Appendix B

Rules of Behavior

Security Awareness and Training for the Government Wide Accounting System Modules

Please read and accept the Terms of Use in order to complete your access request.

GENERAL

- **Exercise only those Governmentwide Accounting (GWA) System capabilities assigned to you by your Organization or Unit GWA Security Administrator:**

  Each user registered to access the GWA System will have a unique User ID. One or more specific roles may be assigned to each user. The level of authority available to a user in a role will determine the level of user authentication required to allow execution of the role. Both User ID and authentication information are the property of the GWA System and the user. Transfer of User ID and authentication to another can result in loss of GWA System access privileges. Attempting to exercise roles other than those assigned by any means can result in loss of GWA System access. Only one GWA Organization or Unit Security Administrator will give each GWA System user access authority. Each OSA and USA must have a backup.

- **Provide appropriate controls over sensitive information available from the GWA System.**

  Information available from the GWA System may be considered sensitive (Privacy Act), sensitive (Business), restricted or classified.
  Sensitive (Privacy Act) information is information that relates an individual by name, social security number or traceable characteristic (User ID, telephone number, etc.) to a financial transaction affecting that individual. Sensitive (Privacy Act) information must be controlled as defined in The Privacy Act of 1974, 5 USC & 552A - as amended. Sensitive (Business) is any information in GWA except that information appearing specifically on financial reports released to the Public by appropriate authority and then only in the context of the public report. Sensitive (Business) information can be released only to those individuals having a business need to see or use it. The GWA System will allow only those users with appropriate formal clearance to access the restricted information. If restricted information is available to you and you have neither appropriate clearance nor need to know, it is your responsibility to report the incident and associated circumstances to your GWA Organization or Unit Security Administrator or the GWA System administrator of the module you are accessing at once.

- **Understand and comply with applicable policies and procedures related to your access to, and use of, GWA resources.**

  Your organization has its own policies and procedures related to access and use of information available through your organization Intranet or the Internet. Your organization may have policies and procedures related to distribution of financial information within the organization and to external organizations. Your internal policies and procedures will be available through your GWA Organization or Unit Security Administrator.
  GWA System policies and procedures related to your access to, and use of, GWA System resources will be included in the GWA System Help Facility, GWA System training materials and through the GWA Web site (www.fms.treas.gov/gwa).

- **Identify potential risks to GWA System and information integrity, timeliness or sensitivity to the appropriate organization authority.**

  Since the financial management data and information in the GWA System is the U.S. Department of the Treasury's picture of information related to user agency financial status, it is critical that all who use the system and data participate in identifying conditions or actions which will impede the integrity, timeliness or sensitivity of the GWA System or data. Risks internal to your organization must be reported through your internal security point of contact. Apparent risks to the GWA System itself must be identified through your GWA Organization or Unit Security Administrator, the FMS Administrator, the GWA Module Administrator or through GWA Web Site.

- **Identify inhibitors to effective performance of your GWA System related responsibilities to the appropriate organization authority.**

  Inhibitors to your effective performance of the GWA System related tasks – non-expenditure transfers, warrants, reconciliation, reclassification, account statement analysis, etc, - have a direct impact on the integrity and timeliness of GWA information available for decision making and reporting. Inhibitors fit into two categories - GWA System oriented and organization infrastructure or system oriented. GWA System inhibitors to your performance may include such things as time to download information, download media, content of records or screens, availability of detail to support research, and the like. To report your GWA System inhibitors contact your GWA Organization or Unit Security Administrator, the FMS Administrator, the GWA Module Administrator or through GWA Web Site. Organization infrastructure or system inhibitors must be reported to the appropriate contact points in your organization.

SPECIFIC

USERS must ensure that the information technology (IT) resources with which they have been entrusted are used properly, as directed by FMS policies and standards, taking care that the laws, regulations, and policies governing the use of such

resources are followed and that the value of all information assets are preserved. Each user is responsible for all activities associated with their assigned User ID.

USERS must be knowledgeable about FMS IT policies and standards. As systems change, users are required to seek additional information in order to ensure current policies and procedures are followed.

USERS must take positive steps to protect FMS data from unauthorized use or disclosure.

USERS must not attempt to circumvent any FMS IT security control mechanisms.

USERS must follow proper logon/logoff procedures.

USERS must complete IT security awareness, training and education as required by their agency's policies and standards.

USERS must not read, alter, insert, copy, or delete any FMS data except in accordance with assigned job responsibilities. Ability to access data does not equate to authority to manipulate data. In particular:

USERS must not browse or search FMS data except in the performance of authorized duties.

USERS must not reveal information produced by the FMS application except as required by job function and within established procedures.

USERS must protect FMS communications/connectivity integrity.

USERS must comply with and provide assistance with IT audits and reviews as appropriate.

USERS must report any known or suspected breaches of IT security to security administrators immediately after discovery of the occurrence.

USERS must retrieve all hard copy printouts in a timely manner.

USERS must ensure that unauthorized individuals cannot view screen contents.

USERS must protect User IDs and passwords from improper disclosure. Passwords provide access to FMS data and resources.

USERS are responsible for any access made under his/her User ID and password.

USERS do not reveal Passwords under any circumstances. Password disclosure is considered a security violation and is to be reported as such. If Password disclosure is necessary for problem resolution, immediately select a new password once the problem has been resolved.

- Do not program login IDs or Passwords into automatic script routines or programs.
- Do not share Passwords with anyone else or use another person's Password.
- Do not write Passwords down.
- Change Passwords in accordance with the system/application requirements.
- Choose hard to guess Passwords, in accordance with the system/application requirements.

ACCEPTANCE

I have read the Financial Management Service (FMS) GWA System Modules Rules of Behavior information technology Terms of Use and fully understand the security requirements of the information systems, modules and data. I further understand that violation of these rules may be grounds for administrative and/or disciplinary action by agency officials and may result in actions up to and including termination or prosecution under Federal law.

[ ] Accept [ ] Do Not Accept

Print Full Name	Signature Date
Department/Agency/Bureau	
Address	E-mail
Phone No.	