

December 13, 2005

COMSECY-05-0061

MEMORANDUM TO: Chairman Diaz
Commissioner McGaffigan
Commissioner Merrifield
Commissioner Jaczko
Commissioner Lyons

FROM: Luis A. Reyes */RA/*
Executive Director for Operations

SUBJECT: INFORMATION SENSITIVITY OF THE NATIONAL SOURCE
TRACKING SYSTEM

The purpose of this memorandum is to inform the Commission that, after considering additional information since the original designation of the system's sensitivity, the staff's plans for the security categorization and protection of the information in the National Source Tracking System (NSTS) has remained the same. The NSTS and its data have been designated Security-Related Information (formerly, Official Use Only (OUO)), which is a category of the recently issued Sensitive Unclassified Non-Safeguards Information (SUNSI) guidance.

Based on the types of information in the NSTS, the sensitivity of the aggregated information, and NRC criteria for information sensitivity, the information in the NSTS has been considered OUO in the past. In accordance with the recently issued SUNSI guidance, staff consider the present classification to be Security-Related Information, SUNSI. The potentially sensitive information in the NSTS is the radioactive material, activity at manufacture, identifying information for sources, licensee name and address, and intent to transfer material or acknowledgment of receipt of material. Licensees are not required to protect OUO information. It is the equivalent of company proprietary information and licensees may share the information at their discretion. After being entered into the database, the information will have additional protections. Licensees will only have access to information concerning their own facilities. Access for other users will be limited to a need-to-know basis, which includes U.S. Nuclear Regulatory Commission (NRC) staff.

CONTACT: Paul Goldberg, NMSS/IMMS
(301) 415-7842

The Commission, and all stakeholders, were informed of the NSTS OUO designation in the Statement of Considerations of the proposed rule (i.e., SECY-05-0092). The Commission approved the proposed rule with that understanding. The proposed rule specifically invited comment on whether information protection under the OUO designation was adequate for the system. The staff received six comments on the issue. While commenters agreed that the data was sensitive, they did not recommend additional security provisions to protect the data. Commenters were opposed to making the information safeguards and noted that designation as Safeguards Information would be onerous to implement and could result in unintended restrictions on routine data. Commenters supported retaining the designation as OUO. Commenters stated concern over the security of the aggregated information and that additional protection measures should be taken. One commenter stated that the information should be excluded from public disclosure under 10 CFR 2.390. The information is considered exempt from disclosure under the Freedom of Information Act and the regulations in Part 2.390.

The new 10 CFR Part 73, "Safeguards Information Protection Requirements," provided to the Commission as a final rule (i.e., the publication of which the Commission disapproved in a November 1, 2005, Staff Requirements Memorandum (SRM), revised November 3, 2005, until the staff makes changes and renotices the rule) would not change the status of the NSTS data. However, the Commission, in the final SRM on Part 73, designated transportation information for Radioactive Material in Quantities of Concern (RAMQC) as Safeguards Information. The staff is concerned with the evolution of the Commission's position on the information categorization concerning RAMQC and how this may impact the information sensitivity in the NSTS.

The staff compared the compiled data to be in the NSTS to information in the orders requiring additional security measures issued to materials licensees. The attachments to those orders, setting out the required security measures, were designated Safeguards - Modified Handling, meaning that the information was considered to require protection but licensees did not need to provide the level of protection required by 10 CFR 73.21 for Safeguards Information for reactors and fuel cycle facilities. The attachments for the orders, including the order for RAMQC, contain information on physical security measures to be taken by materials licensees, making them analogous to Part 73.21 Safeguards Information for reactors and fuel cycle facilities. The NSTS will contain no information on physical security at sites or in transit.

The data to be included in the NSTS, taken individually or as a whole, do not meet the definitions of Safeguards Information in 10 CFR 73.2 or 73.21, even disregarding Part 73.21's application only to reactor and fuel cycle licensees. The staff does not believe that the information sensitivity in the NSTS needs to be altered. The NSTS Working Group, Steering Group, and Interagency Coordination Committee all considered the information sensitivity of NSTS data and decided that a designation stricter than OUO was not necessary. NSTS data do meet the definition of Security-Related Information, a category of SUNSI information:

"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."

The staff has developed requirements for the NSTS, and is presently in the process of selecting a contractor. The NSTS is designed to track transactions of radioactive sources of Categories 1 and 2, including origin (manufacture or import); transfer from one facility to another (shipment and receipt); and endpoints (disposal, decay, export, destruction). Potentially sensitive data on sources in the system will include radioactive material, activity at manufacture, and identifying information (manufacturer, model number, serial number). The system will also include the licensee's name and address (which may be, but is not necessarily, also the location of use of the material) and indication of transfer of material, either domestically or internationally, items that are also potentially sensitive and subject to withholding from public disclosure. NSTS will permit the NRC and other agencies to monitor the location and use of nationally tracked sources; conduct inspections; communicate nationally tracked source information to other government agencies; verify legitimate ownership and use of nationally tracked sources; and further analyze hazards attributable to the possession and use of these sources.

The requirements for the NSTS will provide a robust level of protection for the system. Therefore, the staff intends to protect information in the NSTS at the level of Security-Related Information, SUNSI, as has been planned to date. This is consistent with the Commission's direction for protection of sensitive unclassified information in the SRM for SECY-05-0101, dated October 7, 2005.

If the Commission wants the NSTS information sensitivity designation to be changed from Security-Related Information, SUNSI to Safeguards Information, then the staff would have to revise the current requirements to ensure that the system architecture would be designed to protect the system at the appropriate level. The Statement of Work for the contract would have to be rewritten to reflect the change and the associated increase in cost and time for system development. The staff would have to obtain approval from the Chairman for the new contract amount and issue a new Request for Quotations. The rulemaking would probably have to be rewritten and renoticed. The system's operation would be significantly delayed.

SECY please track.

cc: SECY
OGC
OCA
OPA
CFO