Process for Sharing Safeguards and Classified Information with Foreign Entities

It has been the policy of the U.S. Nuclear Regulatory Commission (NRC) to share safeguards information (SGI) with foreign regulatory counterparts or other foreign government organizations with whom NRC has signed an Arrangement of Cooperation (Arrangement) for the exchange of technical information and subsequently, with whom the Commission has approved staff to share SGI. The request for Commission approval is drafted following the receipt of a request for SGI from a foreign government entity with whom NRC has signed an Arrangement and is based on the Director, Office of International Programs (OIP), Net Advantage determination and a verification of need to know for the requested information. The OIP Director will coordinate with the program offices, as necessary. This is in accordance with COMSECY-04-0034 and Management Directive 12.2 (NRC Classified Information Security Program).

After it is determined that the requesting organization has a need to know, OIP will send a request to the Commission for permission to release the SGI, listing the information to be released, the timing of the proposed release, the recipient of the information, and the outcome of the OIP Director's Net Advantage determination. Once the Commission has approved the request to share SGI, no further approval is required for any other SGI information requests from that foreign entity for 5 years. However, OIP will notify the Commission of any additional SGI requests made by that entity prior to sharing additional information. That notification will be via an OIP Note from the Director, OIP, to the Commission. Once the 5-year period expires and if a new request is received from that foreign counterpart, OIP must again seek Commission approval prior to the sharing of SGI with that requesting foreign counterpart.

Prior to sharing information, OIP will coordinate with the Office of Nuclear Security and Incident Response (NSIR), Information Security Branch, to arrange a brief presentation to inform the intended recipient(s) of the information of the SGI protection requirements according to law and regulation. OIP will also gain assurance from the recipient's government organization that the representatives of that organization are qualified to receive sensitive and protected information.

NRC Management Directive 12.2 provides the criteria for the release of classified information to foreign governments. Specifically, there must be adequate assurances that the foreign government will properly protect and not disclose to third parties, or otherwise misuse the classified information. Generally, a government-to-government, general security-type agreement (administered by the Department of Defense) must be in place as well as an agency-to-agency level arrangement, which primarily spells out the administrative details to implement the classified information exchange.

Before classified information can be shared with one of NRC's foreign counterparts, an agreement for the exchange of classified information between the two parties must be signed and in place. Classified agreements are coordinated with and concurred on by NSIR, Information Security Branch, and the Office of the General Counsel (OGC). Once an agreement for sharing classified information is in place, the approval process for sharing that information is the same as that of SGI: coordination with NSIR and OGC, determination of Net Advantage by the OIP Director, and approval by the Commission, unless approval to share Classified information has been granted to the requestor within the last 5 years. If the Commission has provided approval to share classified information, within the last 5 years, OIP will make the required notification to the Commission, prior to sharing.

Enclosure

OIP will obtain appropriate access authorization from the foreign organization that the visitor(s) represents. Upon receipt, the names of the representatives of foreign governments who need access to classified information will be submitted to the NSIR Information Security Branch for the appropriate security checks and/or verification of security clearance.