



U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

**THE NRC SENSITIVE UNCLASSIFIED NON-
SAFEGUARDS INFORMATION PROGRAM
(SUNSI)**

Russell A. Nichols

(301) 415-7169

RAN2@NRC.GOV

SUNSI DEFINITION

- “SUNSI” means any information of which the loss, misuse, modification, or unauthorized access can reasonably be foreseen to harm the public interest, the commercial or financial interests of the entity or individual to whom the information pertains, the conduct of NRC and Federal programs, or the personal privacy of individuals.

WHAT IS NOT SUNSI?

- Safeguards Information – Atomic Energy Act
- Classified National Security Information – Executive Order 12958 as amended by Executive Order 13292
- Non-sensitive Unclassified Information (public or suitable for public disclosure)

SEVEN SUNSI GROUPS

- Allegation Information
- Investigation Information
- Proprietary Information
- Privacy Act Information
- Security-Related Information
- Sensitive Internal Information
- Federal-, State-, Foreign Government-and International Agency Controlled Information

SUNSI TYPES FOR NRC SUBMITTERS

- Security-Related Information
- Proprietary Information
- Privacy Act and Personally Identifiable Information
- External Agency – Controlled Information

SECURITY-RELATED INFORMATION

- 10 CFR 2.390(d)(1) Information concerning physical or classified matter protection, material control and accounting program for special nuclear materials not otherwise designated as Safeguards information or classified as National Security Information or Restricted Data
- Licensee-submitted information that may qualify as Critical Infrastructure Information as defined by other agencies including –
 - Critical Energy Infrastructure Information (CEII) – Federal Energy Regulation Commission (FERC)
 - Sensitive Security Information (SSI) – Transportation Safety Administration (TSA)
- Information that could be useful, or could reasonably be expected to be useful, to a terrorist in a potential attack that does not qualify as Safeguards or Classified Information

PROPRIETARY INFORMATION

- Trade Secrets, Commercial or Financial Information
- Privileged or Confidential
- Competitive Harm
- 10 CFR 2.390 Requires Affidavit for Proprietary Submittals

PRIVACY ACT AND PERSONALLY IDENTIFIABLE INFORMATION (PII)

Information that can be used to identify or contact a person uniquely and reliably or can be traced back to a specific individual (i.e., a person's name *in conjunction with* any of the following information: relatives' names, home address, home email address, home or cellular telephone number, personal characteristics, Social Security number, date or place of birth, mother's maiden name, driver's license number, bank account information, credit card information, or any information that would make the individual's identity easily traceable). PII is protected to shield individuals from harm, embarrassment, inconvenience, identity theft, or other fraudulent use of personal information due to inappropriate disclosure.

EXTERNAL AGENCY – CONTROLLED INFORMATION

Information for which another Federal, State, Foreign Government or International Agency controls the marking, storage, transmission, dissemination and decontrol.

- Critical Energy Infrastructure Information (CEII) – Federal Energy Regulation Commission
- Sensitive Security Information (SSI) – Transportation Safety Administration
- Protected Critical Infrastructure Information (PCII) – Department of Homeland Security
- Unclassified Controlled Nuclear Information (UCNI) – Department of Energy
- Unclassified Naval Nuclear Propulsion Information (U-NNPI) – U.S. Navy

WHY PROTECT SUNSI?

- Protect the public from terrorist attack
- Protect individuals from unreasonable invasion of privacy
- Protect commercial entities from competitive harm

ACTIONS BEING TAKEN BY NRC TO PROTECT PII

- Encrypting PII on all mobile information technology (IT) devices – laptops, etc.
- Prohibiting removal of unredacted PII from NRC controlled space
- Prohibiting storage of PII on personally-owned computers, removable media, PDA's
- Prohibiting access to NRC IT systems with a dial-up modem unless using an NRC laptop that meets NRC security requirements
- Logging extracts of PII from IT systems to ensure accountability

ACTIONS BEING TAKEN BY NRC TO PROTECT PII (CONT.)

- Reviewing NRC contractors' uses of PII to ensure accountability
- Reviewing business practices to minimize collection and use of PII
- Reviewing all agency IT shared drives to remove PII or restrict access to PII
- Established a PII internal Web site with guidance and frequently asked questions
- Publishing a Regulatory Issue Summary (RIS) about PII

WHAT SUBMITTERS CAN DO TO CONTROL SUNSI

- Thoroughly screen documents submitted to NRC for SUNSI
- Mark documents with the appropriate header
- Portion mark pages containing SUNSI
- Cover letter for submittal containing SUNSI should clearly indicate the content of the SUNSI in the attached document(s)
- Cover letter itself should not bear SUNSI markings unless it incorporates SUNSI
- Consider potential for SUNSI in hidden text of electronic submissions

HOW TO MARK DOCUMENTS SUBMITTED TO THE NRC

- Mark the top of every page of a letter or document containing SUNSI
- Examples:
- “Security-Related Information – Withhold Under 10 CFR 2.390”
- “Personally Indentifiable Information – Withhold Under 10 CFR 2.390”
- “Proprietary Information – Withhold Under 10 CFR 2.390”

SUBMITTING BOTH PUBLIC AND NON-PUBLIC VERSIONS

- Both a public and non-public version of a document may be submitted
- Non-public version containing SUNSI should be marked appropriately
- Public version with SUNSI redacted should indicate information was withheld under 10 CFR 2.390.
- SUNSI can be segregated from the main document(s) and included only in an attachment to the submittal – mark the attachment with appropriate SUNSI marking – do not mark the main document

REFERENCES

- RIS 2005-26- Control of Sensitive Unclassified Non-Safeguards Information Related to Nuclear Power Reactors
<http://www.nrc.gov/reading-rm/doc-collections/gen-comm/reg-issues/2005/ri200526.pdf>
- RIS 2005-31- Control of Security-Related Sensitive Unclassified Non-Safeguards Information Handled by Individuals, Firms, and Entities Subject to NRC Regulation of the Use of Source, Byproduct, and Special Nuclear Material
<http://www.nrc.gov/reading-rm/doc-collections/gen-comm/reg-issues/2005/ri200531.pdf>
- **Coming Soon!** RIS 2007-XX- Personally Identifiable Information Submitted to the U.S. Nuclear Regulatory Commission

QUESTIONS?