Print

OMB Control Number 0584-XXXX
Expiration Date: XX/XX/2011

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.

PART A

1. User Name			2. USDA E-Auth ID, *(if applicable)*	3. Date of Request
Last Name	First Name	Middle Name		

4. Type of User *(select one)*	5. User Information		
	Title	Email	
	Telephone	Contract Expiration Date *(if applicable)*	Temporary Employee Expiration Date *(if applicable)*

6. Security Challenge Question *(for identification purposes)*

New Users, choose one question: *(select one)*	Enter Security Challenge response:

7. Company *(select one)*	8. Office *(select one)*	9. Office Address	
		Street Address	Suite #
10. Department *(select one)*	11. Division *(select one)*	City / State / ZIP Code	

12. System Name	13. Type of Access	14. Form *(applicable for FPRS)*	15. Action Requested	16. State/Locality Codes	17. Login ID *(ISO only)*

18. SSN	19. Enter Home ZIP Code
STOP! Enter SSN for new NFC access Only: _____	STOP! Enter ZIP Code for JP Morgan access Only: _____

20. Comments, Special Instructions

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

- I have read and understand the Privacy Act in Part B and security rules of behavior in Part C of this form.
- 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

To be Completed by the Infrastructure Branch

Has the CSAT and Privacy Training been completed? ☐ YES ☐ NO

User Access Request Form

PART A *(Continued)*

22. Approvals

A. Supervisor

☐ Approve ☐ Deny

Print Name _____

Phone Number _____ Date _____ **Signature** _____

B. System - Authorizing Officials

System: _____ ☐ Approve ☐ Deny

Print Name _____

Phone Number _____ Date _____ **Signature** _____

System: _____ ☐ Approve ☐ Deny

Print Name _____

Phone Number _____ Date _____ **Signature** _____

System: _____ ☐ Approve ☐ Deny

Print Name _____

Phone Number _____ Date _____ **Signature** _____

System: _____ ☐ Approve ☐ Deny

Print Name _____

Phone Number _____ Date _____ **Signature** _____

System: _____ ☐ Approve ☐ Deny

Print Name _____

Phone Number _____ Date _____ **Signature** _____

C. Information Systems Security Officer

☐ Approve ☐ Deny

Print Name _____

Phone Number _____ Date _____ **Signature** _____

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

☐ Approve ☐ Deny

Print Name _____

Phone Number _____ Date _____ **Signature** _____

To be Completed by IT Customer Support

23. Date Received	24. Person Receiving Request	25. Date Completed

PART B 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.

User Access Request Form

Form Instructions

1. **USER NAME** *(Last, First, Middle)* - 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. **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".
3. **DATE OF REQUEST** - Select from the calendar, the date you are requesting access to an FNCS system.
4. **TYPE OF USER** - Select your user type from the drop-down menu; Federal, State, Contractor, JP Morgan or Other.
5. **USER INFORMATION** - Enter the office phone, current Title and FNCS email address, if known. If you are a Contractor, enter your Contractor Expiration Date. Please contact your COTR for this date. If you are a Temporary Employee *(Intern)*, enter your Expiration Date. Please contact your supervisor for this date.
6. **SECURITY CHALLENGE QUESTION AND RESPONSE** - From the drop-down menu, select one security challenge. In the space provided, enter in your response. This information is for identification purposes only. *Please remember your response since you will asked your response when you contact the IT Customer Support or ISO.*
7. **COMPANY** - Select from the drop-down menu, the company you are affiliated with. If you are a full time FNCS employee, choose FNCS. If you are a contractor, find your company and select it. If your company is not on the list, contact the IT Customer Support.
8. **OFFICE** - Select from the drop-down menu the office you are affiliated with, e.g. N.O., MARO, etc.
9. **OFFICE ADDRESS** - Enter the street number, street name, suite number, city, state and zip code of the FNCS facility where the requesting user will be working.
10. **DEPARTMENT** - Select from the drop-down menu, the department you will work in, e.g. OIT, FSP, etc.
11. **DIVISION** - Select from the drop-down menu, the division you will work in, e.g. Technology, Portfolio Management, etc.
12. **SYSTEM NAME** - Enter 1 or more systems that you have requested to access.
13. **TYPE OF ACCESS** - For each system chosen *(in #12)*, enter the type of access requested. Access types are system specific. Please check with the System Owner to determine the appropriate access type.
14. **FORM** - This field is needed for FPRS access only. Enter the form that the user has requested to access.
15. **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.
16. **STATE/LOCALITY CODES** - Enter the state/locality codes that are needed for system access. If you do not know your state/locality code, please contact the System Owner for the code, if it is required for the system.

    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.
17. **LOGIN ID** - For new accounts, the ISO will enter the login ID here. If an existing account, enter in your current login ID.
18. **SOCIAL SECURITY NUMBER (SSN)** - Enter your SSN if requesting access to the NFC only!
19. **HOME ZIP CODE** - Enter your home zip code if you are requesting access to JPMorgan only!
20. **COMMENTS, SPECIAL INSTRUCTIONS** - Enter any comments or special instructions that are needed for the completion of this request for system access.
21. **USER ACKNOWLEDGEMENT** - Please read Part B - Privacy Act and Part C - Rules of Behavior *(ROB)*, then read sign and date the user acknowledgement statement. This must be completed prior to submitting this form to your supervisor.

    CSAT and Privacy Training complete, yes or no. To be completed by the Infrastructure Branch.
22. **APPROVALS** - Prior to the user submitting the Computer Systems Applications Access Request form, it must be approved by the following: the user's Supervisor, the Information Systems Security Officer, the Authorizing Official for the system and the State Computer Security Officer, if applicable.

    DECISION - The appropriate Official will indicate whether they have approved or denied the System Access Request.

    DATE - The date that the system request was either approved or denied.

    OFFICIAL SIGNATURES - The appropriate Official signs their name. After signing, choose the appropriate system from the drop-down menu.

    PHONE NUMBER - The official's seven-digit office telephone number.
23. **DATE RECEIVED** - This section is for FNCS IT Customer Support and Information Security Office Staff use only.
24. **PERSON RECEIVING REQUEST** - This section is for FNCS IT Customer Support and Information Security Office Staff use only.
25. **DATE COMPLETED** - This section is for FNCS IT Customer Support and Information Security Office Staff use only.

User Access Request Form

PART C

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 the IT Customer Support (703-305-2800) or open a ticket through Track-it.

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 their actions when accessing the FNCS Network. At a minimum, FNCS Users are responsible 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 is loaded onto your Government Owner equipment *(GOE)*.
- Limited personal use of the Internet as long it does not interfere with official business nor reflect adversely on FNCS Information Systems.
- Access only those information systems, networks, data, control information, and software that you are authorized to use.
- Know your Information System Security Officers *(ISSOs)* are and how to contact them.
- Determine the sensitivity of the information and programs on their 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 Shawn Jones at (703) 305-2528, or Cord Chase at (703) 305-2796 or send an email to the Security Mailbox at SecurityOfficers.Mailbox@fns.usda.gov.