Instructions for Completing the Request for Access to CMS Electronic File Transfer (EFT) Secure Point of Entry (SPOE) Id form

This form is to be completed and submitted to request a corporate CMS NDM/Connect:Direct ID. This ID will be used only to transmit data to and from CMS.

1. Organization/Company Information – to be completed by Company

Organization/Company Name:	Name of Organization or company who will transmit data to and from CMS.
Organization/Company EIN:	The organization's or company's Employer Identification Number.
Organization Contact Name:	Individual who serves as contact with CMS.
Organization Contact Phone/Fax:	Phone number and fax number for contact person.
Organization Contact Email:	Email address of contact person.
Application(s) Using:	Name of CMS application(s), such as Drug Card Project or PECOS.
MAC id	MAC name affiliated with the request

2. Organization/Company Technical Contact Information – to be completed by Company

Technical Contact Name:	Person who provides technical details and setup for transmittal processing. This person will be contacted with the CMS node name and assigned SPOE ID.
Technical Contact Phone/Fax:	Phone number and fax number for technical contact.
Technical Contact Email:	Email address of technical contact.
Company Node Name:	The organization's or company's NDM node name.

The Organization Contact must read and sign page 2 then forward the signed form to your CMS Contact for approval.

3. CMS Approver Information

Business Owner Approver Name:	The CMS business owner who approves this access request is responsible to immediately inform the EFT GTL's of any change in status of the requesting organization..
Business Owner Phone/Fax:	Phone number and fax number for business owner approver.
Date:	Date of approval
EFT GTL Approver Name:	The CMS Enterprise File Transfer (EFT) GTL who approves this access request. .
EFT GTL Approver Phone/Fax:	Phone number and fax number for EFT GTL approver.
Date:	Date of approval

CMS Approver must review and if appropriate, sign page 2 then mail the signed form to the address below for processing.

Lockheed Martin
Attn: EUA Support Team
7500 Security Boulevard
Mail Point N1-19-18
Baltimore, MD 21244.

Request for Access to CMS
Electronic File Transfer (EFT)
Secure Point of Entry (SPOE) Id

- Provide information on page 1
- Organization Contact* and CMS Approver*** read and sign page 2
- Forward form to CMS, Attn: CMS EFT Support Team, 7500 Security Boulevard, N1-19-18, Baltimore, MD 21244
- Questions regarding this form may be forwarded to the CMS Service Desk at 1-800-562-1963 or 410-786-2580

TYPE OF TW USERID NEEDED:

_____ CMS Connect Direct _____ Digital Certificate
_____ MFT Platform Server (CyberFusion) _____ MFT Internet Server

1. Organization/Company Information

Organization/Company Name: _____
Organization/Company EIN: _____
Organization Contact Name:* _____
Organization Contact Phone: _____ Fax: _____
Organization Contact Email: _____
Application(s) Using: _____
MAC id _____

2. Organization/Company Technical Contact Information

Technical Contact Name:** _____
Technical Contact Phone: _____ Fax: _____
Technical Contact Email: _____
Company Node Name: _____

3. CMS Approver Information

Business Owner Approver Name: _____
Business Owner Phone: _____ Fax: _____
Date: _____

EFT GTL Approver Name: _____
EFT GTL Phone: _____ Fax: _____
Date: _____

* Person who serves as contact with CMS.
** Person who provides technical details and setup for processing. This person will be contacted with the CMS node name and assigned SPOE ID.

DO NOT WRITE BELOW THIS LINE – FOR CMS USE ONLY

IDs Assigned By: _____ Date: _____
Technical Contact Notified: _____ Date: _____

SPOE ID: NDM _____
Digital Certificate: _____

NDMID: TW _____

SECURITY REQUIREMENTS FOR USERS OF CMS'S COMPUTER SYSTEMS

CMS uses computer systems that contain sensitive information to carry out its mission. Sensitive information is any information, which the loss, misuse, or unauthorized access to, or modification of could adversely affect the national interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act. To ensure the security and privacy of sensitive information in Federal computer systems, the Computer Security Act of 1987 requires agencies to identify sensitive computer systems, conduct computer security training, and develop computer security plans. CMS maintains a system of records for use in assigning, controlling, tracking, and reporting authorized access to and use of CMS's computerized information and resources. CMS records all access to its computer systems and conducts routine reviews for unauthorized access to and/or illegal activity.

Anyone with access to CMS Computer Systems containing sensitive information must abide by the following:

- Do not disclose or lend your IDENTIFICATION NUMBER AND/OR PASSWORD to someone else. They are for your use only and serve as your "electronic signature". This means that you may be held responsible for the consequences of unauthorized or illegal transactions.

- Do not browse or use CMS data files for unauthorized or illegal purposes.

- Do not use CMS data files for private gain or to misrepresent yourself or CMS.

- Do not make any disclosure of CMS data that is not specifically authorized.

- Do not duplicate CMS data files, create subfiles of such records, remove or transmit data unless you have been specifically authorized to do so.

- Do not change, delete, or otherwise alter CMS data files unless you have been specifically authorized to do so.

- Do not make copies of data files, with identifiable data, or data that would allow individual identities to be deduced unless you have been specifically authorized to do so.

- Do not intentionally cause corruption or disruption of CMS data files.

A violation of these security requirements could result in termination of systems access privileges and/or disciplinary/adverse action up to and including removal from Federal Service, depending upon the seriousness of the offense. In addition, Federal, State, and/or local laws may provide criminal penalties for any person illegally accessing or using a Government-owned or operated computer system illegally.

If you become aware of any violation of these security requirements or suspect that your identification number or password may have been used by someone else, immediately report that information to the CMS Service Desk at 410-786-2580 or 1-800-562-1963.

Organization Contact Signature: _____Date: _____

CMS Approver Signature: _____ Date: _____