AGILE CYBER DEVELOPMENT & SUSTAINMENT
ASSURED FILE TRANSFER REQUEST / APPROVAL / TRACKING FORM

Section I

Media Control Number: _____ Media Type: _____

Section II

Source IS: _____ Classification: _____

Destination IS: _____ Classification: _____

Media Disposition: _____ Overall Classification: _____

Transfer Type: _____ Destination File: ☐ Upload (Add Files to IS) ☐ Download (Remove Files from IS)

If Non-Human Readable, Identify the Process Name: _____

(Use Procedure Document # As Applicable)

Justification for Transfer:

_____

Files for Transfer: _____

File Names, Types, and Classification:

Name: _____ File Type: _____ Classification: _____

Name: _____ File Type: _____ Classification: _____

Name: _____ File Type: _____ Classification: _____

Name: _____ File Type: _____ Classification: _____

Name: _____ File Type: _____ Classification: _____

Additional File List(s) Attached*: ☐

* **NOTE**: If you have more files than space available, list remaining files on a separate list(s) and attach to the request.

Media Transportation: Will media be transported outside an approved area? ☐Yes ☐No

If Yes, Media Destination: _____

Destination POC / Customer Name: _____

Destination Address / Location: _____

Media Encryption: Cryptographic mechanisms during transport outside of controlled areas shall be either an NSA or FIPS 140-2 compliant algorithm. [MP-5(4)]

Will Media be Encrypted: ☐Yes ☐No

AFT Requester

I certify that the above file(s)/media to be transferred to/from the IS are required to support the development and sustainment contractual efforts on the ACDS contract.

Name: _____ Date: _____ Signature: _____

Media Control Number: _____

Section III

Approval:

If Applicable: This High-to-Low Assured File Transfer Request has been reviewed and is approved using the procedures identified in the ACDS AFT SOP for Unclassified High-to-Low transfers.

Designated Authorizing Official

Name: _____ Date: _____ Signature: _____

This Assured File Transfer Request has been reviewed and is approved by:

Information System Security Manager / Information System Security Officer

Name: _____ Date: _____ Signature: _____

Contractor Program Security Officer

Name: _____ Date: _____ Signature: _____

Section IV

Anti-Virus Scan – Data Transfer Agent

Anti-Virus Scan: Perform two virus / malware scans. The first scan is performed once the file(s) is downloaded to the media on the originating system. The second scan is performed on the media in the target system prior to uploading the file(s) to the system. When possible, use virus / malware scanning products from different vendors. [SI-3]

Origination Media Scan: ☐ Yes ☐ No # Files Scanned: _____ # Threats Found: _____

Destination Media Scan: ☐ Yes ☐ No # Files Scanned: _____ # Threats Found: _____

Transfer – Data Transfer Agent, Requester / Subject Matter Expert (Two-Person Integrity)

The AFT of the requested files has been completed following the approved procedures contained in the ACDS Assured File Transfer Standard Operating Procedures. Two-Person Integrity (TPI) was maintained during the AFT process as required.

Files Transferred: _____ Date: _____

DTA Name: _____ Signature: _____

SME Name: _____ Signature: _____

Section V

Media Disposition – Media Custodian

The data transfer media has been verified as:

Optical Media Destroyed: ☐ Yes ☐ No ☐ N/A
Optical Media Retained: ☐ Yes ☐ No ☐ N/A
SSD Media Sanitized: ☐ Yes ☐ No ☐ N/A

Name: _____ Date: _____ Signature: _____