March 21, 2002

NOTE TO: Vonna Ordaz

FROM: Dennis Gordon

SUBJECT: STAFF REVIEW OF DRAFT RESPONSE TO STAFF REQUIREMENTS MEMORANDUM CONCERNING WITHHOLDING SENSITIVE HOMELAND SECURITY INFORMATION FROM THE PUBLIC

The following comment regarding the Draft "Criteria To Be Used When Deciding Whether To Withhold Information From The Public" is provided.

As worded, criterion #2 and #4 describe information that is already determined to be Safeguards Information as defined by 10 CFR 73.21 and should be deleted as criteria for SHSI.

Recommend the following be added:

Since 9/11/01 the staff has applied a more vigorous review threshold to determining what is Safeguards Information (SGI) but still within the current guidelines of 10 CFR 73.21, such as location of [redacted]. With the introduction of Sensitive Homeland Security Information (SHSI), the staff believes that the NRC must establish a definitive boundary between what is SGI and what is SHSI. The staff understands that SHSI is of a lesser significance than SGI – and must still be released when requested under the provisions of FOIA. The staff believes that there is a potential for some overlap between these information sensitivity designations and believes a clear boundary must be established. The staff is also concerned that when compiled, more than one SHSI designated document could in fact satisfy the criteria for SGI. The staff has begun reviewing these issues as well as a review of current 10 CFR 73.21 requirements to determine if adjustments are needed.

Ex. 2 protection

Ex. 5

Recommend the following **"bolded"** editorial changes be made:

First three bullets: N/A

The NRC staff should always withhold information **determined to be:**
Privacy Act Information as described by the Privacy Act of 1974
Proprietary Information as described by 10 CFR 2.790
Safeguards Information as described by 10 CFR 73.21
Classified Information as described by 10 CFR Part 95

In addition, **the NRC staff** should **also withhold** information **which does not otherwise satisfy the criteria for Privacy Act Information, Proprietary Information, Safeguards Information, or Classified Information but which satisfies** one or more of the following criteria:

1. Plant-specific information **possessed by the** NRC, licensees, **or contractors** that would clearly aid **the development of strategic concepts for use in** planning an assault on **an NRC licensed** facility. **For example,** drawings depicting the location of **necessary** safety equipment within plant buildings, portions of Final Safety Analysis Reports, and Individual Plant Examination material.

Ex. 5

99-10

2. Site-specific information regarding physical or procedural conditions which could clearly be exploited by an adversary to prevent, delay, or interfere with a licensee's ability to respond to, or mitigate, the consequences of adversary activities. For example, site specific security program implementation practices, access controls, personnel clearance procedures, and the specific location and [Ex. 2

3. Site-specific construction details, such as wall thicknesses, dimensions of physical barriers, detailed nuclear facility diagrams, schematics, or cutaways where such information would be of clear and significant benefit to an adversary. Where appropriate, general descriptions instead of exact numbers (i.e., "several feet, several inches, layers of concrete") should be used for general public information.

4. Information which clearly would be useful to defeat a significant component of a licensee security or safety system the loss of which would prevent, delay, or interfere with a licensee's ability to respond to or mitigate the consequences of adversary activities at nuclear facilities.

5. Information in any type of 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.

ADD:

6. Information possessed by the NRC, licensees, or contractors that by itself does not satisfy the criteria stated above but when combined with any known and previously released information would expose a specific vulnerability or weakness of a nuclear facility as otherwise described above, and would clearly be useful to an adversary to prevent, delay, or interfere with a licensee's ability to respond to or mitigate the consequences of adversary activities. For example, a document that identifies a specific water source needed to mitigate the consequences of a specific accident where the identified accident scenario has been previously released as part of an earlier Emergency Preparedness Exercise scenario.

7. Employment or personnel records that do not satisfy the criteria for Privacy Act Information or Proprietary Information but nonetheless would reveal response force size, posts, duties, or weapons that would clearly be of use in planning an assault on an NRC licensed facility.

8. Licensee event reports that have not been analyzed for sensitivity against any of the above criteria.

General categories of information that may now be released:

Performance Indicators.
Inspection findings **that do not otherwise reveal information which satisfies any of the above criteria.**
Corrected OSRE findings.
Plant Status Report (minus "reasons and comments" column).
Specific locations of licensed facilities.
Generic technical or maintenance information common to all power reactors that can be easily gained by a knowledgeable individual without additional site-specific information.
Petitions submitted by members of the public under the provisions of 10 CFR 2.206.

SAFEGUARDS INFORMATION (SGI) 10 CFR 73.21	SENSITIVE HOMELAND SECURITY INFORMATION (SHSI) (Note: Extracted from Homeland Security Vertical Information Sharing Initiative)
(a) General performance requirement. Each licensee who	**This initiative is not predicated on** the development of a massive data warehouse but rather **the creation of exchange networks.**
(1) possesses a formula quantity of strategic special nuclear material, or	
(2) is authorized to operate a nuclear power reactor, or	
(3) transports, or delivers to a carrier for transport, a formula quantity of strategic special nuclear material or more than 100 grams of irradiated reactor fuel, and each person who produces, receives, or acquires Safeguards Information shall ensure that Safeguards Information is protected against unauthorized disclosure.	
To meet this general performance requirement, licensees and persons subject to this section shall establish and maintain an information protection system that includes the measures specified in paragraphs (b) through (i) of this section.	Regulations, policy, and budget allocations must be developed and implemented to support this initiative.
Information protection procedures employed by State and local police forces are deemed to meet these requirements.	
(b) Information to be protected. The specific types of information, documents, and reports that shall be protected are as follows:	The Chief Information Officer (CIO) within each agency shall be responsible for identifying and designating all information, including information in electronic form, that warrants protection as SHSI. He or she may delegate the authority to reviewing officials on a limited basis as needed to implement these guidelines.
(1) Physical protection at fixed sites. Information **not otherwise classified as Restricted Data or National Security Information** relating to the protection of facilities that possess formula quantities of strategic special nuclear material, and power reactors. Specifically:	"Sensitive Homeland Security Information (SHSI)" means **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:
(i) The composite physical security plan for the nuclear facility or site.	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;**

(ii) Site specific drawings, diagrams, sketches, or maps that substantially represent the final design features of the physical protection system.	
(iii) Details of alarm system layouts showing location of intrusion detection devices, alarm assessment equipment, alarm system wiring, emergency power sources, and duress alarms.	
(iv) Written physical security orders and procedures for members of the security organization, duress codes, and patrol schedules.	
(v) Details of the on-site and off-site communications systems that are used for security purposes.	
(vi) Lock combinations and mechanical key design.	
(vii) Documents and other matter that contain lists or locations of certain safety-related equipment explicitly identified in the documents as vital for purposes of physical protection, as contained in physical security plans, safeguards contingency plans, or plant specific safeguards analyses for production or utilization facilities.	
(viii) The composite safeguards contingency plan for the facility or site.	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.
(ix) Those portions of the facility guard qualification and training plan which disclose features of the physical security system or response procedures.	
(x) Response plans to specific threats detailing size, disposition, response times, and armament of responding forces.	
(xi) Size, armament, and disposition of on-site reserve forces.	
(xii) Size, identity, armament, and arrival times of off-site forces committed to respond to safeguards emergencies.	
(xiii) Information required by the Commission pursuant to 10 CFR 73.55 (c) (8) and (9).	
(2) Physical protection in transit. Information not otherwise classified as Restricted Data or National Security Information relative to the protection of shipments of formula quantities of strategic special nuclear material and spent fuel. Specifically:	

(i) The composite transportation physical security plan.	
(ii) Schedules and itineraries for specific shipments. (Routes and quantities for shipments of spent fuel are not withheld from public disclosure. Schedules for spent fuel shipments may be released 10 days after the last shipment of a current series.)	
(iii) Details of vehicle immobilization features, intrusion alarm devices, and communication systems.	
(iv) Arrangements with and capabilities of local police response forces, and locations of safe havens.	
(v) Details regarding limitations of radio-telephone communications.	
(vi) Procedures for response to safeguards emergencies.	
(3) Inspections, audits and evaluations. Information not otherwise classified as National Security Information or Restricted Data relating to safeguards inspections and reports. Specifically:	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;**
(i) Portions of safeguards inspection reports, evaluations, audits, or investigations that contain details of a licensee's or applicant's physical security system or that disclose uncorrected defects, weaknesses, or vulnerabilities in the system. Information regarding defects, weaknesses or vulnerabilities may be released after corrections have been made. Reports of investigations may be released after the investigation has been completed, unless withheld pursuant to other authorities, e.g., the Freedom of Information Act (5 U.S.C. 552).	Designating Officials must ensure that the threat, vulnerability, or risk associated with a critical infrastructure is current before designating information pertaining to it as SHSI.
(4) **Correspondence.** Portions of correspondence insofar as they contain Safeguards Information specifically defined in paragraphs (b)(1) through (b)(3) of this paragraph.	Designating Officials shall ensure that information is of current significance, i.e., is not out-of-date, before designating it as SHSI.
(c) **Access** to Safeguards Information.	**"Need-to-Know"** means a determination made by an authorized holder of SHSI that a prospective recipient requires access to that SHSI in order to perform or assist in a lawful and authorized governmental function.
(1) Except as the Commission may otherwise authorize, no person may have access to Safeguards Information unless the person has an established "need to know" for the information and is:	Routine access to SHSI may, unless prohibited by law, be provided to the following persons who have a demonstrated need-to-know:

(i) An employee, agent, or contractor of an applicant, a licensee, the Commission, or the United States Government. However, an individual to be authorized access to Safeguards Information by a nuclear power reactor applicant or licensee must undergo a Federal Bureau of Investigation criminal history check to the extent required by 10 CFR 73.57;	(a) A Federal government employee;
(ii) A member of a duly authorized committee of the Congress;	(b) an employee of a Federal government contractor, licensee, or grantee;
(iii) The Governor of a State or designated representatives;	(c) A member of Congress or a congressional staff member;
(iv) A representative of the International Atomic Energy Agency (IAEA) engaged in activities associated with the U.S./IAEA Safeguards Agreement who has been certified by the NRC;	(d) State and local government employees; and
(v) A member of a state or local law enforcement authority that is responsible for responding to requests for assistance during safeguards emergencies; or	(e) Individuals directly involved in the operation, maintenance, or protection of any element of critical infrastructure.
(vi) An individual to whom disclosure is ordered pursuant to Section 2.744(e) of this chapter.	SHSI may not be disclosed or disseminated outside the Federal government except to those individuals authorized for routine access in Sec. 2.2. SHSI may be shared with such individuals only when they have a need-to-know and they agree to abide by the access limitations and protection requirements set forth in this document.
(2) Except as the Commission may otherwise authorize, no person may disclose Safeguards Information to any other person except as set forth in paragraph (c)(1) of this section.	FOIA requests for access to SHSI should be processed in accordance with the Attorney General's FOIA Memorandum of October 12, 2001, with consideration of all applicable FOIA exemptions, including one or more of the following: (a) For SHSI pertaining to Federal government operations or assets, agencies should consider applying FOIA Exemption 2. (b) For current SHSI consisting of private-sector or industry information submitted voluntarily to the Government that is customarily protected by the submitter, agencies should consider applying FOIA Exemption 4. (c) For any SHSI the disclosure of which is barred by Federal statute, agencies should consider applying FOIA Exemption 3. (d) For any SHSI that consists of information copiled for law enforcement purposes, agencies should consider applying FOIA Exemption 7.
(d) **Protection** while in use or storage.	

(1) While in use, matter containing Safeguards Information shall be under the control of an authorized individual.	The proper use and handling of SHSI must be reflected in all agency security programs and plans required by the Government Information Security Reform Act of 2000 and implementing policy. Such programs and plans shall provide for the protection of any information designated as SHSI by a third agency. SHSI requires protection commensurate with the risk and magnitude of harm that would result from unauthorized dissemination and must be controlled with a high degree of care consistent with that accorded other types of unclassified but sensitive information, such as proprietary business information, personnel or medical records, and attorney-client information.
(2) While unattended, Safeguards Information shall be stored in a locked security storage container. Knowledge of lock combinations protecting Safeguards Information shall be limited to a minimum number of personnel for operating purposes who have a "need to know" and are otherwise authorized access to Safeguards Information in accordance with the provisions of this section.	During working hours reasonable steps should be taken to minimize the risk of access by unauthorized personnel. After working hours, SHSI should be stored in a secure container, such as a locked desk or file cabinet, or in a facility where Government or Government-contract security is provided.
(e) **Preparation and marking of documents.** Each document or other matter that contains Safeguards Information as defined in paragraph (b) in this section shall be marked "Safeguards Information" in a **conspicuous manner** to indicate the presence of protected information (portion marking is not required for the specific items of information set forth in paragraph Section 73.21(b) other than guard qualification and training plans and correspondence to and from the NRC). Documents and other matter containing Safeguards Information in the hands of contractors and agents of licensees that were produced more than one year prior to the effective date of this amendment need not be marked unless they are removed from storage containers for use.	Documents or information in any form designated as SHSI shall be marked in a **conspicuous manner** with the following notice: ***"Sensitive Homeland Security Information Disseminate on a Need-to-Know Basis Only"***
(f) **Reproduction and destruction** of matter containing Safeguards Information.	
(1) Safeguards Information may be reproduced to the minimum extent necessary consistent with need without permission of the originator.	A document or material containing SHSI may be reproduced to the minimum extent necessary consistent with the need to carry out official duties, provided that the reproduced material is marked and protected in the same manner as the original materials.
(2) Documents or other matter containing Safeguards Information may be destroyed by any method that assures complete destruction of the Safeguards Information they contain.	Material containing SHSI may be disposed of by any method that reasonably prevents unauthorized retrieval (provided that the disposal has been authorized by the Archivist of the United States).

(g) External **transmission** of documents and material.	
(1) Documents or other matter containing Safeguards Information, when transmitted outside an authorized place of use or storage, shall be packaged to preclude disclosure of the presence of protected information.	Documents containing SHSI may be transmitted by U. S. First Class, Express, Certified, or Registered mail.
(2) Safeguards Information may be transported by messenger-courier, United States first class, registered, express, or certified mail, or by any individual authorized access pursuant to Section 73.21(c).	
(3) Except under emergency or extraordinary conditions, Safeguards Information shall be transmitted only by protected telecommunications circuits (including facsimile) approved by the NRC. Physical security events required to be reported pursuant to Section 73.71 are considered to be extraordinary conditions.	Except in emergency situations, electronic communication of SHSI outside a Federal agency should take place via secure network, such as Law Enforcement On-Line (LEO) or the Regional Information Sharing System (RISS), both operated by the Department of Justice.
(h) Use of **automatic data processing (ADP) systems.** Safeguards Information may be processed or produced on an ADP system provided that the system is self-contained within the licensee's or his contractor's facility and requires the use of an entry code for access to stored information. Other systems may be used if approved for security by the NRC.	SHSI may be processed or produced on any information system that fully complies with the requirements of the Government Information Security Reform Act of 2000, implementing policy, and Office of Management and Budget Circular No. A-130, Appendix III, "Security of Federal Automated Information Systems;" or any system that is certified for the processing of classified national security information.
(i) **Removal from Safeguards Information category.** Documents originally containing Safeguards Information shall be removed from the Safeguards Information category whenever the information no longer meets the criteria contained in this section.	Designating Officials shall ensure that information is of current significance, i.e., is not out-of-date, before designating it as SHSI. **Information shall not remain protected as SHSI when it ceases to be of current significance** in relation to the critical infrastructure to which it pertains. Information ordinarily should remain protected as SHSI for no longer than 10 years, unless a designating official makes a new determination that protection is warranted for a longer period.
	SHSI Provisions in Contracts. Each agency shall include in all appropriate contract vehicles specific SHSI handling requirements as part of the security provisions required for all government contractors.