Nuclear Regulatory Commission
Office of the Chief Information Officer
Computer Security Standard

Office Instruction:	**CSO-STD-0040**
Office Instruction Title:	**Warning Banner Standard**
Revision Number:	**1.0**
Effective Date:	**February 16, 2017**
Primary Contacts:	**Jonathan Feibus**
Responsible Organization:	**OCIO/CSO**
Summary of Changes:	CSO-STD-0040, "Warning Banner Standard," provides standardized notification and consent warning banner language approved for use on NRC systems that store or process information up to, and including, the Safeguards Information (SGI) level.
Training:	As requested

Approvals			
Primary Office Owner	Office of the Chief Information Officer (OCIO) / Computer Security Organization (CSO)	**Signature**	**Date**
Chief Information Officer	David Nelson*	/RA/	02/21/2017
Chief Information Security Officer	Fred Brown*	/RA/	02/06/2017
Office of General Counsel Assistant General Counsel for Administration, no legal objection	Mark Maxin*	/RA/	02/16/2017
Office of Administration Director and Senior Agency Official for the Insider Threat Program, approval	Cynthia Carpenter*	/RA/	02/10/2017

TABLE OF CONTENTS

1 PURPOSE 1

2 INTRODUCTION 1

2.1 WARNING BANNERS 1
2.2 NRC STANDARDIZED WARNING BANNERS 2

3 GENERAL REQUIREMENTS 3

3.1 MANDATORY CONFIGURATIONS 3
3.2 SCALABILITY AND TAILORING 4
3.3 ROLES AND RESPONSIBILITIES 4

4 SPECIFIC REQUIREMENTS 5

4.1 STANDARDIZED WARNING BANNERS 5
4.1.1 Standardized Full Warning Banner 6
4.1.2 Standardized Concise Warning Banner 6
4.1.3 Standardized Network Device Warning Banner 7
4.1.4 Standardized Guest Network Warning Banner 7
4.2 STANDARDIZED MANDATORY NOTIFICATION AND CONSENT AGREEMENT 8

APPENDIX A. ACRONYMS 9

APPENDIX B. GLOSSARY 10

List of Figures

FIGURE 4.1-1: STANDARDIZED FULL WARNING BANNER 6
FIGURE 4.1-2: STANDARDIZED CONCISE WARNING BANNER 6
FIGURE 4.1-3: STANDARDIZED NETWORK DEVICE WARNING BANNER 7
FIGURE 4.1-4: STANDARDIZED GUEST NETWORK WARNING BANNER 7
FIGURE 4.2-1: STANDARDIZED MANDATORY NOTIFICATION AND CONSENT AGREEMENT 8

List of Tables

TABLE 3.3-1: ROLES AND RESPONSIBILITIES 5

Computer Security Standard
CSO-STD-0040

Warning Banner Standard

---

1 PURPOSE

CSO-STD-0040 “Warning Banner Standard,” provides standardized notification and consent banner language approved for use on Nuclear Regulatory Commission (NRC) systems that store or process information up to, and including, the Safeguards Information (SGI) level.

This standard is the single official source for authorized warning banner language for use on NRC information systems. Warning banner language specified in this standard supersedes warning banner language contained in prior agency cybersecurity issuances, including language contained in Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) and Center for Internet Security (CIS) Benchmarks accepted as agency standards.

This standard is for system administrators, system owners, and Information System Security Officers (ISSOs) responsible for implementing and configuring the approved warning banner language on NRC information systems to ensure warning banners on NRC information systems are compliant with the NRC Insider Threat Program.

This standard does not provide system or platform specific technical direction for the implementation of warning banners.

2 INTRODUCTION

This section provides high-level explanations for the security and legal justifications for using warning banners at system entry points and introduces the four standardized warning banners to be used on NRC systems and devices.

2.1 Warning Banners

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations,” requires a warning banner to be displayed to users before accessing federal systems. Warning banners:

- Provide security and legal notices to users accessing NRC information systems. Limited options and standardized language facilitate enforcement of the approved warning banner language. Consistent application across NRC systems supports security and legal objectives for user notification and consent.
- Notify users that they are subject to monitoring, and may incur legal penalties for inappropriate or unauthorized use of the system.

- Notify users that use of the system indicates consent to monitoring (as displayed in Figure 4.1-1, Standardized Full Warning Banner) and waiver of liability. Explicit user action, such as clicking an "I agree" button, is required to indicate consent to monitoring, and to further access the system.

2.2 NRC Standardized Warning Banners

NRC provides four standardized warning banners to meet the requirements of systems with varying character restrictions, access capabilities, and user groups.

- Standardized Full Warning Banner: The full warning banner is suitable for any NRC desktops, laptops, and other devices capable of supporting 1,155 or more characters within the banner. Refer to Figure 4.1-1, Standardized Full Warning Banner.
- Standardized Concise Warning Banner: The concise warning banner is suitable for mobile devices and systems (other than network devices) within the NRC infrastructure network which are unable to display the full warning banner due to system-imposed limitations. A consent agreement between users of mobile devices and systems displaying the concise warning banner is necessary to ensure that users explicitly consent to the authorized terms of use, in addition to viewing and consenting to the concise warning banner. The concise warning banner is suitable for mobile devices capable of displaying at least 117 characters within the banner. Refer to Figure 4.1-2, Standardized Concise Warning Banner.
- Standardized Network Device Warning Banner: The network device warning banner is suitable for any network devices (e.g., routers, switches, firewalls, and other appliances) on the NRC network which provide a direct logon interface (e.g., hardware that may be accessed directly by system administrators, NRC contractors, users, or vendors during repair or maintenance activities, without first accessing a bannered NRC system). The network device warning banner is suitable for network devices capable of displaying at least 277 characters within the banner. Refer to Figure 4.1-3, Standardized Network Device Warning Banner.
- Standardized Guest Networks Warning Banner: The guest networks warning banner can *only* be used for the NRC guest networks and other public access NRC systems, which are isolated from NRC infrastructure networks to prevent users from accessing local resources and information (refer to CSO-STD-1004, "Laptop Security Standard"). The guest networks warning banner is suitable for public access systems capable of displaying at least 1,266 characters within the banner. Refer to Figure 4.1-4, Standardized Guest Network Warning Banner.

  Note: In compliance with the NIST SP 800-53, as amended, and CSO-STD-4000, "Network Infrastructure Standard," publicly accessible NRC systems do not have an expectation of strong security controls or hardening, and are segregated from the NRC infrastructure network. Guest networks are not entirely dedicated to the public, but are provided for NRC visitors as a convenience to access the Internet. These systems have less stringent warning banner requirements than systems within the NRC infrastructure, thus a separate warning banner is provided to address these requirements. These systems are considered to be untrusted, because the users and the equipment used to access the Internet are outside of NRC control (refer to CSO-STD-4000).

The language comprising the NRC standardized warning banners is consistent with legal objectives for system warning banners identified by the Department of Justice,[1] including eliminating any Fourth Amendment "reasonable expectation of privacy" that users might otherwise retain in using the network, generating consent to monitor, or generating consent to retrieve stored files or records.

3 GENERAL REQUIREMENTS

This section addresses general requirements for implementing standardized warning banners on NRC information systems. All system administrators, system owners, and ISSOs authorized to configure information system warning banners must comply with these configurations as the minimum set of controls.

All standardized warning banners must be displayed at the human logon interface entry points of all NRC systems.

This standard provides overarching requirements that must be used in concert with:

- "NRC Agency-wide Rules of Behavior for Authorized Computer Use"
- NRC Management Directive (MD) 2.7, "Personal Use of Information Technology"
- NRC MD 12.5, "NRC Cybersecurity Program"
- NIST SP 800-53, as amended, "Security and Privacy Controls for Federal Information Systems and Organizations"
- Executive Order (EO) 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information"
- Presidential Memorandum, "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs," November 21, 2012

3.1 Mandatory Configurations

NRC systems must display a standardized warning banner at each human logon interface, the point at which the user first accesses the system. Systems without a human logon interface do not require warning banners.

Systems that can *only* be accessed by first passing through another warning bannered NRC system *do not* require a warning banner (e.g., users accessing the Information Technology Infrastructure [ITI] encounter a warning banner when first accessing the NRC Local Area Network [LAN]/Wide Area Network [WAN], and pass through to the Agencywide Documents Access and Management System [ADAMS] without encountering an ADAMS warning banner).

Systems that provide remote access to users, without first passing through a warning bannered NRC system, must display a separate logon warning banner at the remote user's initial entry

[1] Department of Justice, Office of Legal Education, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 2009. http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf

point into the NRC information system (e.g., users accessing Citrix®[2] encounter the Citrix warning banner, pass through to ITI, and subsequently pass through to ADAMS without a separate banner).

Applications that provide initial user access to NRC systems must be configured to display a standardized warning banner. Alternatively, the system must be configured to present a warning banner prior to accessing any applications.

The standardized warning banner must be implemented as a click-through banner window at logon, to the extent permitted by the operating system. The warning banner window must prevent further activity on the information system unless and until the user executes a positive action to indicate agreement (e.g., clicking a box indicating "OK"). Other options, such as clicking on the "X" to close a warning banner window or a dialog box without expressly clicking "OK," may not meet legal criteria for user consent.

The standardized warning banner and user agreement configuration settings must be hardened to prevent user-initiated changes.

3.2 Scalability and Tailoring

The standardized warning banner language must be implemented as stated in this standard. Unauthorized modifications may reduce the warning banner's efficacy by failing to meet security requirements and legal objectives for warning banners. Expressly prohibited modifications include, but are not limited to:

- Introducing or removing banner language;
- Rewording banner text; and
- Introducing abbreviations and contractions.

Any modifications to the standardized warning banner language found in this standard are a system deviation and must be authorized by the Office of the General Counsel (OGC) and OCIO.

3.3 Roles and Responsibilities

Table 3.3-1, Roles and Responsibilities, identifies the roles and responsibilities associated with implementing the standardized warning banner on NRC information systems.

[2] Citrix® is a trademark of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries."

Table 3.3-1: Roles and Responsibilities

Role	Responsibility
Chief Information Security Officer (CISO)	• Must authorize standardized warning banner language and implementation direction for use on NRC systems. • Must approve modifications to the standardized warning banner language for use on NRC systems. • Must develop, maintain, and update NRC standardized warning banner language and implementation direction. • Must ensure appropriate legal review of standardized warning banner language and implementation direction.
OGC	• Must provide a no legal objection to standardized warning banner language for use on NRC systems. • Must provide a no legal objection to modifications to the standardized warning banner language for use on NRC systems.
Office of Administration (ADM)	• Must provide approval of the warning banner language for use on NRC systems to ensure compliance with EO 13587 and the agency's Insider Threat Program. • Must provide approval of any modifications to the standardized warning banner language to ensure continued compliance with EO 13587.
System Owner	• Must provide oversight to ensure system warning banner implementations comply with CSO-STD-0040. • Must ensure system-specific user agreements of systems using the standardized concise warning banner include the "Standardized Mandatory Notification and Consent Agreement" (refer to Section 4.2).
System Administrators ISSOs	• Must ensure NRC information systems are configured to: – Use only authorized standardized warning banner language authorized in CSO-STD-0040, without modification or embellishment. – Display the standardized warning banner to users during the logon process, before granting access to the NRC information system. – Retain the standardized warning banner until the user acknowledges the usage conditions and takes explicit action to further access the system. • Must ensure system-specific user agreements of systems using the standardized concise warning banner include the "Standardized Mandatory Notification and Consent Agreement" (refer to Section 4.2).

4 SPECIFIC REQUIREMENTS

This section provides specific requirements for the implementation of the standardized warning banners and the "Standardized Mandatory Notification and Consent Agreement."

4.1 Standardized Warning Banners

This section provides the specific requirements for implementing the appropriate standardized warning banner on each system or device and the specific language required within each warning banner.

4.1.1 Standardized Full Warning Banner

The standardized full warning banner must be used for any application or device that can accommodate this warning banner, which has a length of 1,071 characters.

The standardized full warning banner text must be implemented as it appears in Figure 4.1-1.

I UNDERSTAND AND CONSENT TO THE FOLLOWING:

I am accessing a U.S. Government information system provided by the U.S. Nuclear Regulatory Commission (NRC) for U.S. Government-authorized use only, except as allowed by NRC policy. Unauthorized use of the information system is prohibited and subject to criminal, civil, security, or administrative proceedings and/or penalties.

USE OF THIS INFORMATION SYSTEM INDICATES CONSENT TO MONITORING AND RECORDING, INCLUDING PORTABLE ELECTRONIC DEVICES.

The Government routinely monitors communications occurring on this information system. I have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, the government may for any lawful government purpose monitor, intercept, search, or seize any communication or data transiting or stored on this information system.

Any communications or data transiting or stored on this information system may be disclosed or used in accordance with federal law or regulation.

REPORT ANY UNAUTHORIZED USE TO THE COMPUTER SECURITY INCIDENT RESPONSE TEAM (301-415-6666) AND THE INSPECTOR GENERAL.

Figure 4.1-1: Standardized Full Warning Banner

4.1.2 Standardized Concise Warning Banner

The standardized concise warning banner must be used for mobile devices and other system components unable to display the full warning banner specified in Section 4.1.1, Standardized Full Warning Banner, due to system-imposed character limitations. The standardized concise warning banner must also be used for network devices unable to display the network device warning banner specified in Section 4.1.3, Standardized Network Device Warning Banner, due to system-imposed character limitations. The current concise warning banner contains 117 characters.

The standardized concise warning banner text must be implemented as it appears in Figure 4.1-2.

Unauthorized Access Prohibited by Law -

Use Constitutes a Consent to Monitoring

Users have No Expectation of Privacy

Figure 4.1-2: Standardized Concise Warning Banner

The “Standardized Mandatory Notification and Consent Agreement,” provided in Section 4.2, must be used in conjunction with the standardized concise warning banner.

4.1.3 Standardized Network Device Warning Banner

The standardized network device warning banner must be used for routers, switches, firewalls, and other network appliances. The current network device warning banner contains 232 characters.

The standardized full warning banner text must be implemented as it appears in Figure 4.1-3.

You are accessing a U.S. Government system;

NO EXPECTATION OF PRIVACY - System use indicates consent to monitoring, recording, and auditing of activity; and

Unauthorized use is prohibited and subject to criminal, civil, security, or administrative proceedings and/or penalties.

Figure 4.1-3: Standardized Network Device Warning Banner

4.1.4 Standardized Guest Network Warning Banner

The standardized guest network warning banner must be used *only* for the NRC guest network and other public access NRC systems. The current guest network warning banner contains 1,201 characters. This standardized banner meets security and legal requirements for publicly accessible systems, and is not appropriate for systems within the NRC infrastructure network.

The standardized guest network warning banner text must be implemented as it appears in Figure 4.1-4.

USE OF THIS SYSTEM CONSTITUTES A CONSENT TO MONITORING, INCLUDING PORTABLE ELECTRONIC DEVICES.

The Nuclear Regulatory Commission (NRC) Guest Network provides limited Internet access to authorized NRC visitors who have been granted access by an NRC employee. The NRC Guest Network Access Services portal describes authorized use and access requirements.

Individuals accessing and using the Guest Networks do so at their own risk. Access and use of the Guest Network are subject to monitoring for maintenance, to preserve system integrity and security, and for other official purposes. You should not expect privacy, nor protection of privileged communication with your personal attorney, regarding information you create, send, receive, use, or store on this system. If monitoring reveals possible evidence of violation of criminal statutes, this evidence and any related information, including your identification, may be provided to law enforcement officials, including the Office of the Inspector General. Anyone who violates security regulations or makes unauthorized use of U.S. Government systems is subject to criminal , civil, security, or administrative proceedings and/or penalties.

UNAUTHORIZED ACCESS PROHIBITED BY LAW - TITLE 18 U.S. CODE SECTION 1030

Figure 4.1-4: Standardized Guest Network Warning Banner

4.2 Standardized Mandatory Notification and Consent Agreement

The “Standardized Mandatory Notification and Consent Agreement” must be incorporated in the system user agreement, which may also be referred to as the system Rules of Behavior (RoB), of any system deploying the standardized concise warning banner shown above in Figure 4.1-2, Standardized Concise Warning Banner. The consent agreement ensures that users of mobile devices and systems displaying the concise warning banner explicitly consent to the authorized terms of use prior to gaining access to devices.

Users must review and accept the terms of the “Standardized Mandatory Notification and Consent Agreement” at regular intervals.

The “Standardized Mandatory Notification and Consent Agreement” text must be implemented in the system user agreement as it appears in Figure 4.2-1. The system owner or designee must ensure that <System User Agreement Title> is replaced with the title of the system user agreement document.

STANDARDIZED MANDATORY NOTIFICATION AND CONSENT AGREEMENT FOR SYSTEM USER AGREEMENTS

By acknowledging the *<System User Agreement Title>* containing this agreement, users of Nuclear Regulatory Commission (NRC) information systems acknowledge and consent to the terms of the NRC Standardized Full Warning Banner:

I UNDERSTAND AND CONSENT TO THE FOLLOWING:

I am accessing a U.S. Government information system provided by the U.S. Nuclear Regulatory Commission (NRC) for U.S. Government-authorized use only, except as allowed by NRC policy. Unauthorized use of the information system is prohibited and subject to criminal, civil, security, or administrative proceedings and/or penalties.

USE OF THIS INFORMATION SYSTEM INDICATES CONSENT TO MONITORING AND RECORDING, INCLUDING PORTABLE ELECTRONIC DEVICES.

The Government routinely monitors communications occurring on this information system. I have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, the government may for any lawful government purpose monitor, intercept, search, or seize any communication or data transiting or stored on this information system.

Any communications or data transiting or stored on this information system may be disclosed or used in accordance with federal law or regulation.

REPORT ANY UNAUTHORIZED USE TO THE COMPUTER SECURITY INCIDENT RESPONSE TEAM (301-415-6666) AND THE INSPECTOR GENERAL.

All conditions stated above apply to all users accessing NRC information systems, regardless of whether the system displays a warning banner.

When a warning banner is used, the warning banner functions to remind the user of conditions set forth in this *Standardized Mandatory Notification and Consent Agreement*, regardless of whether the warning banner describes these conditions in full detail or provides a concise summary of conditions, and regardless of whether the warning banner expressly references this *Consent Agreement*.

CSO-STD-0040, *Warning Banner Standard,* is the official source of NRC warning banner language and guidance, and must be referred to for current warning banner language and direction.

Figure 4.2-1: Standardized Mandatory Notification and Consent Agreement

APPENDIX A. ACRONYMS

ADAMS	Agencywide Documents Access and Management System
ADM	Office of Administration
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CSO	Computer Security Organization
DISA	Defense Information Systems Agency
EO	Executive Order
GUID	Guidance
ISSO	Information System Security Officer
IT	Information Technology
ITI	Information Technology Infrastructure
LAN	Local Area Network
MD	Management Directive
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OCIO	Office of the Chief Information Officer
OGC	Office of the General Counsel
SGI	Safeguards Information
SITSO	Senior IT Security Officer
SP	Special Publication
STD	Standard
STIG	Security Technical Implementation Guide
SUNSI	Sensitive Unclassified Non-Safeguards Information
WAN	Wide Area Network

APPENDIX B. GLOSSARY

Concise Warning Banner	Banner suitable for mobile devices and systems (other than network devices) within the NRC infrastructure network which are unable to display the full warning banner due to system-imposed limitations.
Full Warning Banner	Banner suitable for desktops, laptops, and other devices within the NRC infrastructure network.
Guest Networks Warning Banner	Banner for use only on NRC guest networks and other public access NRC systems.
Network Device	A physical or virtual network device (e.g., firewalls, routers, switches, and other network appliances presented on NRC networks).
Network Device Warning Banner	Banner for use only on routers, switches, firewalls, and other appliances within the NRC infrastructure network, which provide a direct logon interface.
NRC Guest Networks	Untrusted networks that provide Internet access to NRC visitors who do not have permission to access the NRC network infrastructure systems. Isolated from NRC infrastructure networks to prevent users from accessing local resources and information.
NRC Infrastructure Networks	Trusted networks that allow NRC employees and contractors to store and process local IT resources and information.
NRC System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Trusted Network	Networks that employs sufficient hardware and software assurance measures to allow its use for processing SUNSI. For the purposes of this standard, NRC managed networks are the only trusted networks.
Untrusted Network	One category of restricted networks with limited security controls applied and an increased risk of information system compromise and breaches. Use of untrusted networks puts general laptops, information, and users at risk of possible compromise or breach due to an assumed lack of verified, effective network security controls.
Warning Banner	Written notices users encounter when authenticating to a system, before access to the system is established, which is also referred to as a “logon banner” or “notification and consent banner.”

CSO-STD-0040 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
3-Feb-17	1.0	Initial Release	OCIO internal Web page and SharePoint site. Will be distributed to the ISSO Forum after its signed.	As requested
7-Jan-19	1.0	Errata changes for document identifier and organizational changes.	Post to OCIO/CSO Web page.	N/A