REGIONS

File Transfer Protocols

SFTP (SSH File Transfer Protocol)

- Can be used via command-line (please check with your technical contact to see if this is available), or via software known as a "Client," such as WS_FTP Pro, Cute FTP, or a variety of other commercially-available products
- Requires authentication via ID, password and SSH key. This means you would be required to generate an SSH key pair and store the private key in the Client you are using, then provide the public key to Regions. Regions will in turn provide you with credentials (user ID, password, host-name and port) for log in purposes
- SFTP lends itself to automation via scripts (using the command-line method) or via scheduling in Client software
- Allows file transfers to occur over the public Internet using SSH to secure the channel

HTTPS (Hyper Text Transfer Protocol Secure)

- Generally requires the use of a Web browser (Internet Explorer, Firefox, etc.)
- Requires authentication via ID, password, and SSL Certificate. Regions will generate an SSL Certificate to import into your Web browser, and then you will be provided with a URL, user ID, and password to access the secure file transfer site
- HTTPS is best suited for manual, non-scripted file uploads and/or downloads
- Allows file transfers to occur over the public Internet using SSL to encrypt the communication

FTPS (File Transfer Protocol with SSL)

- Can be used via command-line (please check with your technical contact to see if this is available), or via software known as a "Client," such as WS_FTP Pro, Cute FTP, or a variety of other commercially-available products
- Requires authentication via ID, password, and SSL Certificate. Regions will provide a public SSL certificate that you would need to load to your system or Client. Then you will be provided with credentials (user ID, password, host-name and port) for log in purposes.
- FTPS lends itself to automation via scripts (using the command-line method) or via scheduling in Client software
- Allows file transfers to occur over the public Internet using SSL to encrypt the communication

Connect: Direct

- Proprietary file transfer system owned and supported by IBM
- Peer-to-peer, meaning Connect: Direct must be licensed and executed on both ends of the file transfer
- Cannot be used over the public Internet – requires either a site-to-site VPN connection, or customer/vendor-provided point-to-point data circuit
- SSL encryption-capable (via optional Secure Plus module)

Applicability Standard 2 (AS2)

- Protocol which is secured using digital certificates and encryption
- AS2 is built on the HTTPS protocol and transfers are encrypted using Secure Sockets Layer
- To use this protocol, one must have AS2 software, which acts as both a Client and a Server
- Due to the complexity of configuring and using this protocol, it is typically passed over for more "traditional" protocols such as SFTP, FTPS and HTTPS