

For: FSA State Offices

**Deployment of the Lease and Reimbursable Agreement Tracking (LRAT) Web Application –
Lease Segment Only**

Approved by: Acting Associate Administrator for Operations and Management



1 Overview

A Background

LRAT will:

- automate 2 existing processes as follows:
 - communication of lease payment information
 - Reimbursable Agreement approvals
- **not** change any current processes, **only** automate existing processes.

AD-1143 (Exhibit 1) **must** be completed for **all** users needing access to LRAT. The State **Office** will complete AD-1143 and **must** attach a spreadsheet with the list of all users needing access.

AD-1143 and spreadsheet **must** be approved by the Security Liaison Representative (SLR). SLR will then send AD-1143 and spreadsheet to Information Security Office (ISO) at **security@kcc.usda.gov** and **either** of the following:

- Laura Quirk by e-mail to **laura.quirk@kcc.usda.gov**
- Kelly Holdman by e-mail to **kelly.holdman@kcc.usda.gov**.

Disposal Date	Distribution
November 1, 2010	State Offices

Notice FI-3001

1 Overview (Continued)

B Purpose

This notice informs FSA State Offices that LRAT will be available for use beginning October 12, 2010. LRAT will be used by FSA, NRCS, and RD. **At this time, users may begin using the Lease segment only. The Reimbursable Agreement segment will be available later.**

Teleconference training sessions for all State Office users will be held on the following dates/times:

Tuesday, October 12:	9 to 11 c.t. at 800-867-6144, pass code #: 7973
	1 to 3 c.t. at 800-867-6144, pass code #: 9263
Wednesday, October 13:	9 to 11 c.t. at 800-867-6144, pass code #: 4074
	1 to 3 c.t. at 800-867-6144, pass code #: 1180
Thursday, October 14:	9 to 11 c.t. at 800-867-6144, pass code #: 9402
	1 to 3 c.t. at 800-867-6144, pass code #: 1747
Friday, October 15:	9 to 11 c.t. at 800-867-6144, pass code #: 3054
	1 to 3 c.t. at 800-867-6144, pass code #: 1279.

Note: Because of limited lines, users **must** select their **top 3** choices. Times will be allotted on a space-available basis.

FSA shall coordinate with the State's respective RD and NRCS offices to ensure that all users are in attendance on the same date/time. All State Office employees who work with leases and/or the lease payment (accounting staff) should plan to attend. The training session will use Microsoft Office Live Meeting for screen sharing. Ensure that users have configured Microsoft Office Live Meeting **before** the training session. A meeting request will be sent out before each training time.

Notice FI-3001

2 Additional Information

A State Office Action

SED's and administrative officers shall determine who in their State will be assigned the responsibility for inputting and monitoring LRAT data.

Employees assigned LRAT responsibilities shall complete AD-1143 (Exhibit 1).

Administrative or executive officers shall:

- complete the spreadsheet (see Exhibit 2 for example and instructions) and attach the completed spreadsheet to completed AD-1143

Note: The spreadsheet **must** include the user's name, eAuthentication ID, role needed for LRAT, e-mail address, and the preferred date chosen to attend a training session (see subparagraph B for dates and times). A sample spreadsheet and instructions on completing the spreadsheet is provided in Exhibit 2.

- provide 3 choices of training dates and times
- ensure that **all** current leases are entered into LRAT by **November 19, 2010**.

Note: States must have **all** current leases entered into LRAT by November 19, 2010. When loading an existing lease (and **not** making any changes to the lease payment information already on file), notate this in the "Comments" field so accounting does **not** treat this as a change to their current lease payment.

SLR **must** approve AD-1143 and then send AD-1143 and spreadsheet to ISO at security@kcc.usda.gov and **either** of the following:

- Laura Quirk by e-mail to laura.quirk@kcc.usda.gov
- Kelly Holdman by e-mail to kelly.holdman@kcc.usda.gov

B Future Enhancement

Currently, LRAT does **not** allow multiple leases to be entered within 1 Organization Code. It is understood, that in some cases, there may be more than 1 lease within an Organization Code. An enhancement to LRAT that will allow this functionality is forthcoming.

C Contacts

State Offices with questions about this notice should contact either of the following:

- Laura Quirk by either of the following:
 - e-mail to laura.quirk@kcc.usda.gov
 - telephone at 816-926-6973
- Kelly Holdman by either of the following:
 - e-mail to kelly.holdman@kcc.usda.gov
 - telephone at 816-926-6246.

Example of AD-1143

The following is an example AD-1143 that is available electronically at <http://165.221.16.90/dam/ffasforms/forms.html> that **must** be completed and e-mailed according to subparagraph 2 A.

AD-1143 U. S. DEPARTMENT OF AGRICULTURE <p style="text-align: center;">CORPORATE SYSTEMS ACCESS REQUEST FORM</p>		1. SYSTEM/APPLICATION NAME Check one or more and complete the applicable section(s) <input type="checkbox"/> Automated Cash Reconciliation Worksheet System <input type="checkbox"/> Corporate Property Automated Information System <input type="checkbox"/> Financial Data Warehouse <input type="checkbox"/> Foundation Financial Information System <input type="checkbox"/> GovTrip.com <input type="checkbox"/> Integrated Acquisition System <input type="checkbox"/> Management Initiatives Tracking System Other – LRAT Application (new on 4/15) 2. FFIS APPLICATION NUMBER(S) (If Applicable)
USER INFORMATION (See Privacy Act Statement)		
3. USER'S SSN (See Instructions) <i>See below</i>	4. USER'S NAME (Last, first, middle initial) <i>See below</i>	5. USER'S TITLE OR CONTRACTOR* <i>See Below</i>
6. USER'S MAILING ADDRESS WITH ZIP CODE		7. AGENCY
		8. OFFICE
9. USER'S E-MAIL ADDRESS		10. USER'S PHONE NUMBER () - -
		11. MANAGER'S PHONE NUMBER () - -
<i>*See special instructions</i>		
ACTION REQUESTED		
NAME CHANGE	12. OLD NAME (Last, first, middle initial)	13. NEW NAME (Last, first, middle initial)
ACCESS	14. (Check all that apply): <input checked="" type="checkbox"/> Add User <input type="checkbox"/> Delete User <input type="checkbox"/> Modify User Profile <input type="checkbox"/> Agency Cross-Service Access	
		15. USER ID(S) (Include NFC, FFIS, E-Auth User ID, if applicable)
AUTOMATED CASH RECONCILIATION WORKSHEET SYSTEM (ACRWS) ACCESS		
16. USER'S ACRWS 52 Roles/Access (Check all that apply)		17. USER'S ACRWS 53 Roles/Access (Check all that apply)
<input type="checkbox"/> Public/Read-Only		<input type="checkbox"/> Public/Read-Only
<input type="checkbox"/> Auditor		<input type="checkbox"/> Auditor
<input type="checkbox"/> Approver		<input type="checkbox"/> Approver
<input type="checkbox"/> Import Manager		<input type="checkbox"/> Import Manager
<input type="checkbox"/> ACRWS 52BRIO/Hyperion		<input type="checkbox"/> ACRWS 53 BRIO/Hyperion
CORPORATE PROPERTY AUTOMATED INFORMATION SYSTEM (CPAIS) ACCESS		
19. USER'S CPAIS ROLE		
<input type="checkbox"/> UMA Manager Real		
<input type="checkbox"/> UMA Manager Personal		
<input type="checkbox"/> UMA User Real (Specify add and/or modify role(s))		
<input type="checkbox"/> UMA User Personal (Specify add and/or modify role(s))		
		21. SIGNATURE OF UMA Manager for all Users. (Sign and date)

Example of AD-1143 (Continued)

GOVTRIP.COM		
33. GovTrip.com Role <input type="checkbox"/> Traveler <input type="checkbox"/> Travel Arranger <input type="checkbox"/> Approver <input type="checkbox"/> Agency FATA	34. GovTrip TRAINING RECEIVED? (If yes, enter date completed) <input type="checkbox"/> Yes <input type="checkbox"/> No Date: _____	35. GovTrip Agency APPROVER (Sign and date when action has been completed) Approver: _____ Date: _____
SPECIAL INSTRUCTIONS		
36. SPECIAL INSTRUCTIONS Grant access to the following users to the LRAT system: (see attached spreadsheet) Contact Laura Quirk (FAO/FRSG) with any questions (816) 926-6973.		
USER ACKNOWLEDGEMENT		
<i>I have read the automated information systems security rules and understand the security requirements of the automated information systems and/or applications described on this form. I understand that any violation of these rules may result in disciplinary action, removal from the agency/USDA, and/or criminal prosecution.</i>		
37. USER'S SIGNATURE	38. DATE	
BACKGROUND INVESTIGATION		
39. <input type="checkbox"/> Initiated <input type="checkbox"/> Completed	40. DATE (Initiated or completed)	41. PRINT MANAGER'S NAME
AUTHORIZATION		
User's Manager – <i>I certify this user has received security instructions for the systems and/or applications indicated, and I approve his/her access to these systems and/or applications and the associated user profiles.</i>	42. MANAGER'S SIGNATURE	43. DATE
ACTION TAKEN		
44. SECURITY ADMINISTRATOR	45. DATE	
46. SECURITY ADMINISTRATOR NOTES		
PRIVACY ACT NOTICE		
In compliance with the Privacy Act of 1974, the following information is provided: Solicitation of your Social Security Number is authorized by Executive Order 9397 of November 22, 1943 and 5 U.S.C. 301. The primary purpose of requesting the Social Security Number (SSN) is to properly identify the employee. Many employees have similar names and the furnishing of the SSN will enable USDA to identify authorized users of USDA's computer systems. The information will be used by offices and employees who have a need for the information in the performance of their official duties. The information will not be disclosed outside USDA. Disclosure of your SSN and other information is mandatory. Failure to provide the requested information will result in the denial of the requested computer access authority.		

Example of AD-1143 (Continued)

**CORPORATE SYSTEMS ACCESS REQUEST FORM
SECURITY RULES**

**VIOLATION OF THESE RULES
MAY RESULT IN
DISCIPLINARY ACTION**

1. **DO NOT ACCESS** research, or change any account, file, record or application not required to perform your official duties. You are forbidden to Access your own account, that of a spouse, relative, friend, neighbor, or any account in which you have a personal or financial interest. If you are assigned to work on one of these accounts contact your supervisor. Behave in an ethical, technically proficient, informed, and trustworthy manner.
2. If you are asked by another person to access an account or other sensitive or private information, **VERIFY** that the requested access is authorized. You will be held responsible if the access is not authorized. As a general rule, you should not use a computer or terminal in behalf of another person.
3. **DIFFERENTIATE TASKS AND FUNCTIONS** to ensure that no one person has sole access to or control over important resources.
4. **PROTECT YOUR PASSWORD** from disclosure. You are responsible for any computer activity associated with your password. **DO NOT SHARE** your password with others or reveal it to anyone, regardless of his/her position in or outside the USDA. **DO NOT POST** your password in your work area. **DO NOT USE** another person's password. USER IDs must be treated with the same care as your password. Everything done with your user ID or password will be recorded as being done by you. Use unique passwords for each system and application you access. **NEVER** give your password out over the telephone. Be alert to others who may try to obtain your password. Social engineering is a practice used when hackers pose as system administrators. A hacker may randomly call a user and say that something is wrong on the system to get arbitrary access to your system. They may tell you that they need your password in order to issue an new one. Always remember that system administrators **DO NOT** need your password in order to issue you a new password. Do not re-cycle passwords by using just a few over and over again, or make minor changes to passwords by adding a number to the base password.
5. **PASSWORD DISTRIBUTION AND REFRESHMENT** must be done securely.
6. **CHANGE YOUR PASSWORD** if you think someone else knows your password. Immediately notify your supervisor or your Functional Security Coordinator or Security Representative. Passwords for FFIS, IAS and the FFIS Data Warehouse will be changed every 30 days as prompted by the system.
7. **DO NOT PROGRAM** your login or password into automatic script routines or programs.
8. **LOG OFF/SIGN OFF** if you go to lunch, or break, or anytime you leave your computer or terminal.
9. **PROTECT** your system against viruses and similar malicious programs. Make certain that updates to desktop virus protection schemes are performed in a timely manner in accordance with vendor or system administration instructions.
10. **FOR ADDITIONAL** security, use personnel firewall applications and do not allow applications not known to you through the firewall.
11. **PARTICIPATE** in organization-wide security training as required and read and adhere to security information pertaining to system hardware and software.
12. **RETRIEVE ALL** hard copy printouts in a timely manner. If you cannot determine the originator or receiver of a printout, dispose of it in a burn waste container or shredder. Store all hardcopy reports and storage media containing Confidential information in a locked room or cabinet.
13. **IDENTIFY ALL** sensitive applications or data that you will be placing on a system, and any equipment processing sensitive information to your Supervisor, so that appropriate security measures can be implemented.
14. **DO NOT USE USDA COMPUTERS** or software for personal use.
15. **DO NOT USE PERSONAL EQUIPMENT** or software for official business without your supervisor's written approval.
16. **DO NOT INSTALL OR USE UNAUTHORIZED SOFTWARE** on USDA equipment. Do not use freeware, shareware or public domain software on USDA computers without your supervisor's permission and without scanning it for viruses. Comply with local office policy on the use of antiviral Software.
17. **OBSERVE ALL SOFTWARE LICENSE AGREEMENTS.** Do not violate Federal copyright laws.
18. **DO NOT MOVE EQUIPMENT** or exchange system components without authorization by the appropriate functions and manager's approval.
19. **PROTECT USDA COMPUTER EQUIPMENT** from hazards such as liquids, food, smoke, staples, paper clips, etc.
20. **PROTECT MAGNETIC MEDIA** from exposure to electrical currents, extreme temperatures, bending, fluids, smoke, etc. Ensure the magnetic media is secured based on the sensitivity of the information contained, and practice proper labeling procedures. **BACK UP** critical programs and data, and store in a safe place. Back ups should be performed as often as program and data sensitivity require. Erase sensitive data on storage media before reusing or disposing of the media.
21. **DO NOT DISCLOSE THE TELEPHONE NUMBER(S)** or procedure(s) which permit system access from a remote location.
22. **DO NOT SEND OR STORE** Government information on a commercial E-mail site.

Example of AD-1143 (Continued)

23. **DO NOT USE** sensitive information for equipment or program test purposes. Vendors should be escorted and monitored while performing maintenance duties.
24. **DO NOT DISCLOSE** or discuss any USDA personnel or vendor related information with unauthorized individuals. The Privacy Act of 1974, 5 USC 552a, prohibits such disclosure. A person making a willful unauthorized disclosure covered by this act may be charged with a Misdemeanor and subject to a fine of up to \$5,000.
25. **PROMPTLY REPORT** all security incidents to your supervisor and in accordance with you agency policy on reporting incidents. For example: unauthorized disclosure of information, computer viruses, theft of equipment, software or information, and deliberate alteration or destruction of data or equipment. NEVER assume that someone else has already reported an incident. The risk of an incident going unreported far outweighs the possibility that an incident is reported more than once.
26. **SEEK** assistance and challenge unescorted strangers in areas where the system is being used.
27. **Complete this form when Duties Change, when a separation from the agency occurs, and to report name changes or request profile changes.**

Example of AD-1143 (Continued)

AD-1143 FORM INSTRUCTIONS

BLOCK NO.

- 1 Check one or more systems. Fill in information for access in Special Instructions for FedTraveler.com
- 2 Enter the agency FFIS application number, i.e., FF34 for APHIS, or FF11 for Forest Service.

USER INFORMATION

- 3 Enter social security number. **The Social Security Number is only required for adding a user to a FFIS application for the first time.**
- 4 Enter name.
- 5 Enter job title or Contractor, if not a USDA employee.
- 6 Enter address where the user can be contacted by mail.
- 7 Enter agency name and agency code/number.
- 8 Enter office, i.e., Financial Management, Procurement Operations.
- 9 Enter e-mail address.
- 10 Enter telephone number.
- 11 Enter manager's telephone number.

ACTION REQUESTED

- 12 Enter "old" name, when requesting a name change.
- 13 Enter "new" name, when requesting a name change.
- 14 Check the appropriate action to be taken. If requesting a modification to your profile, specify in Block 29 the previous profile or job assignment and the new profile or job assignment. If the user performs services for additional USDA agencies, e.g., "cross-servicing, specify the additional agencies(s) and required roles.
- 15 Enter NFC, FFIS, E-Auth, userid AND if Block 14 is "delete user" or "modify user", include existing userid. If action requested in Block 14 is "add user", the Agency Security Administrator will assign the userid.

AUTOMATED CASH RECONCILIATION WORKSHEET SYSTEM ACCESS

- 16 Check appropriate Role(s)/Access for ACRWS52.
- 17 Check appropriate Role(s)/Access for ACRWS53.
- 18 Reserved.

CORPORATE PROPERTY AUTOMATED INFORMATION SYSTEM ACCESS

- 19 Check the appropriate action to be taken. If requesting a modification of your user CPAIS role, specify all role(s) deleted and/or added.
- 21 If requesting UMA manager, this must be approved at a department level.

FINANCIAL DATA WAREHOUSE SYSTEM ACCESS

- 25 Check the appropriate box to grant level of access. Security group is for Security Administrators or individuals who need access per job duties.
- 26 Check the appropriate box to grant level of report access. Check only one box.
- 27 Reserved

INTEGRATED ACQUISITION SYSTEM ACCESS

- 28 Check all appropriate roles.
- 29 Enter requisition approval amount, if user is a Funds Approver.
- 30 Enter warrant amount, if user is a Contracting Officer. Verify the amount to be entered here with your supervisor if you are warranted for a higher amount than your supervisor has authorized you for.
- 31 Does this user purchase for other agencies? If yes, enter the agencies here, e.g., Rural Development, Food and Nutrition Service.

MANAGEMENT INITIATIVES TRACKING SYSTEM ACCESS

- 3 Not required.
- 15 Enter eAuthorization User ID.
- 32 Check required role.
See USDA Corporate Website or the MITS Security Features User's Guide for definitions of each role. Only one role per MITS module should be entered on an individual AD-1143; complete separate AD-1143 documents for each additional role.

For PMA: Enter appropriate initiative(s).

HC – Human Capital	CS – Competitive Sourcing
RP – Real Property	CP – Credit Programs
FM – Financial Management	eGov – E-governement
FBCI – Faith Based	R&D – Research and Development
IPIA – Improper Payments	BPI – Budget and Performance Integration

For PART: Enter appropriate agency(s).
Enter appropriate program(s) or "ALL", default is "ALL".
Enter appropriate agency(s).
Enter mission area(s) (required for mission area coordinators only).
Enter PART program(s) – optional (enter if user should have edit access for limited PARTs)

For BUDGET: Enter appropriate agency(s).
For AUDIT TRACKING: Enter appropriate agency(s).
Enter mission area(s) (required for mission area coordinators only).
Executive Officer and OIG Auditors role – Available to OCFO employees and OIG auditors only.
Audit Follow-up Coordinator role – Available to OCFO employees only.

For Sustainability Scorecard: Enter appropriate initiative(s).
Enter appropriate agency(s).

Example of AD-1143 (Continued)

GOVTRIP.COM

33 Please check the role the user will be in GovTrip.

Traveler – Only view their travel data and submit their own voucher for approval.

Travel Arranger – Able to prepare travel plans for designated personnel in their agency's organization and able to see the information of others.

Approver—Able to approve travel vouchers for designated personnel in their agency's organization.

Agency FATA – Able to set up configuration for their designated agency. This should be only a few personnel.

34 Indicate if training has been received.

35 Signature of the requester's supervisor or designated travel manager in the agency.

SPECIAL INSTRUCTIONS

36 Include any additional information needed to complete access. Specify the security profile or job assignment, or any comments or special instructions.

For CPAIS: Provide organization number(s) for which access is being requested. If access is needed for all organizations within an agency, list agency name and "ALL".

For FFIS: 1) Provide previous profile or job assignment and the new profile or job assignment, if modification to existing model; and
2) Provide the names of the additional agencies(s) and required roles, if the user performs services for additional USDA agencies, e.g., "cross-servicing".

USER ACKNOWLEDGEMENT

A USER SIGNATURE IS REQUIRED IN THE USER ACKNOWLEDGMENT BLOCK WHEN THEY ARE ADDED TO A SYSTEM.

37 User's signature.

38 Date user signed form.

BACKGROUND INVESTIGATION

THIS FIELD MUST BE FILLED OUT. SECURITY ADMINISTRATORS WILL NOT COMPLETE THE REQUEST UNLESS THIS BOX IS FILLED OUT ACCORDING TO THE INSTRUCTIONS BELOW

39 Check whether background investigation has been initiated or completed. This applies to both USDA employees and contractors.

40 Date background investigation was initiated or completed.

41 Name of user's immediate manager

AUTHORIZATION

42 Manager's signature.

43 Date manager approved the requested action.

ACTION TAKEN

44 Security Administrator's signature.

45 Date Security Administrator completed user's request.

46 Security Administrator can use this space to include any notes related to the completion of the request. The agency's Security Administrator will retain each completed form for audit purposes.

User List Spreadsheet

Following are an example of a User List spreadsheet and the instructions to complete that spreadsheet. The spreadsheet must be completed and emailed according to subparagraph 2 A.

Instructions to fill out spreadsheet to attach to AD-1143 for access to LRAT

For each user needing access to the LRAT system:

- 1) Enter name into column A
- 2) Enter eAuthentication ID into column B
- 3) Enter role needed for LRAT into column C (see below for list of roles and descriptions)
- 4) Enter email address into column D
- 5) Enter preferred training date and time in column E (see Notice for list of training dates and times)

List of LRAT Roles (with descriptions)*:

LRAT_STATECLERK – Access to enter leases

LRAT_COUNTYCLERK – Access to view leases only

LRAT_HQ – Headquarters accountant with access to approve leases in all states within their agency

LRAT_HQVIEW – Headquarters accountant with access to view leases in all states within their agency

LRAT_HQSTATE – Same access level as HQ but only for a specific list of states in their agency (additional state access is available via the User Access functionality within the LRAT system)

LRAT_ADMIN – May only approve access requests for additional states/counties within their agency

*Each user will be given an agency-specific role. An example of an FSA role is: FSA_LRAT_STATECLERK, and example of an NRCS role is NRCS_LRAT_STATECLERK, and an example of an RD role is RD_LRAT_STATECLERK. When filling out the access spreadsheet, states will need to distinguish which agency the users need access for.

AD-1143 Spreadsheet Attachment for access to LRAT

Name	eAuthentication ID	Role needed for LRAT	Email address	Training Date and time