# COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT’S OF HUMAN SERVICES, INSURANCE, AND AGING

## INFORMATION TECHNOLOGY STANDARD

<table>
<thead>
<tr>
<th>Name Of Standard:</th>
<th>Number:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Exchange Standards Ver 3.5</td>
<td>STD-EASS004</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Domain:</th>
<th>Category:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration and Middleware</td>
<td>Data Exchange</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date Issued:</th>
<th>Issued By Direction Of:</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/01/01</td>
<td>Robert Doren, Acting Dir of Division of Technical Engineering</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date Revised:</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/01/17</td>
</tr>
</tbody>
</table>
# Table of Contents

COMMONWEALTH OF PENNSYLVANIA ................................................................................. 1
DEPARTMENT’S OF HUMAN SERVICES, INSURANCE, AND AGING.............................. 1
INFORMATION TECHNOLOGY STANDARD........................................................................ 1

Introduction ................................................................................................................. 4
Purpose ......................................................................................................................... 4

Supported Data Exchanges......................................................................................... 5
- SFTP – preferred method - automated ................................................................. 6
- SeGOV Web Browser Exchange – Preferred Method - manual ....................... 6
- COPY – preferred method for internal transfers and batch .......................... 6
- FTP ....................................................................................................................... 6
- FTPS ................................................................................................................. 7

Process Description .................................................................................................... 8
Identification of business requirements ....................................................................... 8
TFS – User Story for SeGOV Data Transfer ............................................................. 8

Security Registration ............................................................................................... 9
- Confidentiality Agreements, Data Agreements and Contracts ....................... 9
- Building the exchange ......................................................................................... 9
- User ID/Passwords .............................................................................................. 9

Testing and Operational implementation .............................................................. 9
- Connectivity Testing .......................................................................................... 10
- Exchange initiation ............................................................................................ 10
- Monitoring and logging ..................................................................................... 10

Data Exchange Files ............................................................................................... 10

Data Exchange Requirements .................................................................................. 11
Technical Requirements .......................................................................................... 11
- SFTP – preferred method - automated ................................................................. 11
- FTPS .................................................................................................................. 11
- SeGOV Web Browser – preferred Methods - manual ....................................... 12
- FTP ............................................................................................................... 13

Firewall Requirements ............................................................................................ 14

File (Payload) Requirements ................................................................................... 14
- File (MIME) Types ............................................................................................ 14
- File Compression ................................................................................................. 14
- File Size .............................................................................................................. 14
- File Naming Conventions .................................................................................. 14
- Trigger files ....................................................................................................... 15
- PGP encryption ................................................................................................. 15

Server Requirements ............................................................................................. 15
- Business Partner's Data Exchange Servers ..................................................... 15
- Business Partner Data Exchange Server Availability .................................. 15
- Business Partner Secure Transfer - Client ...................................................... 15

Network Requirements ........................................................................................... 16
- Transmission Time ............................................................................................. 16
- Batch Cycle Times ............................................................................................ 16
- Transmission Speed ......................................................................................... 16
SeGOVernment Data Exchange Standards

Introduction

This document identifies the policies, operational processes, and considerations for the electronic exchange of information between the Department of Human Services (DHS), Department of Insurance, Department of Aging and its external Business Partners, and internal applications. The SeGOVernment Exchange System (SeGOV) supports parameterized less costly and time-consuming creation of new exchanges/tasks. It also separates the responsibility and method of exchange from specific applications. The application is no longer responsible for delivering files to the Business Partner. The application is responsible for delivering the file to the SeGOV designated staging directory. The SeGOV process provides a secure method of transferring data beyond the capabilities of secure-email. Secure-email provides the method to send confidential information between two individuals. Secure e-mail does not provide the mechanism to send data between applications and individuals, systems, or applications. SeGOV fills this requirement.

Any business partner can now use one or many methods of exchange for multiple applications and a given application can use all modes of delivery depending on the circumstances of the business partner. Business partners can now access multiple folders on SeGOV. The Internet is the preferred method to deliver sensitive data securely thus avoiding the high cost of dedicated point-to-point networks.

This document primarily defines the operational use of the SeGOVernment Data Exchange system. The creation of new exchanges/tasks are considered operational configurations and do not require time consuming and costly systems software generations.

The development, implementation, and administration of these Data Exchange standards are the responsibility of the Technical and Architecture Development Unit (TADU) within the Bureau of Information Systems (BIS).

Purpose

The purpose of this document is to provide a standard set of policies and procedures to control the exchange of information between the Department’s network, the private networks of DHS Business Partners, and the Internet. The effective exchange of data requires:

- Timely, accurate, efficient transfer of data files between the Department and Business Partners
- Adherence to Best Practices and Federal (HIPAA and IRS) security requirements for transfer of sensitive data
- Structured non-proprietary protocols and tools for problem resolution
- Efficient utilization of resources to transfer data between the Bureau of Information Systems (BIS) and various stakeholders/Business Partners
- Documented procedures and interfaces
- Performance metrics and standards
- Effective audit trails for mission-sensitive data

Use of SeGOVernment meets requirements set forth in OA Information Technology Bulletin (ITP SEC031- Encryption Standards for Data in Transit). This document can be accessed at

http://www.oa.pa.gov/Policies/Documents/itp_sft005.pdf

The concern is the protection of critical and sensitive electronic data and the secure delivery thereof, Standards for Privacy of Individually Identifiable Health Information (PII) and Health Insurance Portability and Accountability Act (HIPAA) data. Because of the nature of the Department’s business, all data is considered sensitive and transfers are required to be encrypted.

**Supported Data Exchanges**

DHS has acquired the enterprise version of the MOVEit Suite manufactured by IPSwitch. This includes MOVEit DMZ and MOVEit Central. BIS requires that Business Partners use a client that is compatible with the MOVEit Suite. A current list of these clients can be found at


Business Partners are required to review selected client with DHS prior to proceeding with selection and implementation.

Additional information regarding the MOVEit Suite can be found at

http://www.ipswitchft.com/moveit-managed-file-transfer

Data Exchanges/tasks use current industry standard technology to securely transfer data over both trusted (private) and untrusted networks (the Internet). The preferred protocol for SeGOVernment Exchanges is Secure File Transfer Protocol (SFTP) or the SeGOV web browser. SFTP is designed to transfer the files over the Internet using encrypted sessions. This is done over port 22 with the exchange of SSH keys and authentication of UserID and password. Data at rest in the DHS DMZ is encrypted. FTP is supported only for Internal Transfers with approval from DTE Technical and Architecture Development unit.

All connections must be registered in the Office of Administration (OA) firewall. Only designated ports are permitted. All passwords must be renewed as required by Security Standards.
SFTP – preferred method - automated
This data exchange is for high volume data transfers to and from Business Partners (with specialized servers) using an approved SFTP client that is compatible with DHS software. These data transfers will occur over the Internet via port 22 with exchange of RSA/SSH2 client/public key and authentication of DHS Supplied UserID and Password provided by DHS Unified Security (USEC). Each server must be registered in Unified Security. Each entity must be registered in the Office of Administration (OA) firewall. Please allow two weeks for this process.

This is an automated process. Sessions are encrypted. File delivery can be either event driven or scheduled. Not all data transfers lend themselves to event driven transfer. Email notices can be sent to team members if required. We request that teams create an exchange distribution list for this purpose.

SeGOV Web Browser Exchange – Preferred Method - manual
This data exchange is for low volume data transfers to and from Business Partners (without specialized servers) using a web browser interface. The transport protocol is HTTPS over port 443 with client authentication via BIS Unified Security System (USEC) issued userIDs and passwords. Generic userIDs are not supported in this system. Each user must be registered in Unified Security. Each entity must be registered in the Office of Administration (OA) firewall. As personnel transitions to or from the entity, the new user MUST be registered and the former user must be suspended. Please allow two weeks for this process.

Web Browser users have the ability to upload or download files from their unique folder on the SeGOVernment webpage. An email will be sent to the Business Partner announcing the availability of the file. The Business Partner will click on the URL provided and will be connected to the SeGOV webpage. Files are routed based on filename and are archived for a maximum of 60 days (if uniquely named). If not downloaded within 7 days, the user will receive a notice that the file has NOT been downloaded. Users are expected to maintain their site and Download and Delete files as they are received. Files are automatically purged from the site if not deleted after 30 days. SeGOVernment IS NOT a storage facility for user data. Failure to delete files may result in shortening the window of availability.

COPY – preferred method for internal transfers and batch
Transfers to the SeGOVernment Staging directories from internal applications and servers should be sent via COPY. This method IS NOT supported for any transfers outside the DHS firewalls.

FTP
FTP is only supported between DHS and internal applications. Use of dedicated data circuits over Port 20/21 are no longer valid methods for data transfers. Transfers sent from UNISYS mainframe must use FTP. Please contact Middleware Services Unit (MSU) to arrange for transfer to SeGOVernment staging area.
FTPS
FTP over SSL (FTPS) is an extension to the commonly FTP that adds support for the Transport Layer Security (TLS) and the Secure Sockets Layer (SSL) cryptographic protocols. Sessions are encrypted. Use of this method requires exchange of Digital Certificates and exchange of UserID and Password. The Commonwealth only supports port 990 implicit traffic. Use of this method also requires use of high ports (3000-3007).
Data Transfers between Business Partners and BIS

Process Description

New or revised data exchanges/tasks are created as a routine process of doing business. The current versions of the SeGOVERNment data transfer processes only address file transport process.

- The following is a brief outline of the process for identifying, configuring and implementing new exchanges. Once a business requirement and TFS task is communicated to a Program Office Coordinator, BIS personnel will actively assist the Program Office Business Coordinator and the Business Partners in navigating through this process and completion of the data exchange requests. Submission of the following items will initiate the process.
  - SeGov Data Transfer Worksheet
  - TFS – User Story for SeGOV data transfer

Identification of business requirements

DHS’s Bureau of Information Systems (BIS) will coordinate and oversee the configuration of all new exchanges/tasks for DHS, Department of Insurance, and the Department of Aging. The Program Offices will identify a Coordinator to interface with BIS in the definition of new exchanges.

Business Partners requiring new data exchanges should work with their Program Office contacts and BIS in the development of new data transfers. Business Partners are not expected to navigate the registration process unassisted. They will work together with the Program Office Coordinator and BIS.

The Program Office Coordinator is responsible for ensuring that all necessary contracts and data agreements are in place between DHS and the Business Partner prior to initiating any exchange of data. The Coordinator is also responsible to notify BIS that the contract/data agreement has expired and that data exchanges are to be terminated.

The Coordinator will also work with application developers in the definition of new exchanges/tasks. The Coordinator is responsible for providing the TFS number and project account code assigned to create the exchange.

Once a new requirement is identified, DTE will oversee its implementation using the resources of the Bureau of Information Technology (BIS). The SeGOVERNment team supports the Enterprise. It is requested that coordinators allow a minimum of two weeks to process requests.

TFS – User Story for SeGOV Data Transfer

Program Office Coordinator will create a User Story in TFS. Listed below are steps necessary to complete a task.
Title – all stories must have a Title – it would be helpful if the Title started with “SeGOV Data Transfer to …….”
Assign the task to either Robert Ziegler or Barbara Wadlinger.
Complete Details within the story
- Due Dates for each environment (minimum two week lead time requested)
- Description of work to be done
- Include analyst name if working with someone specific
- Open Attachments - attach completed SeGOV Data Transfer worksheet – incomplete worksheet will increase the amount of time it takes to complete the task.

Security Registration
All SeGOVernment security authorizations are made using the established security procedures of DHS’s Business and Technical Standards. These standards can be located at:

http://www.dhs.pa.gov/provider/busandtechstandards/index.htm

This includes use of standard ports as defined by OA, use of digital certificates or exchange of public keys, and validation of user access through LDAP interface to security servers.

Confidentiality Agreements, Data Agreements and Contracts
It is the Program Office’s responsibility to ensure that all data agreements and contracts with Business Partners are in place prior to initiation of the data exchange. Users will be asked to accept this agreement electronically during online configuration of user HINT questions. It is expected that if the contract or data agreement expire that the Program Office will notify BIS so appropriate action may be taken to terminate any active data exchanges.

Building the exchange
New exchanges are configured by BIS based upon the requirements of the exchange as defined in TFS and the SeGOVernment Registration Form. Program Office Coordinator will work with the Business Partner, application support teams and BIS to define the requirements and establish an implementation timeframe. Completion timeframes will depend on the complexity of the exchange but it is requested that a minimum of two weeks be provided to configure the tasks.

User ID/Passwords
All SeGOV passwords are issued by BIS Unified Security Team. Passwords follow established security standards regarding creation and changing of passwords (Attachment #1, Attachment #2). At this time ALL passwords must be changed as defined in DHS Security Standards.

Testing and Operational implementation
BIS will provide the Program Office Coordinator and the Business Partner with the relevant documentation for the use of each exchange. BIS and the Program Office Coordinator will continue to coordinate activities with the Business Partner until the exchange is implemented.
Connectivity Testing
As SeGOVernment data exchanges/tasks are added or modified, BIS will develop a connectivity test plan to ensure that no barriers exist prior to moving the new exchange through each environment (Attachment #3).

The steps in testing connectivity include:

- BIS configures host connection
- BIS configures a new task
- OA opens firewall as necessary
- The Business Partner configures their systems and firewalls
- Login credentials are exchanged via secure email
- A mutually agreed upon number of connectivity tests are performed between DHS and the Business Partner
- BIS and the Business Partner monitor the success of SeGOVernment data exchanges for an agreed upon number of cycles
- The data exchange is moved into production

Exchange initiation
The exchange is considered to be in production after the new data exchange has successfully passed the required connectivity tests and the exchange has been “accepted” by BIS, the Business Partner and Program Office as operational.

Monitoring and logging
The SeGOVernment System will record the occurrences of all data exchanges including the submission and receipt of data, file name the success and failure status, and time of transmission. Logs are available for diagnostic and business purposes. If requested the business partner will be notified by email of the success of each exchange transmission.

Data Exchange Files
An application interface is the point at which an application retrieves or submits data to a Business Partner. The application developer must stage the files to be transferred in the designated SeGOVernment staging directory. This can be done programmatically or manually. Based on requirements, the data exchange/task flow service will move the files from the staging directory and deliver files to the Business Partner. Once Browser files are moved to the SeGOVernment DMZ, an email is sent programmatically, advising the business partner that files are ready for download.

SeGOVernment transfers data. It does not manipulate data. Any questions concerning file content should be directed to the Program Office Coordinator.

Files are staged to the SeGOVernment staging directory when they are ready for release to the Business Partner. Staged files are archived for a maximum period of 60 days from the time the exchange is executed. If the files are not uniquely named, they are overwritten in the archive with each execution of the exchange/task. The SeGOVernment exchange is not designed to store files. These files are automatically purged after maximum retention period is reached (not to exceed 60 days).
Files on the SeGOVernment Browser are purged after 30 days. Any requests for re-send must be directed to the Program Office Coordinator.

**DataExchange Requirements**

The effective use of these Data Exchange Standards require adherence to the following requirements. Data exchanges consume network resources. To allow for maximum network throughput for daily DHS operations, it is expected that data files will be exchanged during non-peak hours (6:00PM – 6:00AM Monday-Friday and anytime Saturday or Sunday). If files are transferred during peak hours, network latency may be experienced. If such a condition occurs the business partner will be asked to transfer files during non-peak hours. If large files cause network latency, sender will be asked to zip or break files into smaller more manageable files.

**Technical Requirements**

The Business Partner must support the following configurations to use the indicated exchange. Except for the SeGOV web browser, it is expected that DHS will PUT files on the Business Partner Server and the Business Partner or application will PUT files in the designated directory path on the DHS server. Exception to this method requires DTE approval. DHS policy does not allow FTP GETs to the UNISYS mainframe. The UNISYS mainframe will FTP files to the designated staging directory for delivery to other applications or business partner.

**SFTP – preferred method - automated**

1. FTP Server – An industry standard ftp server (manufactured within the last 3 years) is required. Examples include Microsoft Server 2003 or later version, Apache, etc.
2. Use of Internet to transfer data
3. Use of approved compatible SFTP client
4. Exchange of RSA SSH2 client keys (public key)
5. Authentication use UserID/Password
6. Sessions are encrypted.
7. Most data transfers are event driven. File is delivered upon receipt. It is recommended that these transfers occur during non-peak processing hours (6:00pm–6:00am). Peak hour transfers may result in network latency. Should a specific set of transfers become problematic, user will be asked to
   - Troubleshoot connectivity
   - Change scheduled exchange time to non-peak hours
   - Compress file
   - Break file into manageable pieces (multiple exchanges)
   - Receive the file via physical media (requires exception approval).
8. Standard SFTP port (22) for data transmission.
9. All files must have a MIME (Multipurpose Internet Mail Extension) type: doc, txt, xls, mdb, zip, etc.
10. If using file compression, file must be in standard .zip format.
11. The Business Partner firewall may require changes to allow successful transfer or data. Refer to the firewall section of this document.
12. The Business Partner must supply an IP Address, Client Key, User Name and Login for SeGOV access to the Business Partner web server. Business Partner will define path for successful delivery of files.

13. Business Partner Server Permissions – MODIFY

14. Firewall requirements
   - Allow port 22 (SFTP) for encrypted data exchanges
   - Supply SeGOV with the IP address used for such file transfers
   - The Business Partner technical team must be available to troubleshoot connectivity problems

**FTPS**

1. FTP Server – An industry standard FTP server (manufactured within the last 3 years is required. Examples include Microsoft Server 2003 or later version, Apache, etc.
2. Use of Internet to transfer data
3. Use of approved compatible FTPS client
4. Exchange or Digital Server Certificate – An industry standard digital server certificate that supports 128-bit encryption is required. Examples include VeriSign, Entrust, Baltimore, etc.
5. Sessions are encrypted.
6. Most data transfers are event driven. File is delivered upon receipt. It is preferred that these transmissions occur during non-peak processing hours (6:00pm–6:00am). Peak hour transfers may result in network latency. Should a specific set of transfers become problematic, user will be asked to
   - Troubleshoot connectivity
   - Change scheduled exchange time to non-peak hours
   - Compress file
   - Break file into manageable pieces (multiple exchanges)
   - Receive the file via physical media (requires exception approval).
7. Standard FTPS port 990, implicit mode. Use of defined high ports (3000-3007)
8. Exchange of login credentials
9. All files must have a MIME (Multipurpose Internet Mail Extension) type: doc, txt, xls, mdb, zip, etc.
10. If using file compression, file must be in standard .zip format.
11. The Business Partner firewall may require changes to allow successful transfer or data. Refer to the firewall section of this document.
12. The Business Partner must supply an IP Address, Digital Certificate, User Name and Login for DHS access to the Business Partner server.
13. Firewall requirements
   - Allow port 990 (FTPS implicit) for encrypted data exchanges
   - Allow High Ports (3000-3007)
   - Supply BIS with the IP address used for such file transfers.
   - The Business Partner technical team must be available to troubleshoot connectivity problems

Note: The Commonwealth does not support FTPS explicit over port 21.
**SeGOV Web Browser – preferred Methods - manual**

1. Windows based PC.
2. Microsoft Internet Explorer 6.0 or greater (128 bit encryption).
3. It is recommended that the Business Partner have a high speed internet connection (DSL, Cable, Broadband)
4. Access to email
5. Registration of user ID within BIS Unified Security system. A Business Partner UserID and Login is required for access to DHS web server.
6. All outbound actions are initiated by DHS. An email is sent to the Business Partner advising that a file is available for download.
7. The Business partner initiates all inbound actions. An email notice can be sent when the file is moved to its predetermined destination. It is preferred that these transmissions occur during non-peak processing hours (6:00pm –6:00am). Peak hour transfers may result in network latency. Should a specific set of transfers become problematic, user will be asked to retransmit during recommended processing hours.
8. All traffic must use port 443 (standard SSL port).
9. All files must have a MIME (Multipurpose Internet Mail Extension) type: doc, txt, xls, mdb, zip, etc.
10. If using file compression, file must be in standard .zip format
11. Transmission times are governed by the size Business Partner’s pipe to the Internet, and associated Business Partner policies. If files reach a size where they time-out in upload, the Business Partner may be asked to:
   - Change scheduled exchange time to non-peak hours
   - Upgrade current Internet connection to provide more bandwidth
   - Compress file
   - Break file into manageable pieces (multiple exchanges)
   - Receive the file via physical media (requires exception approval)
12. Firewall requirements
   - Registration of Business Partner static, external, routable IP address in OA firewall
   - Allow port 443 (SSL) for encrypted data exchanges
   - Allow for upload/download of files via the Internet
   - The Business Partner technical team must be available to troubleshoot connectivity problems

**FTP**

FTP as a transport protocol is only permitted for internal transfers. DTE management must approve any requests for FTP traffic. Please refer to the previous exchanges to select an appropriate method of file transmission.

Requirements include:
- A server class machine
- FTP Versions supported: FTP, FTPxxx, MS FTP etc.
- Commonwealth internal network
- Allow for PASSIVE FTps
- Default transmission type for FTP is BINARY except for UNISYS mainframe where default transmission type is ASCII
Firewall Requirements:

The Commonwealth Firewalls must be opened to allow the Business Partner access to DHS servers. The Program Office must submit these requests to DTE. The Business Partner's firewall or firewalls must be configured to allow SeGOVernment servers into the Business Partner network on Commonwealth defined ports. DHS cannot support traffic over non-standard ports.

File (Payload) Requirements
The SeGOV Data Exchanges require adherence to the following file types, compression standard and naming conventions:

File (MIME) Types
For all new data exchanges, transferred files must have a Mime (Multipurpose Internet Mail Extensions) types: doc, txt, zip, xls, mdb, tif etc.
DHS will assist the Coordinator and Business Partner in determining the file names to be transferred.

File Compression
Any Business Partner may elect to compress files using WIN ZIP.

File Size
SeGOV has encountered limited failures due to file size. Large files increase the potential for network latency. In addition, receiving servers/applications may implement directory quotas that restrict the number of files, size of file, or amount of data within a given directory. If the configured data transfer experiences slowness or errors in delivery of a given file, the application team and business partner technical team will be contacted to assist in resolution.

File Naming Conventions
File naming conventions control the routing of a file during execution of the data exchange. SeGOV is dependent on standard file naming patterns in order to move files to their intended locations. To ensure that file names follow existing conventions, file name formats must be coordinated with BIS before any development work is begun. BIS will assist in the definition of file names for data exchanges. It is strongly suggested that applications create unique file names to be transferred. This can be done with a core static name and addition of a sequence or date/time stamp.

For applications involving file transfers from the mainframe application developers must create a parameter file containing a list of files to be sent from the mainframe to the SeGOV staging server. DEA will assist with this process.
**Trigger files**

.end files or trigger files are not required for successful execution of SeGOV. These files may be required for successful execution of the applications that receive files from SeGOV. When creating new exchanges/tasks, application teams must work with BIS team to establish these requirements.

**PGP encryption**

PGP encryption is not required for secure transmission of files. Secure methods defined earlier fulfill these requirements. Within the SeGOV DMZ, files, filenames and folders are encrypted.

Some business partners may request pgp encryption of files. Any requests for this type of transfer MUST be directed to TADU staff. Staff will work with the Business Partner to determine best method of data transfer.

**Server Requirements**

Business Partners using automated transfers must provide current production class servers and configurations as specified below:

**Business Partner’s Data Exchange Servers**

Business Partners must perform data exchanges from systems capable of meeting the availability and performance specifications of these guidelines. This requires the use of current industry standard server class systems and proficient technical support, and precludes the use of workstations and manual processes. “Current” is defined as an industry standard server manufactured within the last three years.

**Business Partner Data Exchange Server Availability**

The Business Partner transfer server must be available to receive files from DHS during the mutually agreed upon transmission time for scheduled data exchanges. It is preferred that all data exchanges occur during non-standard business hours (Monday-Friday 6:00PM – 6:00AM and anytime weekends). DHS requests that notices of planned system maintenance be sent to the Program Office Coordinator and ra-wmadmins@pa.gov.

**Business Partner Secure Transfer - Client**

The department uses the MOVEit Enterprise software suite to configure and exchange data with our business partners. Business Partners are required to use a compatible client to exchange data with the department.
Network Requirements
Business Partners must configure their networks as specified below to optimize exchange reliability and response time.

Transmission Time
Transmission capabilities can be determined by the size of a data transfer and the available network bandwidth. Firewalls may cut off data transmissions that exceed firewall rules. For this reason, we request that large files be zipped during transfer.

Connection speed is only as good as the slowest link to the destination. Please consult with local network personnel to determine that bandwidth is sufficient to accomplish the transfer without delay or failure.

Batch Cycle Times
To avoid negative impact to “online availability and network performance” during core business hours (Monday-Friday 6:00AM through 6:00PM), batch processing and file transfers are to be scheduled during non-peak hours (Monday-Friday 6:00PM through 6:00AM, or anytime Saturday-Sunday).

It is understood that some transfers must occur as a prerequisite for mainframe batch to run. These transfers must be coordinated with BIS SeGOVernment staff and DIMO scheduling staff.

Transmission Speed
The speed of the data transmission is determined by the size of the file and the speed of the slowest communications link between the sender and receiver. The Internet plays a role in this transmission speed. The Internet Service Provider (ISP) that the Business Partner uses and the circuit bandwidth purchased from that ISP are two factors to consider. The bandwidth that is purchased from the ISP is only guaranteed from the purchaser to the ISP. The ISP itself generally has a connection to another ISP to pass traffic to the Internet backbone. Purchasing from the ISP closest to the backbone generally provides less congestion to and from the backbone. It is highly recommended that Business Partners use a high-speed Internet connection (DSL, cable, broadband).

Load Balancing
All stakeholders should avoid unnecessary traffic load peaks and valleys, which strain communications and computing resources. File transfers should be scheduled to occur during non-peak hours between 6:00pm and 6:00am. Applications and regulations should be written to discourage end-of-week and end-of-month processing windows. Stagger file transfers for a given application, to and from specific locations, across the month.

Network Connections
Business Partners must provision Internet bandwidth of sufficient capacity to meet the availability and performance standards as contained in this document. These connections require use of static, routable IP addresses from the gateway to the Internet.
Notifications
Email notifications can be sent to those individuals specified on the data exchange registration form. These notifications are sent to announce the success of transmission or availability of files for download. We prefer that distribution lists be used if more than two individuals in a group need notification. SeGOV is not an email exchange server. It does not manage email groups.

The Program Office Coordinators manage the email addresses with OIS account administration. The SeGOV team does not provide this service.

A failed file transfer is defined as one that failed to successfully deliver or pick up a file. The scheduler presently attempts to re-send the file a maximum five times. Each attempt occurs at a five minute interval. After the sixth attempt the transfer issues an error message that destination host could not be reached. The task must be restarted when connectivity is restored.

An email notification is sent to notify the Business Partner that Browser files are available for download. Email notices can also be generated to notify Business Partners that files have been delivered to the designated destination (FTP, SFTP FTPS). If files are not received as per the designated transmission schedule, the Program Office coordinator must contact SeGOVernment staff and report that the file has not been received. Any requests for retransmission of a file(s) must be submitted to the SeGOVernment team.

The common reasons for a failed transfer and general problem resolution responsibilities and procedures are specified in Attachment (3).

For files that are sent to SeGOV DMZ, email notices are sent
- When a file is uploaded
- When a file is delivered to next location
- When a new file is available
- When file has NOT been downloaded in 7 days
- When file is deleted

Responsibilities
The following responsibilities have been defined to facilitate use of the SeGOVernment data exchanges:

DTE – Infrastructure Management Section
- Back-up support in event of DTE staff absence
- Configuration of Hosts in MOVEit Central
- Configuration of Tasks to move files in MOVEit Central
DTE
• Develop/Update Data Exchange Standards and Procedures
• Physical Architecture Planning
• Technology Proto-typing
• Configure Hosts in MOVEit Central
• Configure/Maintain Hosts in MOVEit Central
• Maintenance of users in MOVEit DMZ
• Server Configuration Management
• Server Capacity Planning
• Manage DHS Server Digital Certificates
• Manage Server Security
• Outreach and Education on use of SeGOVernment
• Migration of new tasks and updates into Production
• Ensuring the ongoing efficient transfer of mission-sensitive data
• Fault isolation and resolution
• Ensures compliance with standards
• Operates the system

DEA
• Understands the process
• Enforce SeGOVernment Coding Standards
• Enforce Date Exchange Standards
• Configure tasks in MOVEit Central
• Maintenance of Tasks in MOVEit Central

DHS Program Office Coordinators
• Owns the business interface with the Business Partners
• Ensures that contracts and data agreements are in place
• Understands the process and standards
• Communicates Business Partner Obligations
• Ongoing Business Partner training for SeGOVernment access and use
• Ensures compliance to Standards in contracts
• Ensures compliance to Standards in operations
• Represents the Business Partners to the Team

Business Partners
• Use the system to do business with DHS
• Communicate business and technical requirements for SeGOVernment exchange participation
• Meet the technical requirements for system use
• Communicate the effectiveness of the process to Program Office Coordinators
• Comply with BIS Standards and Regulations for sensitive data exchange
### Responsibility Matrix

<table>
<thead>
<tr>
<th>Responsibility</th>
<th>DEA</th>
<th>DTE</th>
<th>DTE Infrastructure Management</th>
<th>Coordinators</th>
<th>Business Partner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier 1 support questions</td>
<td></td>
<td>R</td>
<td>C</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Tier 2 support questions</td>
<td>I</td>
<td>A/R</td>
<td>C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tier 3 support questions</td>
<td>I</td>
<td>R</td>
<td>C</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>Determining the size and periodicity of the transfer</td>
<td>A/R</td>
<td>I</td>
<td>I</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>Determining if the file should be electronically transferred</td>
<td>I</td>
<td>A</td>
<td>I</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>eGOV server engineering or configuration</td>
<td>I</td>
<td>A</td>
<td>R/C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Load balancing (peaks and valley avoidance)</td>
<td>C</td>
<td>R</td>
<td>C</td>
<td>I</td>
<td>A</td>
</tr>
<tr>
<td>Generation and distribution of event log</td>
<td></td>
<td>A</td>
<td>R</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notification of receipt or failure</td>
<td>I</td>
<td>A</td>
<td>R</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>Resolution of poor BUSINESS PARTNER performance</td>
<td>C</td>
<td>A</td>
<td>C</td>
<td>I</td>
<td>R</td>
</tr>
<tr>
<td>Security registration of new Business Partners</td>
<td>R</td>
<td>R</td>
<td>A</td>
<td></td>
<td>R</td>
</tr>
<tr>
<td>Security registration of new files</td>
<td>C</td>
<td>R</td>
<td>I</td>
<td>A</td>
<td>C</td>
</tr>
<tr>
<td>Standards enforcement</td>
<td>R</td>
<td>R</td>
<td>A</td>
<td>R</td>
<td>I</td>
</tr>
<tr>
<td>Maintain up to date business / technical contact information</td>
<td>I</td>
<td>A</td>
<td>C</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>Contract compliance</td>
<td>I</td>
<td>I</td>
<td>C</td>
<td>A</td>
<td>R</td>
</tr>
<tr>
<td>Guidelines revision and maintenance</td>
<td>C</td>
<td>R</td>
<td>C</td>
<td>I</td>
<td>I</td>
</tr>
</tbody>
</table>
Reports and Logs

Logs are maintained for all data exchanges. The log displays the application name, file name, sending and receiving party, date of action, action (upload, download), file size and the success of the action.

System Maintenance

SeGOVernment is dependent on network services, database, server and firewall operations for operability. As such, established maintenance windows designated by these teams and the Office of Administration affect SeGOVernment. Outages may occur during these windows. Data transfers will resume once system availability and operations have been restored.

The MOVEit Software will be periodically updated to meet expanded operational business requirements. The SeGOVernment Exchange System will be maintained according to current business standards. Requests for enhancement will be reviewed, prioritized and forwarded to the software vendor. The software vendor has final approval of any submitted enhancements. The software vendor will determine release requirements for any submitted requests.

Change Management

All changes to the MOVEit Software Suite will follow the DHS standard Change Management procedures as specified by DHS’s Business and Technical Standards. The creation of new exchanges are considered operational configurations and do not require time consuming and costly systems software generations.

Change requests must be submitted through the Program Office Coordinator. Please complete a TFS User Story and SeGOV data transfer worksheet. DEA will maintain the list of MSU requests and assign to available personnel. As the SeGOV team supports the enterprise, we request two week notice to complete these requests. Program Office Coordinators are required to maintain copies of these requests for future use.

Backup Procedures

The DHS SeGOVernment exchange servers are backed-up according to established department procedures and schedules. The Server support contractor is responsible for the backup of these servers. A back up of all files on the server is done every weekend and incremental backups are done daily for all the files that changed since the last incremental backup. All backups are stored for a period of 30 days.

Disaster Recovery

The MOVEit SeGOVernment Application has been identified as a critical component in the DHS Disaster Recovery Plan. The SeGOVernment exchange servers will be a part of the DHS Enterprise Disaster Recovery Plan. DIMO has responsibility for this process. Please contact DIMO for assistance or questions regarding the Enterprise plan.
### Attachments

#### Attachment #1 – SeGOV User Registration Form

**SeGOV user Registration Form**  
Request for new Managed Domain Account

<table>
<thead>
<tr>
<th>Field</th>
<th>Requirement</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>OU</td>
<td>To be completed by OIS Account Administration</td>
<td></td>
</tr>
<tr>
<td>Last Name</td>
<td>Mandatory</td>
<td></td>
</tr>
<tr>
<td>First Name</td>
<td>Mandatory</td>
<td></td>
</tr>
<tr>
<td>Do you have a DPW userid</td>
<td>Mandatory - Y/N</td>
<td></td>
</tr>
<tr>
<td>If Y - please provide id(s)</td>
<td>Mandatory - if Y above</td>
<td></td>
</tr>
<tr>
<td>Account</td>
<td>b-</td>
<td>To be completed by OIS Account Administration</td>
</tr>
<tr>
<td>Password</td>
<td>To be completed by OIS Account Administration</td>
<td></td>
</tr>
<tr>
<td>Phone Number</td>
<td>Mandatory</td>
<td></td>
</tr>
<tr>
<td>email Address</td>
<td>Mandatory</td>
<td></td>
</tr>
<tr>
<td>User IP Address</td>
<td>Mandatory</td>
<td></td>
</tr>
<tr>
<td>DPWmoveitprogram</td>
<td>Mandatory - Select Value from Drop Down List</td>
<td></td>
</tr>
<tr>
<td>DPWmoveitsubfolder</td>
<td>If this is a county organization, enter County Name</td>
<td>For a joinder enter the first County in the joinder name Else, leave blank</td>
</tr>
<tr>
<td>FEIN</td>
<td>Mandatory</td>
<td></td>
</tr>
<tr>
<td>Enable Account</td>
<td>Yes</td>
<td>OIS Account Administration will enable upon completion</td>
</tr>
<tr>
<td>Environment</td>
<td>Select Value from Drop Down List</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Enter Entity Name - Follow by Browser, FTP, SFTP, FTPS</td>
<td></td>
</tr>
<tr>
<td>Full Name Description</td>
<td>Enter Entity Name</td>
<td></td>
</tr>
<tr>
<td>Business Partner Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enter Business Partner Address1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Business Partner Address2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>City, State, Zip</td>
<td></td>
</tr>
<tr>
<td>Expires</td>
<td>Yes</td>
<td>follow standard 60 day expiration of all passwords</td>
</tr>
<tr>
<td>User IP Address</td>
<td>Please consult your Technical person or Internet Service Provider.</td>
<td>We need to know the IP address that will come through the OA Firewall at the Commonwealth.</td>
</tr>
<tr>
<td>FEIN</td>
<td>This is the Federal Tax ID assigned to the entity</td>
<td></td>
</tr>
<tr>
<td>Environment</td>
<td>Default is Production, please indicate is test or both are required</td>
<td></td>
</tr>
<tr>
<td>FTP Accounts</td>
<td>FTP Accounts will be issued machine service accounts that begin with b-srv</td>
<td>These accounts will be manually created in AD with DPWmoveitsubfolder being added by OIS account administration. DPWmoveitprogram attribute is FTP.</td>
</tr>
</tbody>
</table>
### Attachment #1.1 – SeGOV User Registration Change Form

**SeGOV user Registration Form**

Request Update email Managed User Information

<table>
<thead>
<tr>
<th>Current Information</th>
<th>CHANGE</th>
<th>Effective Date is 5-day Minimum</th>
</tr>
</thead>
<tbody>
<tr>
<td>OU</td>
<td></td>
<td>To be completed by OIS Account Administration</td>
</tr>
<tr>
<td>Last Name</td>
<td></td>
<td>Mandatory - cannot change Users from a change form. New user requires full registration.</td>
</tr>
<tr>
<td>Middle Initial</td>
<td></td>
<td>Mandatory</td>
</tr>
<tr>
<td>First Name</td>
<td></td>
<td>Mandatory</td>
</tr>
<tr>
<td>Account</td>
<td>b-</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Phone Number</td>
<td></td>
<td>Mandatory</td>
</tr>
<tr>
<td>email Address</td>
<td></td>
<td>Mandatory</td>
</tr>
<tr>
<td>User IP Address</td>
<td></td>
<td>Mandatory</td>
</tr>
<tr>
<td>FEIN</td>
<td></td>
<td>Mandatory</td>
</tr>
<tr>
<td>Active/Suspend</td>
<td></td>
<td>Mandatory</td>
</tr>
<tr>
<td>Environment</td>
<td></td>
<td>Mandatory Select Value from Drop Down List</td>
</tr>
<tr>
<td>Type of Connection</td>
<td></td>
<td>Select type of Connection from list: Browser, FTP, SFTP, FTPS</td>
</tr>
<tr>
<td>Full Name Description</td>
<td></td>
<td>Mandatory Enter Entity Name</td>
</tr>
<tr>
<td>Business Partner Address</td>
<td>Enter Business Partner Address1 Business Partner Address2 City, State, Zip</td>
<td></td>
</tr>
<tr>
<td>Expires</td>
<td>Yes</td>
<td>Follow standard 60 day expiration of all passwords</td>
</tr>
<tr>
<td>Reason for Change</td>
<td></td>
<td>MANDATORY New users CANNOT be registered as a change. Users that need to be SUSPENDED need to be identified as such. Also include attributes DPWmoveitprogram folder name and DPWmoveitsubfolder (both supplied by Program Office) for all suspended accounts and additions to user attributes.</td>
</tr>
</tbody>
</table>

**User IP Address**

Please consult your Technical person or Internet Service Provider. We need to know the external routable IP address that will come through the OA Firewall at the Commonwealth.

**FEIN**

This is the Federal Tax ID assigned to the entity

**Environment**

Default is Production; please indicate if test or both are required.

**FTP Accounts**

FTP Accounts will be issued machine service accounts that begin with b-srv. These accounts will be manually created in AD with DPWmoveitsubfolder being added by OIS account administration. DPWmoveitprogram attribute is FTP.
# Attachment #2 – SeGOV (Secure FTP) Setup Sheet

<table>
<thead>
<tr>
<th></th>
<th>SAT</th>
<th>PROD</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business Partner</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Business Partner Full Name</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Business Partner Address 1</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Business Partner Address 2</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Business Partner City, State, Zip</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>DPW IP (Source/Destination)</strong></td>
<td>199.5.88.8</td>
<td>199.5.87.8</td>
</tr>
<tr>
<td><strong>BP2DPW UserID (supplied by DPW)</strong></td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td><strong>BP2DPW Password (supplied by DPW)</strong></td>
<td>Send under separate cover</td>
<td>Send under separate cover</td>
</tr>
<tr>
<td><strong>Upload Path:</strong></td>
<td><a href="https://missl.dhs.state.pa.us">https://missl.dhs.state.pa.us</a></td>
<td><a href="https://missl.dhs.state.pa.us">https://missl.dhs.state.pa.us</a></td>
</tr>
<tr>
<td><strong>Static File Name:</strong></td>
<td>Program Office to provide</td>
<td>Program Office to provide</td>
</tr>
<tr>
<td><strong>Port to connect to State of Pennsylvania</strong></td>
<td>22</td>
<td>22</td>
</tr>
<tr>
<td><strong>DPW Secure FTP</strong></td>
<td>MOVEit</td>
<td>MOVEit</td>
</tr>
<tr>
<td><strong>DPW Secure FTP Software Provider</strong></td>
<td>IPSwitch</td>
<td>IP Switch</td>
</tr>
<tr>
<td><strong>DPW Operating System</strong></td>
<td>Server 2008</td>
<td>Server 2008</td>
</tr>
<tr>
<td><strong>BP Technical Contact Name</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>BP Technical Contact Email</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>BP Technical Contact Phone</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>BP FEIN</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Business Partner URL</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Business Partner Source IP</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Business Partner Destination IP</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>DPW2 Business Partner UserID</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>(supplied by Business Partner)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>DPW2 Business Partner Password</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>(supplied by Business Partner)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>How will BP access site</strong></td>
<td>Internet</td>
<td>Internet</td>
</tr>
<tr>
<td><strong>Circuit/Internet</strong></td>
<td>SFTP</td>
<td>SFTP</td>
</tr>
<tr>
<td><strong>Method of Transfer SFTP</strong> (Requires exchange of Userid/Pwd and keys on Port 22)**</td>
<td>SFTP</td>
<td>SFTP</td>
</tr>
<tr>
<td><strong>BP Secure Client Operating System</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>BP Secure Client in Use</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>BP Secure Client Software Provider</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>DPW Connectivity Contact</strong></td>
<td>Barbara Wadlinger</td>
<td>Barbara Wadlinger</td>
</tr>
<tr>
<td><strong>DPW Connectivity Contact Email</strong></td>
<td><a href="mailto:bawadlinger@state.pa.us">bawadlinger@state.pa.us</a></td>
<td><a href="mailto:bawadlinger@state.pa.us">bawadlinger@state.pa.us</a></td>
</tr>
<tr>
<td><strong>DPW Connectivity Contact Phone</strong></td>
<td>717-346-4332</td>
<td>717-346-4332</td>
</tr>
</tbody>
</table>
Attachment #3 – Error Handling

Data exchange problems can be reported by contacting ra-wmadmins@pa.gov. Please provide the following information:

**SeGOVernment data exchanges** -
Business Partner name
Name of person to contact
Phone Number
Email address
File Name in Question
Date/Time it should have run
Description of the problem including error message
Copy of Error log (inbound server transfers)

**Mainframe Transfers** –
Business Partner Name
Name of person to contact
Phone Number
Email address
File Name in Question
Date/Time it should have run
Mainframe Job or Qualifier*Filename

BIS will perform all structured problem testing.

**Central Site Data Exchange Errors** -
BIS will identify and resolve problems dealing with failures or resource limitations of the central site environment. These failures include:

- Mainframe problems
- Application problems affecting the generation of output files or the processing of input files
- Failures of the transfer servers
- Saturation of the data link to the Business Partner
- Load saturation of the DHS server
### FTP and SeGovernment Error Messages -

<table>
<thead>
<tr>
<th>Error</th>
<th>Exchange</th>
<th>Most Likely Failure</th>
<th>Tier 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access denied</td>
<td>B</td>
<td>Remote server configuration or environment</td>
<td>Notify technical staff. Verify that IP address, directory, password, keys (if required) have not changed</td>
</tr>
<tr>
<td>Broken pipe – lost connection</td>
<td>F</td>
<td>Communication error – transfer has been stopped</td>
<td>Verify file size, contact technical staff to analyze lost connection failure</td>
</tr>
<tr>
<td>Connection refused</td>
<td>B</td>
<td>Remote server configuration or environment</td>
<td>Notify technical staff. Verify directory, password, and file name has not been changed</td>
</tr>
<tr>
<td>Connection timed out</td>
<td>B</td>
<td>Communication errors, excessive line loading</td>
<td>Notify technical staff – Firewall may be denying access.</td>
</tr>
<tr>
<td>Login failed</td>
<td>B</td>
<td>Invalid credentials</td>
<td>Notify user and verify UserID, password have not expired. Verify that keys (if required) have not changed</td>
</tr>
<tr>
<td>Lost connection</td>
<td>F</td>
<td>Communication errors, excessive line loading</td>
<td>Notify technical staff. Attempt a TRACERT then verify IP address and firewall allow traffic.</td>
</tr>
<tr>
<td>No such file or directory</td>
<td>B</td>
<td>Remote server configuration or environment has changed</td>
<td>Notify technical staff. Verify file and directory structure</td>
</tr>
</tbody>
</table>

W = eGOV Exchange   F = Legacy FTP   B = Both
Exemptions from this Standard:
In the event an exemption is required for reasons such as the need to comply with requirements for a federally mandated system, please contact the manager of DHS DTE Technical Architecture and Development Unit.

Refresh Schedule:
All standards and referenced documentation identified in this standard will be subject to review and possible revision annually or upon request by the DHS Information Technology Standards Team.

Standard Revision Log:

<table>
<thead>
<tr>
<th>Change Date</th>
<th>Version</th>
<th>Change Description</th>
<th>Author and Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/01/01</td>
<td>1.0</td>
<td>Initial creation.</td>
<td>BIS/DIMO</td>
</tr>
<tr>
<td>09/15/03</td>
<td>2.0</td>
<td>Comply with DHS Technical Standards</td>
<td>BIS/DIMO</td>
</tr>
<tr>
<td>07/31/06</td>
<td>2.1</td>
<td>Updated but not published</td>
<td>BIS</td>
</tr>
<tr>
<td>08/14/07</td>
<td>2.2</td>
<td>Update of Technical Standards</td>
<td>BIS</td>
</tr>
<tr>
<td>11/07/11</td>
<td>3.0</td>
<td>Update of Technical Standards</td>
<td>BIS</td>
</tr>
<tr>
<td>09/06/13</td>
<td>3.1</td>
<td>Update of Technical Standards</td>
<td>BIS-B Wadlinger</td>
</tr>
<tr>
<td>04/08/14</td>
<td>3.1</td>
<td>Reviewed – no changes</td>
<td>BIS-B Wadlinger</td>
</tr>
<tr>
<td>02/27/15</td>
<td>3.2</td>
<td>Update of Technical Standards</td>
<td>BIS-B Wadlinger</td>
</tr>
<tr>
<td>11/18/15</td>
<td>3.3</td>
<td>Reviewed – no change</td>
<td>BIS-B Wadlinger</td>
</tr>
<tr>
<td>02/24/16</td>
<td>3.3</td>
<td>Reviewed – no change</td>
<td>BIS-B Wadlinger</td>
</tr>
<tr>
<td>02/01/17</td>
<td>3.4</td>
<td>Reviewed – minor Change</td>
<td>BIS-B Wadlinger</td>
</tr>
</tbody>
</table>