as “test”, “Dummy”, or something similar so that we clearly recognize them as test files we can ignore. Also, we suggest you delete the files using the EFT Server function button (folder with a X in it) in the upper-right pane when you finish your testing.

Q: Can we use one account to upload information for multiple entities that we manage?

A: No. Each entity has its own defined folder and the user account can only map to a single folder. The user account cannot change between entity folders as users for one entity cannot see the contents of another entity’s folder.