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 not releasing 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 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 or breach of 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

With holding of these types of licensee information would apply to only those nuclear facilities that have the potential for exceeding the specified levels of harm.

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.

DD - 1

Working Definition

Information that:

1) is site specific,
2) was originated by the NRC or the licensee / ~~contractors, vendors~~
3) is not already classified or considered sensitive unclassified Safeguards Information
4) would provide a clear and significant benefit to a terrorist in carrying out an attack on an NRC-licensed facility

Discussion: OHS's definition of SHSI is more conservative that the NRC's current control of information. In fact, SHSI includes information that is outside of all of the NRC's four systems of information control: classified information, sensitive unclassified Safeguards Information (10 CFR 73.21), proprietary information (10 CFR 2.790(d)), and the as-yet unnamed new category of information discussed in the SRM dated January 25, 2002.

Protecting against terrorist attack requires a national scope; therefore, information should be treated as sensitive on a consistent basis across all infrastructure elements. OHS has satisfied that requirement by providing a definition of SHSI that spans all industries. It is imperative that all industries comply with the same definition. The NRC should closely examine the impact of releasing some information that OHS would consider withholding under SHSI. For example, what if NRC's guidance allowed release of the information about a particular licensed entity that OHS would withhold, and which OHS would require other, non-NRC, Federal agencies to withhold?

**Outline for Process and Interim Guidance for the Staff
on Release of Information to the Public**

- Information should present a **clear and significant benefit** to a terrorist in a potential attack

    What categories of documents would likely be included under this description? (All)

- Documents are currently widely available

    What does this constitute (Web, PDR, ADAMS, GPO, etc.?)
    Should we differentiate pre-9/11 from post-9/11? (All)

-

- Decisions to withhold information should be balanced with costs and benefits of withholding (NRR, NMSS, RES)

    What are resource implications (FTE, $$)?
    Is document legally required to be made public? (OGC to provide list, if possible)
    Would our strategic goals be adversely affected, i.e. public confidence?

- Alternative means provided for release of relevant information on important subjects to the public. Can it be redacted or rewritten? (NRR, NMSS, RES)

- Process instituted that provides for management review of withholding decisions, including designation of final decision maker. (OCIO)

    What is the current practice in each office?
    Can we use the management controls similar to those currently used for the web postings?
    How do we institute quality control?

- Which documents can we restore to the public domain **at this time** without final Commission decision (which documents comport w/ present version of SRM)

    OCIO to inform us of which categories of documents have been remove
    High priority documents include plant status report, performance indicators (ROP) web pages
    Documents that may have been deleted because they identified location of specific facilities

- Process for licensees to submit information that may be considered sensitive under the new criteria. What types of documents could be affected? Timing needs to be considered. Need to develop guidance to the staff first on how to handle/control such information. (NRR)