Guidance:

1) Information that has already been made widely available should not be withheld. Examples include Regulatory Guides, NUREGs, location of plants.
2) The staff should seek to identify what exemption from FOIA pertains to this category of information.
3) The staff should develop guidance on how this category of information will be shared with stakeholders but not be made available to the general public.

Problems:

1) The information must be equally shared among stakeholders, so no form of clearance would be required. On the other hand, this information would not be made publicly available, so the staff must consider with whom -- and how -- it will be shared while ensuring its limited distribution. (Note: Certain stakeholders have as operating assumptions that they will share all information they get with the public and media, e.g., NCI. Therefore, although NCI is a stakeholder and a significant player in the development of new requirements and guidance, can the information be shared with them?)

Revised Criteria

1. Information should be considered for withholding only if the release of the information could provide a clear and significant benefit to a terrorist in a potential attack. ~~There needs to be a clear nexus to aiding a potential terrorist in any information we withhold, and~~ that information **should** ~~has to~~ be information that only we and our licensees ~~control:~~ **have originated.** Information of a general nature **(i.e., generic security equipment or information and not site-specific details)** ~~or that is of marginal relevance~~ should not be withheld. **Similarly, information regarding the location of the plant, since such information is widely known already, should not be withheld.**

2. The NRC should not withhold information that ~~is already currently~~ **has already been made** widely available to the public, **such as NRC publications made available for general distribution.** ~~For example,~~ **However,** information that had been previously placed in the physical PDRs or previously on the NRC web page should not necessarily be considered **currently** ~~"currently~~ "widely available". ~~However, information currently available to the public via ADAMS or the web may be considered widely available.~~

3. Any decision to withhold information should be guided by a balancing of the costs and benefits of withholding. Among the considerations, the staff should examine whether release is needed to meet our strategic goals, including efficiently communicating with and informing the public, other stakeholders, States, or Tribal or local communities. If the balancing is uncertain the information should be released.

4. Any withholding of information should be narrow. **That is, partial redactions should be used whenever possible to avoid withholding entire documents.**

5. **The staff should seek alternative means for sharing sensitive information with stakeholders when the subject is a significant regulatory issue.** ~~Alternative means~~

~~should be provided for the release of relevant information on important public subjects in a fashion that would not provide significant assistance to a terrorist. The staff should be prepared to redact details or to rewrite important documents to eliminate sensitive information.~~

New

6. **The staff should develop guidance on how this category of information differs from proprietary information (protected under 10 CFR 2.790(d)) and sensitive unclassified Safeguards Information (protected under 10 CFR 73.21), including guidance on marking, handling, transmission, and storage.**

6. **There should be a process for management review of decisions to withhold information, when a review of that decision is requested by a stakeholder.** ~~The staff should develop a process that will involve management review of withholding decisions so as to ensure that the principles are applied in a uniform manner. The staff should identify a final decision maker if there is a difference of opinion as to whether something should be released to the public. The guidance should advise the staff to screen all incoming and outgoing documents for sensitivity for security reasons. Similarly, guidance should be developed as to how information that meets the stringent limits for non-disclosure is to be handled and protected. The staff should also develop a process for licensees to use to identify and submit documents that contain information that the staff would not release to the public under the guidelines.~~

7. In attempting to limit release of sensitive information, the staff should generally avoid providing information to one group of interested stakeholders, and not providing it to other interested stakeholders. **(see criteria 3 and 5, above)**

8. The staff must continue to comply with any obligation to release information that is required by law. For example, staff must release information that is subject to the Freedom of Information Act unless an exemption applies. The guidance does not alter the standards governing FOIA compliance.

9. The staff should work with OGC to explore a potentially more expansive view of section 147 safeguards information. The staff should ensure that safeguards information is consistently identified and secured.

10. In developing the revised criteria, the staff should ensure that it is consistent with any final guidance concerning the release of "sensitive homeland security information."

11. **In addition to the above general criteria, the staff should consider the following specific criteria in developing guidance:**
~~Although the guidance should be revised entirely in light of these general comments, observations on the specific proposed criteria are provided to illuminate the Commission's views on the application of these considerations to the specific proposals.~~

Criterion 1

12. Although it is possible that Emergency Plans might include information of interest to a terrorist, the need for such information by the public may require that it continue to be

publicly accessible. Acces to this type of information should not be unnecessarily restricted ~~and~~ **Information in the** Emergency Plan ~~information~~ that is **especially sensitive** ~~restricted~~ **and can be separated from the Emergency Plan without reducing the overall utility of the document** should be specifically justified and possibly reclassified as safeguards information.

13. Rather than withholding an entire Final Safety Analysis Report, it may be appropriate to hold back only certain sections containing information meeting the threshold for withholding. **(See discussion of redactions in Criterion 4, above.)**

14. The Commission is opposed to withholding physical protection and emergency planning performance indicators or inspection findings (except of course for the backup information on physical protection inspection findings which is safeguards information). Specifically, adverse OSRE findings that are promptly corrected, and a color finding in an OSRE, posted months after the OSRE, will make no plant more likely to be targeted.

15. ~~In order to achieve the narrowing of the withholding, this criterion could be revised along the lines of "Plant-specific information, entirely in NRC's and our licensees' control, that would clearly aid in planning an assault on a facility. An example might be drawings depicting the location of vital equipment within plant buildings."~~ **[Note: Emphasis on withholding only site-specific information (not generic security information) is discussed in criterion 1, above.]**

16. ~~There is no point in withholding information as to the specific location of a facility because this information is already widely known and is readily available from non-NRC sources. Attempting to withhold information that is known to the public would serve no purpose other than to breed suspicion.~~ **[Note: This thought has been merged with criterion 1, above.]**

17. ~~In order to achieve the narrowing of the withholding, this could be rewritten as "Physical vulnerabilities or weaknesses of nuclear facilities which would clearly be useful to terrorists, such as site specific security measures, access controls, or personnel clearance procedures."~~ **[Note: This thought is already captured in the "clear and significant benefit" phrase in Criterion 1.]**

18. In order to achieve the narrowing of the withholding, this could be revised by changing "could" to "clearly would", and "any" to "key."

19. Information such as to the quantities of nuclear material that are authorized to be possessed may be used for legitimate purposes and at the same time be of no use to a terrorist. For example, information concerning the types and quantities of material at a SDMP site may be of interest to the public, but pose no security concerns. Access to this type of information should not be unnecessarily restricted. **The staff should consider classifying the amount of HEU present at category 1 fuel cycle facilities.**

20. The amount of radioactive material authorized to a licensee is docketed information and generally appears on the license as a possession limit for most materials licensees. For nuclear power plants, one can calculate approximately how much material is in the reactor core and spent fuel pools.

21. ~~The staff should consider classifying the amount of HEU present at category 1 fuel cycle facilities~~. **[Note: Moved up to Criterion 19.]**

22. The staff should withhold information in any type of agency document (e.g., plant status report, press release) that provides the current status or configuration of systems and equipment that could be used to determine facility vulnerabilities if used by an adversary. This does not include general conditions such as 100 percent power or shutdown. **[Note: This thought should be raised to Criterion 1.]**

A Note About Consistency with SHSI

OHS defines Sensitive Homeland Security Information (SHSI) as

> "current information the public disclosure of which could be expected to have a harmful impact on the security of Federal operations or assets, the public health or safety of the United States or its residents, or the nation's long-term economic prosperity; which is not currently classified as national security information; and which consists of or reflects:
>
> (1) the ability of any element of the critical infrastructure of the United States to resist intrusion, interference, compromise, theft, or incapacitation by either physical or computer-based attack or other similar conduct that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;
>
> (2) any currently viable assessment, projection, or estimate of the security vulnerability of any element of the critical infrastructure of the United States, specifically including but not limited to vulnerability assessment, security testing, risk evaluation, risk-management planning, and risk audit; and
>
> (3) any currently applicable operational problem or solution regarding the security of any element of the critical infrastructure of the United States; specifically including but not limited to repair, recovery, redesign, reconstruction, relocation, insurance, and continuity."