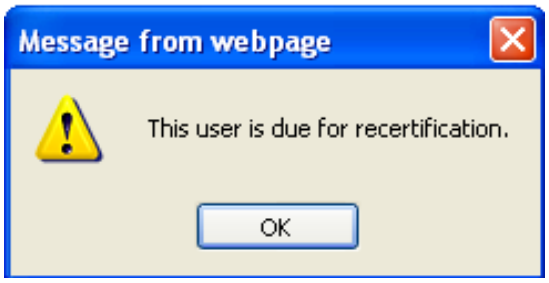
Recertifying your ITM Access

1. Log into the Integrated Travel Manager (ITM) application:

   https://itm-prod.rdc.noaa.gov/cgi-bin/90ipi/docprep/login.w

2. Upon login the ITM Recertification notice will appear onscreen. Users will be required to click OK to acknowledge the notification.



3. The ITM Recertification screen will automatically be populated with your name and user account information. All ITM application roles which are assigned to your account will be listed and the check boxes will automatically default as checked [✓].

   a. Review each role and determine if your access is still required. **If yes, make no changes and proceed to Step b.** If no, click the check box to remove the check mark located next the role(s) that is no longer required before proceeding to Step b.

   b. Read the information contained within the Recertification Details block.

   c. Click, *I agree to the above* check box if you accept the terms of the agreement.

   d. Click on the Recertify button to certify your access. Note the Recertify button will only enable if you check "I agree to the above".

User Recertification -- User ID: *cur3186* Name: *Cynthia E. Curtis*

Quick Tip
Your account is due for recertification. You should: 1) Read the text below 2) Check the 'I agree to the above' box to indicate you have read and agree with the terms presented 3) Uncheck any roles that are no longer needed and leave any roles still needed checked 4) Click Recertify (Note: The Recertify button is only enabled if you check 'I agree to the above')

D

E

For this Page you can:

- **Recertify** By clicking Recertify I acknowledge that I am the user identified, I accept the agreement presented, and I require the Roles specified (AS SHOWN BELOW)
- **Proceed** into Travel Manager without recertifying at this time
- **Exit** Travel Manager without recertifying at this time
- **Reset** screen to initial values

Recertification Details

B

AUTHORITY

This certification notice is issued under the authority of the Federal Information Security Management Act of 2002 (Pub.L No 107-307. Title 8.

USER AGREEMENT

By selecting the "I Accept" items I signify the understanding and acceptance of these policies and practices concerning access to the Commerce Business Systems (CBS) and that I will be held accountable for any breach of these policies and practices. CBS is a U.S. Government computer system used to conduct official Government business and shall be conducted in a manner above reproach and in accordance with the highest ethical standards to ensure the confidentiality in the integrity of the Government, its employees and systems.

1. I understand that the CBS systems are U.S. Government systems for the purpose of conducting official Government business
2. I understand the User ID and any other information related to access and use of the CBS systems are considered sensitive
3. I will not enter classified information into the CBS systems
4. I will protect my personal password from disclosure
5. I will log off or otherwise restrict access to any CBS system session when I am not personally attending to it
6. If I suspect someone else has tried to learn my password or fraudulently gain access to the CBS systems, I will immediately report the incident to my supervisor.

NON-DISCLOSURE AGREEMENT

As an employee or contractor of the Department of Commerce (DOC) with access to the National Oceanic and Atmospheric Administration (NOAA) Commerce Business Systems (CBS), you are required to be aware of, and comply with all applicable laws, regulations, not limited to the Privacy Act of 1974, Computer Fraud and Abuse Act of 1988, DOC Policy on Password Management, NOAA Information Technology (IT) Security Policy, and the NOAA Rules of Behavior. All users must complete the IT Security Awareness Training course every year to obtain and/or continue access to NOAA IT resources.

The CBS is an integrated financial management system intended to assist bureaus in complying with sound federal accounting practices. The CBS is a collection of administrative / management systems that are integrated with the Core Financial System (CFS). The administrative systems include budget information, requisitions and procurement, time reporting, personnel and payroll, property, purchase card, travel and grants. The CFS modules include Data Warehouse, Labor Distribution, General Ledger, Cost Accumulation, Budget Execution and Funds Management, Accounts Receivable, Accounts Payable and other standard interfaces.

The information and data, if disclosed to unauthorized sources, could violate the Privacy Act, OMB M06-16 (PII) and/or result in financial loss or adverse legal actions.

I hereby consent to this agreement in consideration for my being granted conditional access containing sensitive but *unclassified information, personally identifiable information and privacy act information* concerning financial acquisition, travel, human resources, real or personal property, budget and other areas. Information may be in the form of system data, files and records, contract data, analyses, memos meeting content, conversations, or any other form. I understand and agree to the following terms and conditions:

- I will only access, or attempt to access, *sensitive but unclassified information* systems for which I am granted conditional access authorization and have a "need to know/access".
- I will not divulge my password(s) or share them with any other person.
- I will not disclose or extract any confidential data, Privacy Act / PII data, employee information, or bureau specific sensitive but unclassified information which could adversely affect the Government's interest or the privacy to which individuals are entitled.
- I will not use, release, or disclose any *sensitive but unclassified information*, in any form whatsoever, to any person or entity other than authorized individuals without written authorization. *Note: Individuals providing services under contractual arrangements cannot share information with their company/organization nor with any other external individual, corporation, business, or organization.*
- I will protect *sensitive but unclassified information* in accordance with the provisions of the Privacy Act, OMB M06-16 (PII) and other pertinent laws and regulations governing the confidentiality of privileged information. If I become aware of any improper use, extract, release or disclosure of Privacy Act / PII data or non-public information, I will advise NOAA management and complete the NOAA IT Security Incident Reporting Form as soon as possible. *Note: Contractors are required to provide a copy of this User Agreement to their employers to ensure that they are aware of non-disclosure responsibilities.*
- I understand that any unauthorized use, release or disclosure of non-public information in violation of this agreement may subject me to administrative actions that range from a verbal or written warning, removal of system access, reassignment of duties, and/or termination of employment or contract, depending on the severity of the violation.

APPROVING OFFICIAL RESPONSIBILITIES

ITM Users re-certifying for the role of ITM APPROVING OFFICIAL further acknowledge and accept the following responsibilities:

1. Approving Officials are responsible for knowing current travel policy
2. Approving Officials must determine if travel is essential to the agency mission, ensure adequate funds are available prior to authorizing travel and make sure the mode of transportation selected is most advantageous to the Government
3. Approving Officials must determine if travel expenses are necessary, reasonable, justified and consistent with completing the assigned objectives or mission, review the accounting code(s) selected to ensure the correct funding is being charged for the travel being performed
4. Approving Officials must ensure travel claims are properly prepared in accordance with pertinent regulations and agency procedures, the types of expenses claimed are authorized and allowable, the amounts claimed are accurate, and the required receipts, statements, and justifications are attached with the voucher and are retained for six years and three months.

C ☑ **I agree to the above**

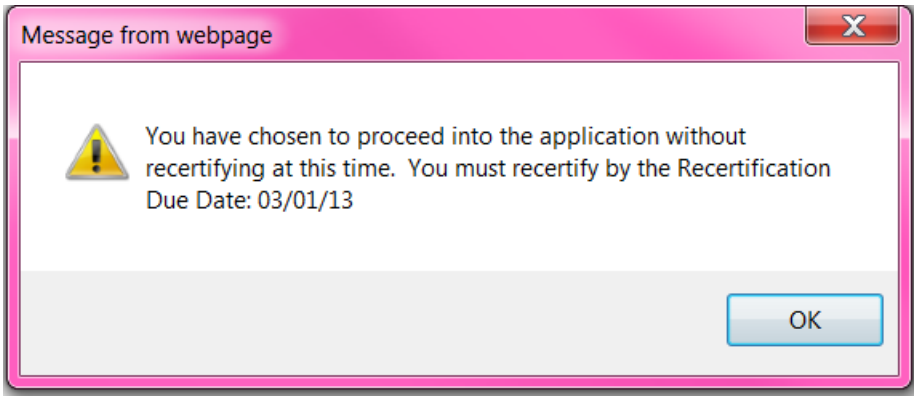
The Following Roles Are Still Required (uncheck unneeded roles)

A

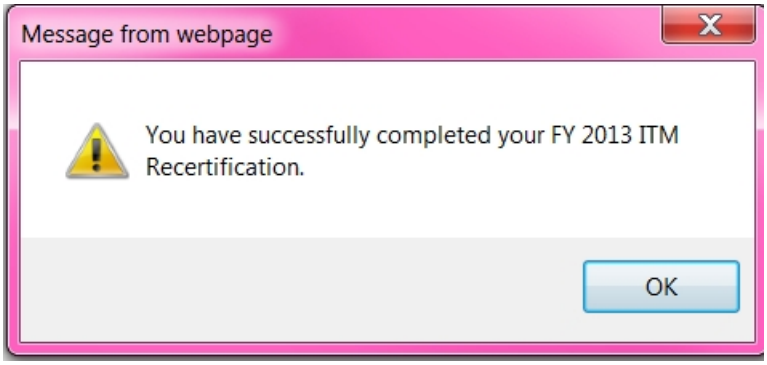
- ☑ DISABLED - Allows user to disable user accounts
- ☑ ITM USER - Allows user access into ITM
- ☑ ITM APPROVING OFFICIAL - Allows access to approve documents
- ☑ ITM GROUP ADMIN / REVIEWER - Allows group/review access
- ☑ ITM FINANCE OFFICE USER - Allows access to Finance functions
- ☑ ITM ROUTING ADMINISTRATOR - Allows access to Routing Maint.
- ☑ UNUSED - Reserved for future use
- ☑ UNUSED - Reserved for future use
- ☑ CLIENT SERVICES HELP DESK - Allows access to Admin screens
- ☑ APPLICATION ADMINISTRATOR - Allows access to Admin functions

e. [Optional – Not Recommended] – Click Proceed, to temporarily defer recertification. Note: In order to retain access to the ITM application, you must recertify by the recertification due date. Once the recertification due date is reached, the Proceed button will no longer be an available option. Users will be required to recertify or Exit the system.

The following message displays only when a user elects to Proceed without recertifying:



f. Upon recertifying your access a confirmation window will appear informing the user they have successfully completed the recertification process.



Note: Once this onscreen confirmation notice is received no further action will be required by the user until the next annual recertification cycle.