Integrated Source Management Portfolio (ISMP) Rules of Behavior for Resident Application Users and the User Acknowledgment

The Integrated Source Management Portfolio (ISMP) Rules of Behavior (hereinafter Rules of Behavior) establish a set of rules that describe ISMP resident application user responsibilities and expected behavior with regard to information and system usage.

Applicability

The Rules of Behavior apply to all individuals who use the ISMP resident applications: the National Source Tacking System (NSTS), Web-Based Licensing (WBL), the License Verification System (LVS), and the Portfolio Enrollment Module (PEM).

Consequence for Noncompliance

The Rules of Behavior comply with the Rules of Behavior for all Nuclear Regulatory Commission (NRC) Automated Information System (AIS) Users provided in NRC Management Directive 12.5, "NRC Cybersecurity Program," Section IV. B (ML17278B085). The Rules of Behavior are to be followed by all ISMP resident application users. Users shall be held accountable for their actions on the ISMP resident applications. Non- compliance with the Rules of Behavior may subject the user to sanctions including, but not limited to, verbal or written warnings; removal of access to an ISMP resident application for a specific period of time or permanently; and/or prosecution under applicable Federal law consistent with the nature and the severity of the violation. NRC employees may also be subject to reassignment to other duties or termination. The Office of the Inspector General (OIG) is charged with the investigation of allegations of misconduct related to the misuse of ISMP resident applications, and ISMP management shall report all allegations of violations of the Rules of Behavior to the OIG.

General Protections

Users:

- Shall use the ISMP resident applications in accordance with procedures provided in each resident application User Guide.

- Shall only use the ISMP resident applications to perform authorized functions.

- Shall complete the security awareness training prior to using an ISMP resident application for the first time and annually thereafter. Also, users shall complete additional security awareness training as required by changes to the ISMP resident applications.

- Shall take appropriate precautions to protect ISMP resident application data, including securing output generated from the system (i.e., printed or digital reports, query results, other system output), from unauthorized access.

- Shall follow established procedures for requesting and disseminating information.

- Shall not attempt to bypass or circumvent security features within the ISMP resident applications.

- Shall immediately report anomalies and security incidents to the ISMP Helpdesk at 1-877-671-6787. Security incidents include attempted access by unauthorized individuals; violations of the Rules of Behavior; disclosure of sensitive information; loss of availability of the application; destruction of data; detection of malicious code or other compromise of the system; or unexplained system activity.

- Shall promptly follow the advice and direction of the ISMP Helpdesk in response to security incidents.

- Shall promptly report when no longer requiring access to ISMP resident applications to the ISMP Helpdesk at 1-877-671-6787.

Cryptography
Users:

- Shall only use browsers that are Federal Information Processing Standard (FIPS) 140-2 compliant with FIPS mode configurations as directed by the NRC Identity, Credential, and Access Management (ICAM) End User Subscriber Agreement.

Authenticators
Users:

- Shall use NRC ICAM-issued digital certificates stored on the ICAM-issued hard token or soft token OTP (One Time Password) to access ISMP. Tokens and digital certificates are personal identification number (PIN)-protected.

- Shall take reasonable measures to safeguard all authenticators (i.e., digital certificates, hard tokens, soft tokens, passwords, and PINs) including maintaining possession of individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately to the ISMP Helpdesk at 1-877-671-6787.

- Shall remove hard tokens from card readers when not in use and shall ensure that hard tokens are stored in a secure location, if applicable.

User Desktops and Laptops
Users:

- Shall logout of ISMP resident applications by clicking the logout link. This is especially important when using tabbed browsers to ensure maximum protection of data.

- Shall close internet browsers immediately after logging out of ISMP resident applications.

- Shall keep computers used to access ISMP resident applications current with the latest security patches and updates.

- Shall use anti-virus software on computers used to access ISMP resident applications and shall ensure that it is configured with the latest anti-virus updates/virus definition files.

- Shall take appropriate precautions to prevent the entry of malicious code into the ISMP environment, especially when using non-NRC furnished desktops and laptops; shall ensure that this equipment is configured with the latest anti-virus software to scan for malware of email and media (e.g., USB flash drives, CDs, etc.) before accessing them from equipment used to access ISMP resident applications.

- Shall either log off ISMP resident applications by clicking the logout link, or log off or lock the computer (for example, by using Ctrl-Alt-Delete) before leaving computers used to access ISMP resident applications unattended.

- Shall position computer monitors to prevent the viewing of sensitive data by unauthorized individuals.

- Shall ensure that the screen-saver password protection option on computers used to access ISMP resident applications is selected and that the wait time is set to 15 minutes.

Acknowledgement for the Integrated Source Management Portfolio (ISMP) Rules of Behavior for Resident Application Users

The ISMP Rules of Behavior must be reviewed and the Acknowledgment must be received in order for a user to be granted authorization to access any of the ISMP resident applications. Users will be prompted to acknowledge the ISMP Rules of Behavior upon the first login to the system and reviewed annually thereafter. If a user does not accept the Acknowledgment, then access will not be permitted to any ISMP resident application. Please keep a copy of the ISMP Rules of Behavior for reference.

By having reviewed these rules you are acknowledging your acceptance of the rules.