Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION

User Access Request Package
Financial Management System (FMS)

Version 2023.1
April 2023

FMS is an FSA Mission Important System and is Categorized by FIPS 199 as a Moderate Impact System

DOCUMENT CLASSIFICATION
This document is UNCLASSIFIED and does not contain sensitive information
For Official Use Only

US Department of Education
Federal Student Aid
Union Center Plaza
830 First Street, NE
Washington, DC 20002

Table of Contents

Revision History

Version	Description of Change	Date	Author	Approver
2023.1	Rebuilt forms in Word/PDF for Section 508 compliance	April 2023	FMS Security	FMS Security
2022.1	Changed the version and date on the cover page. Updated page headers with new dates. Added back removed roles. Added ability for Security to initial each role request Improved 508 compliance	May 2022	FMS Security	FMS Security
2021.2	Changed the version and date on the cover page. Updated page headers with new dates. Updated the UARF to be 508 compliant. Added new responsibility “FSA SRVC TROR Reporting” to Table of FMS Responsibilities.	September 2021	FMS Security	FMS Security
2020.2	Changed the version and date on the cover page. Updated page headers with new dates. Added AIMS check box in Section III for internal users.	September 2021	FMS Security	FMS Security

Instructions on How to Apply for Access to FMS

The Federal Student Aid (FSA) security forms and security awareness and training materials are being provided to grant you access to the Oracle Federal Financial Management System (FMS). The information requested in the security form and attachments will be used ONLY to grant you system access and will be used for no other purpose. Please follow the instructions below and EMAIL THE COMPLETED FORM TO THE FMS OPERATIONS HELP DESK UPON COMPLETION OF THE FORM. The email address is FMS.OPERATIONS@ed.gov. Important note to Federal Loan Servicers (TIVAS/NFPs): Please wait to submit your FMS User Account Request Package until you have the following items: Federal Student Aid network account (ed.gov email) and US Department of Education PIV card/USAccess PIV card.

Step	Description
1	Save the FMS User Access Package to your local drive.
2	Complete Section 1 – User Information
3	If you selected "Internal User" in Section I, item I-1, please complete the following sections: • Section II: Supervisor Information/Approval • Attachment A.1 – Internal User Rules of Behavior • Attachment B – Privacy Act Statement • Attachment C – Table of FMS Responsibilities (**except** for users from Federal Loan Servicers – TIVAS/NFPs) • Security Training Acknowledgement Form: Sign and submit the last page of the security awareness presentation.
4	If you selected "External User" in Section I, item I-1, ensure the following sections are completed: • Section II: Supervisor Information/Approval with Printed Title of Executive (e.g., President, CEO, CIO, CFO, etc.), Printed Name of Executive, Signature, and Date in which signatory authority was provided for SECTION II-8. • Attachment A.2 – External User Rules of Behavior • Attachment B – Privacy Act Statement • Security Training Acknowledgement Form: Sign and submit the last page of the security awareness presentation.
5	Complete Section I-10 - Shared Secret. Please select ONE of the listed questions and provide an answer in the space provided. The answer to the question you selected will be used to verify your identity when calling the FMS Help Desk.
6	Complete **Section I-11 - FSA/FMS/FPASS ID Information.** Please complete all the fields within this sections that pertain to you (may be more than one). • I-11.1. Please provide your current FSA Logon ID (e.g., JOHN.DOE.FSA) if applicable. • I-11.2. If you are a current or former FMS user, please list all your FMS Logon IDs. • I-11.3. If you access FSA resources via FPASS, please provide your FPASS ID (e.g., John.Doe).
7	Have your supervisor complete and sign Section II – Supervisor Information/Approval. *Note: A supervisor who is also a user should obtain the signature of his or her next level of authority.* **Only external users** must ensure that a Titled Executive from your organization provides signed acknowledgement that security due diligence has been performed and the individual is trustworthy.
8	Skip Section III - ED/Federal Student Aid FMS Information System Security Officer (ISSO) Approval. The FMS ISSO will complete this section after confirming your identity and access privilege.
9	Review the security awareness and training information sent with this package. After your review, sign the training acknowledgement form at the end of the training material.
10	Submit the *signed* User Access Request Form and *signed* Security Training Acknowledgement Form. You can do this by submitting them directly to the FMS Operations Help Desk/FMS Security Team. Completed forms can also be mailed to the address listed on the cover page of the FMS User Access Request Package.
11	Keep a copy of the completed, signed, Security User Access Package and Training Acknowledgement Form for your records.

Note for Internal Users (Servicers and Department of Education Users): You will receive an email from the FMS Operations Help Desk with instructions for login with your PIV card after your form and training acknowledgement are received and processed. Any FMS user who fails to logon and access FMS or fails to login within a period of 30 days thereafter will have their access automatically changed to a status of inactive. To re-activate your account, please contact the FMS Help Desk. The telephone number is 1-800-433-7327 Option 1. The FMS Operations Help Desk hours of operation are Monday – Friday 7:30am-5:30pm ET.

Note for External Users (Lenders and Guaranty Agencies): You will receive an email from the FMS Operations Help Desk with your User ID and instructions on how to obtain your password and access to the system after your form and training acknowledgement are received and processed. Any FMS user who fails to logon and access FMS to change the temporary password within the first 24 hours or who, after establishing a password, fails to logon and access FMS for a period of 30 days will have their access automatically changed to a status of inactive. You may request to have your FMS User ID be re-established by the FMS Operations Help Desk. The FMS Help Desk telephone number is 1-800-433-7327 Option 1. The FMS Operations Help Desk hours of operation are Monday – Friday 7:30am-5:30pm ET.

FMS User Access Request Form

This form replaces all previous FMS User Access Request Forms

Section I: User Information

I-1. User Type (check applicable box):

□ Department of Education (Internal User)
□ Contractor (Internal User)
□ Federal Loan Servicer (TIVAS/NFPs)
□ External User (Employee or Agent of a Guaranty Agency or Lender/Servicer)

If you are a new internal user, please provide your e-QIP number:

I-2. Account Action Requested (check applicable box):

□ New User
□ Change Access
□ Renew Access
□ Deactivate User

I-3. First Name, Middle Initial, Last Name:

I-6. Job Title:

I-7. Work Location:

I-8. Work Telephone Number:

I-9. Work Email Address:

I-10. Shared Secret (Please select ONE of the following security questions):

□ What street did you live on in third grade?

□ What is the name of your favorite food?

□ What is the name of the high school you attended?

□ What is the location of your favorite vacation or trip?

□ What is the name of your favorite restaurant?

I-11.1. Do you have an FSA Logon ID (e.g., JOHN.DOE.FSA):

I-11.2. List all FMS Logon IDs (if any):

I-11.3. FPASS ID (if any, e.g., John.Doe):

I-12. Organization Information and Level of Access (check the applicable box):

□ Guaranty Agency

Access Level (select one):

□ FSA GA Manager

□ FSA GA User

□ FSA GA Inquiry

Enter GA Number:

Enter GA Name:

□ Servicer or Servicer Trustee (Note: The responsibility ‘FSA LARS Lender/Servicer’ will automatically be granted)

Enter Servicer ID:

Enter Servicer Name:

□ Lender or Lender Trustee (Note: The responsibility ‘FSA LARS Lender/Servicer’ will automatically be granted)

Enter Lender ID:

Enter Lender Name:

I-13a. Lender ID Information for Lenders and Lender Trustees

For each Lender ID (LID) for which you have responsibility, *identify the level of access you are requesting by completing the information below*. If more space is required, please submit additional pages. The following levels are available:

- Submit Level: Allows the user to view, maintain, edit, and submit invoice data to FSA
- Maintain Level: Allows the user to view, maintain, and edit invoice data, but not to submit invoices to FSA
- View Level: Allows the user to view invoice data, but not to make any changes or submit any invoice data to FSA

Line #	Lender ID (LID)	Level of Access	Action
		Maintain Level	Add
		Maintain Level	Add
		Maintain Level	Add
		Maintain Level	Add
		Maintain Level	Add

I-14. Person Requesting Access Signed Acknowledgement:

Signature of Person Requesting Access and Date

Section II: Supervisor Information and Approval

II-1. Supervisor’s Full Printed Name:

II-2. Supervisor’s Job Title:

II-3. Supervisor’s Telephone Number:

II-4. Supervisor’s Work Email:

II-5. Supervisor’s Signed Acknowledgement:

Signature of Supervisor and Date

II-6. Printed Title of Executive (e.g., President, CEO, CIO, CFO):

II-7. Printed Name of Executive:

II-8. Titled Executive for External Users Signed Acknowledgement:

I hereby acknowledge that our organization has provided security due diligence and will only hire and maintain trustworthy staff to access Federal Student Aid (FSA) data. As a Department of Education Partner, we have followed recommended guidance and completed the applicable and appropriate background checks (in accordance with state and local laws) prior to allowing this employee access to FSA data and systems. I certify this individual to be trustworthy.

Signature of Titled Executive and Date

Section III: Federal Student Aid FMS Information Systems Security Officer Approval

Note: This section shall be completed by the FMS ISSO and is for Federal Student Aid use only.

□ External User/No Clearance Required

Federal Student Aid Personnel Security Clearance Level:

□ T1
□ T2
□ T4
□ None

Federal Student Aid Personnel Security Clearance Type:

□ Preliminary
□ Pending
□ Final

Federal Student Aid Personnel Security Level Required (based on responsibilities selected):

□ T1
□ T2
□ T4

□ AIMS Access Required

Printed Name of ISSO:

Printed Name of Alternate ISSO:

Signature of ISSO or Alternate ISSO and Date

Acknowledgement of Internal User Responsibilities

Internal User Security Access Agreement

Attachment A.1 – Internal Rules of Behavior for the Federal Student Aid Financial Management System

I hereby accept the obligations contained in this agreement in consideration of my being granted access to the Department of Education (ED), Federal Student Aid (FSA), Financial Management System (FMS), and/or its component applications. I understand that the equipment and software provided is the property of the Department of Education, and I acknowledge and accept that access is a conditional privilege granted to me for only as long as I have a bona fide need. I will adhere to the governing United States Laws and the Department of Education policies, rules, and guidelines. I accept the Department of Education's right to monitor application use for security purposes and that I have no expectation of privacy when using Department of Education computing resources. I understand that failure to comply with these rules can result in the suspension or termination of my access to FMS.

Accordingly, I hereby certify that:

On the Subject of Information Assurance, I will:

a. Know the sensitivity of the information processed on FMS computing resources (e.g., financial sensitive, privacy act sensitive, proprietary information).

b. Ensure that system media and system output are marked according to their sensitivity.

c. Take reasonable care to protect FMS information whether electronic or in hardcopy, limiting access to a need-to-know basis, and prevent disclosure to unauthorized personnel.

d. Take necessary steps to avoid the introduction of malicious code into any computing resource. I am aware of the anti-virus software available to me and am familiar with its use.

e. Know who my site computer security personnel are and how they can be contacted.

f. Report immediately all security incidents, compromise, or suspected compromise, and potential threats and vulnerabilities involving computing resources to designated computer security personnel including my supervisor, the Help Desk, or the Information System Security Officer. This includes the use of my User ID and password or PIV by someone else.

g. Use the data accessed from ED computing system only for its intended purpose.

h. I understand the availability and use of the Help Desk if I have questions about the use of the assigned hardware and software.

i. In the event that I have remote access to the system, I will ensure that all government materials are adequately protected while the information is accessible off-site.

On the Subject of Access Security, I will:

a. Inform FMS security when access to an FMS computing resource is no longer required, such as when I complete a project, transfer to another position, or terminate employment.

b. Access only systems, networks, data, and software for which I have been authorized.

c. Use ED computing resources and social media only for official government business.

d. Exercise due diligence to prevent physical damage to and theft of any Departmental computing resource.

e. Notify management before relocating computing resources.

On the Subject of Unacceptable Use, I understand that the following activities are prohibited uses of FMS computing resources:

a. Exporting software, technical information, encryption software, or technology

b. Revealing password or account details to others or allowing others to use the account without adhering to procedures

c. Transmitting sensitive information via the Internet unless protected from viewing by unauthorized personnel

d. Accessing illegal or unlawful material, using government equipment for private or unofficial business, promoting slanderous material based upon race, creed, or national origin, or downloading and viewing pornography

e. Using government resources to actively engage in procuring or distributing material that is in violation of sexual harassment or hostile workplace laws

f. Introducing malicious programs into the network or server

g. Accessing the network to gain or attempt to gain unauthorized access to data, system applications, or other information or control that is not expressly authorized unless within the scope of duties. This includes disruption or attempted disruption of the network, user access, or system controls.

h. Port scanning or security scanning is expressly prohibited without prior notification and approval of the Information System Security Officer

i. Executing any form of network monitoring that will intercept data that may affect the performance of the network unless authorized as part of the normal duties

j. Circumventing user authentication of any host, network, or account

k. When using e-mail, never

   - Put in a mail message anything you would not put in a postcard
   - Create or forward chain letters via electronic mail
   - Send unsolicited e-mail, including junk mail or other advertising material, to individuals who did not specifically request or require that information
   - Attempt to forge or use an e-mail address other than your own.

On the Subject of Termination

a. I will return all materials, which have or may have come into my possession or for which I am responsible because of such access, upon demand by an authorized representative of the United States Government or upon the conclusion of my employment or other relationship with the ED.

b. I understand that violation of these Rules of Behavior may result in disciplinary action ranging from a warning to involuntary termination of employment.

On the Subject of Continuation of Obligations

The obligations of this agreement shall remain in effect and bind the heirs, successors, assignees, and legal representatives of each party to this Agreement for a period of five (5) years after the expiration or termination of this Agreement.

On the Subject of Remediation

I understand that the United States Government may seek any remedy available to it to enforce this agreement, including, but not limited to, application for a court order prohibiting disclosure of information in breach of this agreement.

On the Subject of Enforcement and Sanctions:

At the immediate discretion of the Information System Security Officer, appropriate disciplinary action can be taken as one of the following:

- Verbal or electronic warning and demand to stop activity or provide satisfactory explanation.
- Monitoring of the activity for possible criminal or civil activity without notification.
- Termination of access after stating the violating activities.
- Immediate transfer of the violation to senior management or federal authorities for further action. Such transfer may be with or without notification.
- Sanctions may be imposed for whatever duration the Information System Security Officer determines appropriate, provided management concurs.

Should the affected party wish to challenge the sanction, he/she must provide such rebuttal in writing to the Information System Security Officer, through their supervisor, and include the details and explanation of the incursion. Final decision of access will ultimately rest with the Chief Financial Officer (CFO), Federal Student Aid.

Acknowledgement and Signature:

I understand that all information to which I may obtain access by signing this agreement is now and will forever remain the property of the United States Government. Further, I do not now, nor will I ever, possess any right, interest, title, or claim whatsoever to such information.

I have read this agreement carefully and my questions, if any, have been answered to my satisfaction by the Information System Security Officer.

Acknowledged and Accepted By:

Signature of Person Requesting Access and Date

Acknowledgement of External User Responsibilities

External User Security Access Agreement

Attachment A.2 – External Rules of Behavior for the Federal Student Aid Financial Management System

I hereby accept the obligations contained in this agreement in consideration of my being granted access to the Department of Education (ED), Federal Student Aid (Federal Student Aid), Financial Management System (FMS), and/or its component applications. I acknowledge and accept that access is a conditional privilege granted to me for only as long as I have a bona fide need. I will adhere to the governing United States Laws and the Department of Education policies, rules, and guidelines. I accept the Department of Education's right to monitor application use for security purposes and that I have no expectation of privacy when using Department of Education computing resources. I understand that failure to comply with these rules can result in the suspension or termination of my access to FMS.

Accordingly, I hereby certify that:

On the Subject of Information Assurance, I will:

a. Know the sensitivity of the information processed on FMS computing resources available to me (e.g., financial sensitive, privacy act sensitive, proprietary information).

b. Ensure that system media and system output are marked according to their sensitivity.

c. Take reasonable care to protect FMS information, whether electronic or in hardcopy, limiting access to a need-to-know basis, and prevent disclosure to unauthorized personnel.

d. Take necessary steps to avoid the introduction of malicious code into any computing resource. I am aware of the anti-virus software available to me and am familiar with its use. I agree to keep such software installed and configured for automatic protection, and to keep virus signature files up to date on computers used to access FMS.

e. Know who my FMS computer security contacts are and how they can be contacted.

f. Report immediately all security incidents, compromise, or suspected compromise, and potential threats and vulnerabilities involving computing resources to designated FMS computer security. This includes the use of my User ID and password or PIV by someone else.

g. Use the data accessed from ED computing systems only for its intended purpose.

h. I understand the availability and use of the Help Desk if I have questions about the use of the FMS system.

In the event that I have remote access to the system, I will ensure that all government materials are adequately protected while the information is accessible off-site.

On the Subject of Access Security, I will:

a. Inform FMS security when access to an FMS computing resource is no longer required.

b. Access only systems, networks, data, and software for which I have been authorized.

c. Use ED computing resources and social media only for official government business.

On the Subject of Unacceptable Use, I understand that the following activities are prohibited uses of FMS computing resources:

a. Exporting software, technical information, encryption software, or technology

b. Revealing password or account details to others or allowing others to use the account without adhering to procedures

c. Transmitting sensitive information via the Internet unless protected from viewing by unauthorized personnel

d. Accessing illegal or unlawful material, using government equipment for private or unofficial business, promoting slanderous material based upon race, creed, or national origin, or downloading and viewing pornography

e. Using government resources to actively engage in procuring or distributing material that is in violation of sexual harassment or hostile workplace laws

f. Introducing malicious programs into the network or server

g. Accessing the network to gain or attempt to gain unauthorized access to data, system applications, or other information or control that is not expressly authorized unless within the scope of duties. This includes disruption or attempted disruption of the network, user access, or system controls.

h. Port scanning or security scanning is expressly prohibited without prior notification and approval of the Information System Security Officer

i. Executing any form of network monitoring that will intercept data that may affect the performance of the network unless authorized as part of the normal duties

j. Circumventing user authentication of any host, network, or account

k. When using e-mail, never

   - Put in a mail message anything you would not put in a postcard
   - Create or forward chain letters via electronic mail
   - Send unsolicited e-mail, including junk mail or other advertising material, to individuals who did not specifically request or require that information
   - Attempt to forge or use an e-mail address other than your own.

On the Subject of Continuation of Obligations:

The obligations of this agreement shall remain in effect and bind the heirs, successors, assignees, and legal representatives of each party to this Agreement for a period of five (5) years after the expiration or termination of this Agreement.

On the Subject of Remediation:

I understand that the United States Government may seek any remedy available to it to enforce this agreement, including, but not limited to, application for a court order prohibiting disclosure of information in breach of this agreement.

On the Subject of Enforcement and Sanctions:

At the immediate discretion of the Information System Security Officer, appropriate disciplinary action can be taken as one of the following:

- Verbal or electronic warning and demand to stop activity or provide satisfactory explanation.
- Monitoring of the activity for possible criminal or civil activity without notification.
- Termination of access after stating the violating activities.
- Immediate transfer of the violation to senior management or federal authorities for further action. Such transfer may be with or without notification.
- Sanctions may be imposed for whatever duration the Information System Security Officer determines appropriate, provided management concurs.

Should the affected party wish to challenge the sanction, he/she must provide such rebuttal in writing to the Information System Security Officer, through their supervisor, and include the details and explanation of the incursion. Final decision of access will ultimately rest with the Chief Financial Officer (CFO), Federal Student Aid.

Acknowledgement and Signature:

I understand that all information to which I may obtain access by signing this agreement is now and will forever remain the property of the United States Government. Further, I do not now, nor will I ever, possess any right, interest, title, or claim whatsoever to such information.

I have read this agreement carefully and the Information System Security Officer has answered my questions, if any, to my satisfaction.

Acknowledged and Accepted By:

Signature of Person Requesting Access and Date

Attachment B - Privacy Act Statement

FMS is a system that stores personal information in the form of a name, Social Security or other identifying number, or symbol assigned to an individual that is covered by the Privacy *Act of 1974*. I understand that in the normal course of my duties I may have access to such personal information stored in FMS.

I understand that this information is to be closely guarded and is not to be disclosed except under certain specific conditions clearly defined in the Privacy Act, as outlined below.

PRIVACY ACT CONDITIONS OF DISCLOSURE

No agency shall disclose any record that is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be:

1. To those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;
2. Required under section 552 of this title;
3. For a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section;
4. To the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of Title 13;
5. To a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;
6. To the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has such value;
7. To another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;
8. To a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;
9. To either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;
10. To the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the Government Accountability Office;
11. Pursuant to the order of a court of competent jurisdiction; or
12. To a consumer reporting agency in accordance with section 3711(e) of Title 31.

I also understand there are both civil and criminal penalties which may result from unapproved disclosure, and that these penalties include:

1. Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information, the disclosure of which is prohibited by this section or by rules or regulations established there under, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

2. Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e) (4) of this section shall be guilty of a misdemeanor and fined not more than $5,000.
3. Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000.

I accept responsibility for my use of the U.S. Department of Education, Federal Student Aid, Financial Management System (FMS). I will ensure that system usage is for official government business only. By signing this document, I confirm my awareness of this responsibility regarding the protection of Privacy Act data. I understand Education and Federal Student Aid personnel will monitor the system for security violations on a regular basis.

Acknowledged and Accepted By:

Signature of Person Requesting Access and Date

Attachment C - Table of FMS Responsibilities

This table of FMS Responsibilities does not need to be submitted by **External Users** and **Federal Loan Servicers (TIVAS/NFPs)**.

Note: Revised Trust Level designations from 1C, 5C, 6C to new OPM Tier levels (T1, T2, T4): 1C = T1, 5C = T2, 6C = T4.

Internal Users: Please specify the FMS responsibilities you need by checking the corresponding box in the Production column.

System Name: Archiving

Responsibility Name	Production[1]	FMS Security Initials
FSA Archive FFEL GA AP Inquiry – T1	□	
FSA Archive Financial Partner Manager Inquiry – T1	□	
FSA Archive FP Annual Inquiry – T1	□	
FSA Archive GA Inquiry – T1	□	
FSA Archive GL Inquiry – T2	□	
FSA Archive LARS ED Inquiry – T1	□	
FSA Archive Lender Payable Inquiry – T1	□	
FSA Archive Lender Receivable Inquiry – T2	□	

System Name: Campus Based

Responsibility Name	Production[1]	FMS Security Initials
FSA CBS Manager – T2	□	

System Name: COD

Responsibility Name	Production[1]	FMS Security Initials
FSA CODX Manager – T2	□	

System Name: Cross Program

Responsibility Name	Production[1]	FMS Security Initials
Alert Manager – T4	□	
Application Developer – T4	□	
FSA Allocation User – T1	□	
FSA CFO General Ledger Accounting User – T4	□	
FSA CFO General Ledger Operations User – T4	□	
FSA CFO General Ledger Ops Setup User – T4	□	
FSA CFO Open and Close Period – T2	□	
FSA FMS Operations User – T2	□	
FSA GL Inquiry – T2	□	

Responsibility Name	Production[1]	FMS Security Initials
FSA GL User – T2	□	
FSA IPPP Manager – T1	□	
FSA User/Lender System Administrator – T4	□	
FSA XVCI Manager – T2	□	
Oracle Diagnostics Tool – T2	□	
System Administrator – T4	□	
Workflow Administrator – T4	□	
FSA DLC Funds Disbursement Process Manager – T4	□	
FSA DLC Payables Operations User – T4	□	
FSA DLC Payables Ops Setup User – T4	□	
FSA DLC Purchase Invoices Manager – T2	□	
FSA DLC Payment Manager – T4	□	
FSA DLC Federal Administrator – T2	□	

System Name: APEX

Responsibility Name	Production[1]	FMS Security Initials
FSA APEX ACS DLS – T2	□	
FSA APEX APD – T2	□	
FSA APEX AD – T2	□	
FSA APEX CFO – T2	□	
FSA APEX FFELGA – T1	□	
FSA APEX FFELLEN – T1	□	
FSA APEX FRD – T1	□	
FSA APEX Operations – T2	□	

System Name: FFEL GA

Responsibility Name	Production[1]	FMS Security Initials
FSA FFEL GA AP Inquiry – T1	□	
FSA FFEL GA Federal Administrator – T2	□	
FSA FFEL GA Federal Administrator Operations User – T4	□	
FSA FFEL GA Funds Disbursement Process Manager – T4	□	
FSA FFEL GA GL User – T2	□	
FSA FFEL GA Payables – T2	□	

Responsibility Name	Production[1]	FMS Security Initials
FSA FFEL GA Payables Accounting User – T4	□	
FSA FFEL GA Payables Operations User – T4	□	
FSA FFEL GA Payables Ops Setup User – T4	□	
FSA FFEL GA Payments Manager – T4	□	
FSA Financial Partner Annual – T2	□	
FSA Financial Partner Manager – T2	□	
FSA Financial Partner Manager Inquiry – T1	□	
FSA GA Inquiry – T1	□	
FSA GA Payment Inquiry – T1	□	
FSA GA Manager – T1	□	
FSA GA User – T1	□	
FSA FP Annual Inquiry – T1	□	

System Name: FFEL Lender (LAP/LARS)

Responsibility Name	Production[1]	FMS Security Initials
FSA LAP ED Manager – T2	□	
FSA LARS ED Inquiry – T1	□	
FSA LARS ED Manager – T2	□	
FSA LARS ED User – T2	□	
FSA LARS Lender/Servicer – T1	□	
FSA Lender Fed Admin Ops Setup User – T4	□	
FSA Lender Federal Administrator – T4	□	
FSA Lender Manager – T1	□	
FSA Lender Payable Inquiry – T1	□	
FSA Lender Payable Manager – T4	□	
FSA Lender Funds Disbursement Process Manager – T4	□	
FSA Lender Payable Ops Setup User – T4	□	
FSA Lender Payables Operations User – T4	□	
FSA Lender Payment Manager – T4	□	
FSA Lender Receivable Inquiry – T2	□	
FSA Lender Receivable Manager – T2	□	

Responsibility Name	Production[1]	FMS Security Initials
FSA Lender Receivable Ops Setup User – T2	□	

System Name: Desktop Integration (GLDI)

Responsibility Name	Production[1]	FMS Security Initials
FSA CFO Desktop Integration – T2	□	
FSA FMS Ops Desktop Integration – T2	□	
FSA APEX Servicers – T1	□	
FSA APEX WIP Transfers – T2	□	
FSA SRVC Dashboard User – T1	□	

System Name: Loan Purchase Program

Responsibility Name	Production[1]	FMS Security Initials
FSA Lender Purchase Invoices Manager – T2	□	

System Name: Title IV Additional Servicers (TIVAS)

Responsibility Name	Production[1]	FMS Security Initials
FSA LNC Payables Supplier Inquiry – T4	□	
FSA SRVC Federal Administrator – T2	□	
FSA SRVC Federal Administrator Operations User – T4	□	
FSA SRVC Funds Disbursement Process Manager – T4	□	
FSA SRVC Invoice Manager – T4	□	
FSA SRVC Invoice User – T2	□	
FSA SRVC Payables Inquiry – T1	□	
FSA SRVC Payables Operations User – T4	□	
FSA SRVC Payment Manager – T4	□	

System Name: TROR

Responsibility Name	Production[1]	FMS Security Initials
FSA SRVC TROR Reporting – T1	□	

System Name: FSA FMS Security Team

Responsibility Name	Production[1]	FMS Security Initials
FSA FMS Security Team User – T4	□	
FSA FMS Security Team User: Read Only[2] – T4	□	

System Name: Other Application Instances[3]

Responsibility Name	Test Env – T2	FMS Security Initials
FMS TST	□	
FMS UAT	□	
FMS PAY	□	
FMS NFP	□	
FMS STG	□	

Note: FMS developers should NOT be provided any of the above responsibilities unless an explicit email is sent to FMSG Security team providing justification, instance name, start and end date for access.

System Name: Other Responsibilities

Responsibility Name	Test Env	FMS Security Initials
Development Environment – T2	□	
Functional Administrator – T4	□	
SLA Super User – T4	□	
Trading Community Manager – T4	□	
Application Diagnostics – T2	□	
FSA LC Federal Administrator Operations User – T4	□	
US Super HRMS Manager – T4	□	

Footnotes to Table of Responsibilities:

[1] The Production instance allows users to enter financial data, run reports and queries.

[2] This responsibility is granted to provide read-only access to auditors to review completed security reports and artifacts.

[3] For FMS Operations and/or Development Team Only. FMS users requesting access to other application instances do not need to specify the Oracle responsibilities. Responsibilities are assigned as necessary.

FMS Security Awareness Training Instructions for FMS Access

User General Security Awareness Training

If you are an internal user (i.e., a Department of Education employee or contractor or Federal Loan Servicer); an external user (i.e., an employee or agent of a Guaranty Agency, Lender, Lenders/Servicer, or State LEAP/SLEAP Agency; or you are submitting a request to become an FMS user.

1. Please refer to the FMS General Security Awareness Training slide presentation (PowerPoint or PDF) version located on the FSA Knowledge Center.
2. Read and review all Security Awareness Training slides
3. Sign the training acknowledgement form on the last page (**Page 29**) of the training presentation to confirm that you have completed the training and email it along with your FMS User Access Form to the FMS Operations Help Desk at FMS.OPERATIONS@ed.gov.

Specialized User Security Awareness Training

If you are a system administrator, database administrator, or Information System Security Officer, you are required to complete specialized security awareness training. The FSA Chief Information Security Officer (CISO) or FMS ISSO will notify you when specialized training must be completed.