Additional Help: 545
File Name: 545sag_062501_cd24
Last Revised: 06/04/2000

SUGGESTED WARNING SCREEN MESSAGES

As a means of discouraging unauthorized network use, increasing computer security awareness, and providing a legal basis for prosecution in cases involving unauthorized network access, Network Managers/Administrators must ensure users attempting network access are presented with a pre-logon warning massage. Successful use of this security measure depends upon the following:

* All messages must be short so they can be read in a glance;
* The content and appearance of the messages should be changed frequently;
* Introductory messages must not invite system exploration or exploitation; and
* All messages should use very large easy to read fonts and graphics.

It is essential the introductory screen be read rather than passed over with one quick key stroke.

The following screens are suggested for use:

This information system is intended for non-sensitive unclassified business only. Unauthorized access or use is a violation of law and may lead to prosecution.

Only UNCLASSIFIED, NON-SENSITIVE information is to be transmitted through this network. Unauthorized access or use of this network is a violation of law and may lead to prosecution.

This E-Mail system is not designed or intended for the transmission of privacy information, sensitive information or classified national security information. Unauthorized access or use of this network is a violation of law and may lead to prosecution.

*SUGGESTED WEB PAGE SECURITY AND MONITORING STATEMENTS

* AIDNET AND INTERNAL USAID WEB SITES:

USAID SECURITY/MONITORING STATEMENT

You are using an official United States Government system, which may be used only for authorized U.S. Government purposes. Unauthorized access or use of this system may subject you to administrative, civil, or criminal actions, as well as fines or other penalties. In accordance with Federal Regulations, employees have "a duty to protect and conserve Government property and shall not use such property, or allow its use, for other than authorized purposes."

This computer system may be monitored and information disclosed for any lawful purposes, including for the management and maintenance of the system, to ensure that the system is authorized to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security.

You have no reasonable expectation of privacy while using this system. Use of this system by any user, authorized or unauthorized, constitutes express consent to this monitoring.

Point of Contact for Security and Monitoring: [insert ISSO's name, hyperlinked to trigger an email window for comments] Information Systems Security Officer (ISSO) for USAID, M/IRM/OD, (202) 712-4559.

***** **EXTERNAL AND PUBLICLY AVAILABLE USAID WEB SITES:**

***** **SECURITY/MONITORING STATEMENT**

For SITE SECURITY purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act.

NOTICE: We will not obtain personally identifying information about you when you visit our site, unless you choose to provide such information to us.

Point of Contact for Security and Monitoring: [insert ISSO's name, hyperlinked to trigger an email window for comments] Information Systems Security Officer (ISSO) for USAID, M/IRM/OD, (202) 712-4559.