United States Office of Personnel Management

Coverage Determination Application

CDA USER PROFILE

Section I - Applicant Information

CDA UserID

- ☐ New CDA UserID
- ☐ Existing CDA UserID
  (Furnish CDA UserID in CDA UserID box on left.)
- ☐ Deactivate CDA UserID
  Specify deactivation date: _____
  (Furnish CDA UserID in CDA UserID box on left.)
- ☐ Modify existing CDA UserID
  Specify effective date: _____
  (Furnish CDA UserID in CDA UserID box on left.)
  Specify what is being modified *(Name, type of access, etc.)*

☐ Federal Employee — Agency Name: _____

- ☐ Permanent — Department: _____
- ☐ Temporary Exp. Date: _____

(If applicant is a contractor, a Federal employee supervisor must fill out form and have contractor sign and date in blocks 7 and 8.)

☐ Contractor — Expiration Date of Contract: _____

Company: _____ Agency Name: _____

Contract Number: _____ Department: _____

1. Name *(Last, First, Middle Initial)*	2. Telephone Number *(Include Area Code and Extension)*
3. Last Four Digits of Social Security Number	4. Title/Position
5. Duty Location *(City, State, Zip Code)*	6. E-mail address

Computer UserID and Password Disclosure Statement

I understand that my UserID and password are for my use only. I agree to protect my password from disclosure by all reasonable means, and not willingly divulge it or allow its use by any other person(s). If I believe that another person has learned my password, I will notify my supervisor immediately. I understand that my use of Government equipment, including computer systems, must comply with the policies specified in the OPM "Policy on the Use of Government Office Equipment." If I am an employee of an agency other than OPM, I must also comply with my Agency's policy. I must also read, sign and date the Rules of Behavior on page 3.

7. Signature of applicant	8. Date of signature *(mm/dd/yyyy)*

Section II - Federal Supervisor Information on page two (2) must be completed by your supervisor.

PRINT SAVE CLEAR

Section II - Applicant's Federal Supervisor Information

(Applicant's Federal Supervisor must complete this section)

9. Grant the applicant the following CDA user access. Check one box.

☐ **General Access** - (Create employee record, update record, execute coverage determination, and view record)

☐ **General Access with Manual Override** - (General Access PLUS manual override authority, an authorization in the CDA that is generally granted to senior staff and supervisors. It is used when a retirement coverage determination made by the CDA differs from the retirement plan of record that was entered by the CDA user. Someone in your office should have this authority.)

10. Applicant's Federal Supervisor Name (Last, First, Middle Initial) *(The approving official must be a Federal employee supervisor.)*

11. Title/Position	12. Telephone Number *(Include Area Code and Extension)*
13. Duty Location *(City, State, ZIP Code)*	14. E-mail address

15. **Must complete for All New CDA UserID Requests -** Supervisor must provide status of Background Investigation of new user. Provide date in either the "Completed On" or "In Progress" area and your initials.

Completed On Date: Supervisor's Initials:	In Progress Date CDA UserID should be activated *(if in progress)*: Supervisor's Initials:

16. Supervisor's signature	17. Date of signature *(mm/dd/yyyy)*

All information and proper signatures must be completed or this User Profile Form will not be processed. If you have any questions, please contact OPM at: 1-800-239-2492 or CDAHelp@opm.gov. After you complete this form online, print form, and sign and date blocks 7 and 8. Your supervisor completes Section II, signs and date blocks 16 and 17. You must read the "Rules of Behavior, " (page 3), sign and date. Fax all 3 pages of this form to: (202) 606-1108. We cannot accept a completed form by email.

Section III - OPM Security Officer Information

(To be completed by OPM Security Officers Only)

18. Comments

19. Signature of OPM Designated Security Officer (DSO)	20. Date of signature *(mm/dd/yyyy)*

PRINT SAVE CLEAR

Rules of Behavior

(OPM Computer User Responsibilities)

As a user of OPM's computer systems, you are expected to understand and comply with the responsibilities outlined below. You will be held accountable for your actions when using these systems. If you violate OPM policy regarding these responsibilities, you may be subject to administrative action ranging from counseling to removal from the Agency, as well as any criminal penalties or financial liability, depending on the severity of the misuse. As required by OPM policy, users of OPM's Coverage Determination Application (CDA) have responsibilities for protecting OPM's information resources from loss; theft; misuse; destruction; and unauthorized access, disclosure, modification or duplication.

Privacy While Using Government Equipment - You do not have the right to privacy while using any Government equipment, including Internet or email services. Furthermore, your use of Government office equipment, for whatever purpose, is not secure, private or anonymous. While using Government office equipment, your use may be monitored or recorded.

Protection of Software, Data and Hardware - You are not allowed to introduce any unauthorized software and data (including software and data protected by copyright, trademark, privacy laws, other proprietary data or material with other intellectual property rights beyond fair use), hardware or telecommunications devices or modify any configurations. In addition, you will protect all sensitive information residing in OPM computer systems, preventing unauthorized access, use, modification, disclosure or destruction of that information. This includes records about individuals requiring protection under the Privacy Act, sensitive financial information and information that cannot be released under the Freedom of Information Act. Disclosure of sensitive information, trade secrets and intellectual property to unauthorized individuals is also prohibited.

Service Restoration - The availability of the computer systems is a matter of importance to you. You are responsible for assisting in any way that you can for restoring service in the event the computer systems becomes non-operational.

System Privileges - You are given access to the computer systems based on a need to perform specific work. You are expected to work within the confines of the access allowed and are not to attempt to access systems or applications for which access is not authorized.

Telework - Refer to www.telework.gov for information on the policy and procedures for authorizing telework. In general, immediate supervisors approve, on a case-by-case basis, employee requests to telework. Teleworkers who access OPM's general support systems must adhere to all IT security policy and procedures that would apply if the individual was accessing OPM's systems in the office.

Use of Government Office Equipment - You will comply with the policies specified in the OPM Policy on Personal Use of Government Office Equipment.

Use of Passwords - You will create and use passwords as specified in the IT Security Policy. You must keep your passwords confidential and not share them with anyone. Individual applications may have more stringent password requirements than the general policy requirements.

Protection of software copyright licenses - The copyright licenses associated with the Commercial off-the-shelf (COTS) components of the Coverage Determination Application (CDA) are complied by OPM personnel, as well as by contractors responsible for developing and maintaining the CDA. OPM requires that all copyright licenses for all software (especially web-server based software) used by program personnel and contractor personnel are understood and that these personnel comply with the license requirements. End users, supervisors, and function managers are ultimately responsible for this compliance.

Basic Security Awareness Training - National Institute of Standards and Technology (NIST) Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, states: "The organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and annually thereafter." Your agency is responsible for providing you with this required security awareness training yearly.

Notify OPM - You or your supervisor must notify OPM immediately if you no longer require access to the CDA for any reason, or change your position, or transfer to another agency. Contact OPM at: 1-800-239-2492 or CDAHelp@opm.gov.

Signature of CDA Applicant	Date *(mm/dd/yyyy)*
Printed Name of CDA Applicant	Agency

PRINT SAVE CLEAR