Print

OMB APPROVED NO. 0584-0532
Expiration Date: 03/31/2018

U.S. Department of Agriculture - Food, Nutrition and Consumer Services

User Access Request Form

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of Information unless it displays a valid OMB control number. The valid OMB control number for this information collection is 0584-0532. The time required to complete this information collection is estimated to average 10 minutes per response, including the time to review instructions, search existing data resources, gather the data needed, and complete and review the information collection.

User Information

1. Last Name	First Name	Middle Name	2. Title	3. Date of Request

4. Email	5. USDA E-Auth ID, *(if applicable)*

6. Type of User *(select one)*	7. Telephone	8. Contract Expiration Date *(if applicable)*	9. Temporary Employee Expiration Date *(if applicable)*

10. Company	11. Division	12. Department

13. Office *(select one)*	Street Address	Suite #
City	State	ZIP Code

14. System Name	15. Type of Access / Role	16. Form *(applicable for FPRS)*

17. Action Requested	18. State/Locality Codes	19. Login ID *(current users)*

20. Enter a pass phrase for NFC verification (new NFC access only): _____

21. Enter Home ZIP Code for JP Morgan access Only: _____

22. Comments, Special Instructions and/or Justification (if "Other" is selected in fields 6, 13, or 14). *(attach separate sheet if more space is needed)*

Privacy Act Statement

The privacy act is stated for individuals requesting access to the National Finance Center *(NFC)*. The authority in collecting this information is 5 U.S.C. 301. The use of the requesting person's Social Security Number *(SSN)* is for identification purposes only. Existing NFC users requesting modification or termination of access to the NFC are not required to provide their SSN.

23. User Acknowledgement *(Users requesting system access must read, sign and date prior to submitting this form)*

- I have read and understand the Privacy Act Statement above and the FNCS Rules of Behavior (see page 2 for complete verbiage)
- Decisions in personnel matters involving disciplinary action will be based on the assumption that I am familiar with the security requirements presented in these rules and I am aware of my obligation to abide by them.
- I understand that systems require security to protect user and system files from unauthorized access.
- I have completed this form to the best of my abilities.

User Signature _____ Print Name _____ Date _____

Approvals

24. a. Supervisor / COR

Print Name _____ ☐ Approve ☐ Deny
Phone Number _____ Date _____ Signature _____

b. System - Authorizing Official (FNCS)

Print Name _____ ☐ Approve ☐ Deny
Phone Number _____ Date _____ Signature _____

c. Information Security Office (FNCS)

Print Name _____ ☐ Approve ☐ Deny
Phone Number _____ Date _____ Signature _____

d. State Computer Security Officer *(if applicable)*

Print Name _____ ☐ Approve ☐ Deny
Phone Number _____ Date _____ Signature _____

To be Completed by IT Customer Support (FNCS)

25. Has the Security and Privacy Training been completed? ☐ YES ☐ NO	26. Date Received	27. Person Receiving Request	28. Date Completed

Rules of Behavior *(ROB)* - FNCS General User

User ID and password

The User ID and password being issued to you must not be shared with or given to anyone else. FNCS Users who share their User ID or password will be in violation of the Computer Fraud and Abuse Act of 1986. If you forget your password or believe your password has been compromised, contact the ISO immediately. To have your account reset, contact IT Customer Support (1-888-OIT-4FNS) or open a ticket through the Help Desk ticketing system.

Monitoring and Auditing of FNCS Information Resources

At anytime, FNCS/USDA may monitor and/or audit user activity and/or network traffic. In addition, USDA may access your system and disclose information obtained through audits to third parties, including law enforcement authorities. Acceptance of the warning banner prior to logging onto the FNCS network is your acknowledgment of the FNCS/USDA monitoring/auditing.

Violations

Violations of information system security guidelines and procedures may lead to disciplinary action up to and including termination of employment.

Manager/Supervisor Responsibilities

All persons in a management role at FNCS must be aware of and knowledgeable in information system security practices. Managers are responsible for enforcing these practices within their areas and will be held accountable for ensuring that users are aware of and acknowledge their responsibilities. FNCS Management is also responsible for ensuring that all FNCS Users, i.e. Employees, Contract Personnel and Official Visitors attend mandatory computer security training.

FNCS User Responsibilities

FNCS User's access to information system resources indicates a level of trust between the User, FNCS Management and ISO. Therefore, FNCS Users are held accountable for the following:

- Ensure the ethical use of FNCS information resources in accordance with FNCS guidelines and procedures.
- Utilize all security measures that are in place to protect the confidentiality, integrity and availability of information and systems.
- Refrain from using FNCS information resources for inappropriate activities.
- Adhere to all licenses, copyright laws, contracts, and other restricted or proprietary information.
- Always safeguard User IDs, passwords, and smartcards.
- Protect FNCS information resources when working remotely by ensuring the latest patches and antivirus software are loaded on your Government Furnished equipment *(GFE)*.
- Limited personal use of the Internet is allowed as long it does not interfere with official business or reflect adversely on FNCS Information Systems.
- Access only those information systems, networks, data, control information, and software that you are authorized to use.
- Know who your Information System Security Officers *(ISSOs)* are and how to contact them.
- Determine the sensitivity of the information and programs on your computing resources *(e.g. non-sensitive, sensitive but unclassified)*.
- Avoid the introduction of harmful files/data that may contain spy-ware, viruses, etc. into any computing resource.
- Please refer to the Guidance on Acceptable Use of FNCS Information System in the 702 handbook for additional acceptable uses of the system.
- If you have any questions on FNCS Information Systems Security, please contact IT customer support (1-888-OIT-4FNS) or send an email to the Security Mailbox at SecurityOfficers.Mailbox@fns.usda.gov.

Form Instructions

1. **LAST, FIRST, MIDDLE NAME** - Enter the last name, first name and middle name *(if applicable)* of the person requesting FNCS computer system access. If middle name does not exist, enter n/a.

2. **TITLE** - Enter current Title.

3. **DATE OF REQUEST** - Select from the calendar, the date you are requesting access to an FNCS system.

4. **EMAIL** - Enter the FNCS email address, if known.

5. **USDA E-AUTH ID** - Enter your official e-Authentication ID, (existing users).

   To obtain an e-Auth ID go to http://www.eauth.egov.usda.gov/index.html and click on "Create an Account"

6. **TYPE OF USER** - Select your user type from the drop-down menu; Federal, State, Contractor, JP Morgan or Other. "If "Other" was selected in this field, please provide an explanation in Field 22 of what "Other" means as well as the justification for the selection."

7. **TELEPHONE**- Enter telephone.

8. **CONTRACT EXPIRATION DATE** - If you are a Contractor, enter your Contractor Expiration Date. Please contact your COTR for this date.

9. **TEMPORARY EMPLOYEE EXPIRATION DATE -** If you are a Temporary Employee *(Intern)*, enter your Expiration Date. Please contact your supervisor for this date.

10. **COMPANY** - Enter your company/agency affiliation.

11. **DIVISION** - Enter your division affiliation.

12. **DEPARTMENT** - Enter your department affiliation.

13. **OFFICE** - Select your office affiliation from the drop-down menu. Enter the street number, street name, suite number, city, state and zip code of the facility where the requesting user will be working. "If "Other" was selected in this field, please provide an explanation in Field 22 of what "Other" means as well as the justification for the selection."

14. **SYSTEM NAME** - Enter the system that you are requesting to access. "If "Other" was selected in this field, please provide an explanation in Field 22 of what "Other" means as well as the justification for the selection."

15. **TYPE OF ACCESS / ROLE** - For the system, enter the type of access or role requested. Access and role types are system specific. Please check with the System Owner to determine the appropriate access or role type.

16. **FORM** - This field is needed for FPRS access only. Enter the form that the user has requested to access.

17. **ACTION REQUESTED** - Enter the type of access requested for this system, if you are not sure, please contact the system owner for the appropriate action.

18. **STATE/LOCALITY CODES** - Enter the state/locality codes that are needed for system access. State/Locality codes are FNCS organization codes that specific systems may require. If required, these codes will determine the information that you can access within the FNCS system. If you do not know your state/locality code, please contact the System Owner for the code.

19. **LOGIN ID** - If an existing account, enter in your current login ID.

20. **PASS PHRASE -** Enter a pass phrase if you are requesting new NFC access only! An FNCS Information Security Officer will contact you to obtain your social security number for NFC and will provide your pass phrase to you.

21. **HOME ZIP CODE** - Enter your home zip code if you are requesting access to JPMorgan only!

22. **COMMENTS, SPECIAL INSTRUCTIONS** - Enter any comments or special instructions that are needed for the completion of this request for system access.

23. **USER ACKNOWLEDGEMENT** - Read the Privacy Act Statement and the FNCS Rules of Behavior *(ROB)*, sign and date the user acknowledgement statement. This must be completed prior to submitting this form to your supervisor.

24. **APPROVALS** - Prior to the user submitting the User Access Request form, it must be approved by the following: the user's Supervisor, the Authorizing Official for the system, the Information Security Office and the State Computer Security Officer, if applicable.

25. **SECURITY and PRIVACY TRAINING COMPLETE -** This section is for FNCS IT Customer Support and Information Security Office Staff use only.

26. **DATE RECEIVED** - This section is for FNCS IT Customer Support and Information Security Office Staff use only.

27. **PERSON RECEIVING REQUEST** - This section is for FNCS IT Customer Support and Information Security Office Staff use only.

28. **DATE COMPLETED** - This section is for FNCS IT Customer Support and Information Security Office Staff use only.