Information System Security Warning Screen Messages Guidelines

for System Owners and System Administrators

A Mandatory Reference for ADS Chapter 545

New Reference: 06/01/2006
Responsible Office: M/DCIO
File Name: 545sah_060106_cd44

Information System Security
Warning Screen Messages Guidelines
for System Owners and System Administrators

1. Introduction

Warning messages are a means of discouraging unauthorized network use, increasing computer security awareness, and providing a legal basis for prosecution in cases involving unauthorized network access. Where possible you must display a security warning message to users when they attempt to connect to USAID networks.

Warning messages should appear prior to logon, when users connect to a USAID workstation, server, or USAID web site (internal or external). You should adhere to the following general guidelines when creating warning messages:

- They must be short so they can be read at a glance,
- They must not invite system exploration or exploitation, and
- They should use very large, easy to read fonts and graphics, where possible.

2. Introductory Screens

Warning messages on introductory screens should be no more than a sentence or two. You should include information about security restrictions for that particular system or technology. You must make sure that users read the screen rather than pass over it with one quick key stroke. The following are examples of warning messages to use on introductory screens:

- 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 classified national security information. Unauthorized access or use of this network is a violation of law and may lead to prosecution.

3. USAID Workstations and Internal Web Sites

Warning messages for USAID workstations and internal web sites can be detailed. You should include information about usage restrictions, security monitoring, and privacy expectations for the system. Users have no expectation of privacy when using these workstations and web sites. The following is an example of a warning message to display when users connect to USAID workstations or internal 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 must 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.

4. External and Publicly Available USAID Web Sites

Warning messages for USAID external and publicly available web sites can be detailed. You should include information about usage restrictions, security monitoring, and privacy expectations for the system. Users can expect their personally identifying information to be kept private when using these web sites. The following is an example of a warning message to display when users connect to 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.