2/12/02

EDO

MAJOR ACTIVITIES TO IMPLEMENT SHSI-REVIEW PROCESS

- Develop Plan and Schedule for Revising Public Determination Process
- Finalize the Revised SHSI Criteria
- Resolve Policy Issues that Need to be Addressed before Process can be Designed/Finalized
- Determine Scope of Documents Needing SHSI Review Before Release
- Document the Current Review Process
- Design & Implement Interim Process
- Provide Guidance to External Parties on Marking & Submission of SHSI Information
- Design & Implement Final Revised Process
- Update All Relevant Documentation/Procedures

DD-43

In addition to withholding information properly determined to be exempt from disclosure, such as classified, proprietary, privacy or safeguards information, you should **not** release information if its disclosure would be a clear and significant benefit to terrorists in a potential attack that would have a harmful impact on the government, public health and safety, and the nation's long-term economic prosperity. The information should be that which only the government controls or the licensee's have originated and control. You should consider limiting the release the following types of information:

1. Information related to the security of Government operations or assets. For NRC this includes information about:
   - building physical security
   - continuity of government plans
   - computer security measures for mission critical and business essential information technology systems.

2 Information about the ability of any element of the critical infrastructure of the United States to resist terrorist attacks or conduct that violates laws, harms interstate commerce, or threatens public health and safety. In so far as licensees are considered an element of the Nation's critical infrastructure, this would include security information related to protecting against the loss of control of radioactive material and include:
   - current inventories or throughput
   - site specific locations of material and vital equipment
   - specific security measures to control of the use and storage of licensed material
   - access controls and personnel clearance procedures
   - data clearly useful to defeat or breach key barriers

3 Information about **currently** viable assessment, projection, or estimate of the security vulnerability of any element of the critical infrastructure of the United States. In so far as licensees are considered an element of the Nation's critical infrastructure, information would encompass vulnerability assessments, security testing, risk audits, risk evaluations, and risk-management planning. Risk information would also include:
   - facility physical vulnerabilities or weaknesses
   - specific design and constructions details
   - specific accident analysis that reveal design details useful to defeat or breach key barriers

4. Information about currently applicable operational problems or solutions about security of any element of the critical infrastructure of the United States. In so far as licensees are considered an element of the Nation's critical infrastructure, this information would include:
   - current status of configuration of systems and equipment that could be used to determine facility vulnerabilities. (This does not include general conditions such as 100 percent power or shutdown)
   - currently uncorrected OSRE findings

Withholding of these types of licensee information would apply to only those nuclear facilities that have the potential for exceeding the specified levels of harm (to be defined). Elements of critical infrastructure, essential to the economy of the U.S., for NRC to consider include systems, facilities, and stockpiles essential for: telecommunications, electrical power, transportation, water supply, and public health.