POLICY ISSUE
(Notation Vote)

May 18, 2005 SECY-05-0091

FOR: The Commissioners

FROM: Karen D. Cyr
General Counsel /RA/

Luis A. Reyes
Executive Director for Operations /RA/

SUBJECT: TASK FORCE REPORT ON PUBLIC DISCLOSURE OF SECURITY-RELATED INFORMATION

PURPOSE:

To obtain Commission approval of Task Force recommendations.

DISCUSSION:

In a Staff Requirements Memorandum dated March 22, 2005, the Commission directed that a task force with representatives from the Office of the General Counsel and the Executive Director for Operations be established to review the application of the Freedom of Information Act (FOIA) to security-related information, such as that contained in the recent National Academy of Sciences (NAS) report entitled, "Safety and Security of Commercial Spent Nuclear Fuel Storage." The Commission sought to ensure that NRC strikes the appropriate balance between making information publicly available and withholding information for homeland security reasons. The Commission expressed a particular interest in the extent to which information may be withheld from public disclosure under a compilation or mosaic approach applied to either Safeguards Information or sensitive unclassified information. The Commission also requested the task force to address lessons learned from the discussions with the NAS regarding the public release of the spent nuclear fuel storage report by that body.

The attached task force report sets forth the legal framework governing disclosure of security-related information under the FOIA, explains the relationship between Sensitive Information Screening Project (SISP) reviews and FOIA reviews, proposes additional guidance for NRC staff on implementation of FOIA that could be included in a forthcoming revision to Management Directive 3.1, "Freedom of Information Act," and discusses lessons learned regarding the protection of information resulting from the NAS Study experience.

CONTACT: Catherine M. Holzle, OGC
415-1560

The Commissioners

RECOMMENDATIONS:

The task force recommends:

1. That the staff ensure that all agency records within the purview of 5 U.S.C. 552(a)(2), the mandatory disclosure provision of the Freedom of Information Act, are promptly made available to the public via the Publicly Available Records System (PARS) soon after the records are generated.

2. That to the extent practicable, any documents withheld under the SISP criteria should likely be withholdable under FOIA, either in whole or in part.

3. That the SISP reviews be carefully done so information made available to the public as a matter of administrative discretion does not include sensitive information that the agency would withhold if requested under FOIA.

4. That the Commission endorse the standards for withholding security-related information under FOIA set forth in the attachment to this report and that those standards be incorporated into Management Directive 3.1, Freedom of Information Act.

5. That when the NRC requests that external organizations produce documents under NRC contract, grant or other agreement containing classified information, or sensitive unclassified information (including Safeguards Information), controls over information disclosure are clearly articulated in the document that describes the work to be performed.

/RA/
Karen D. Cyr
General Counsel

/RA/

Luis A. Reyes
Executive Director
for Operations

Attachment: Task Force Report on Public Disclosure of Security-Related Information

The Commissioners

RECOMMENDATIONS:

The task force recommends:

1. That the staff ensure that all agency records within the purview of 5 U.S.C. 552(a)(2), the mandatory disclosure provision of the Freedom of Information Act, are promptly made available to the public via the Publicly Available Records System (PARS) soon after the records are generated.

2. That to the extent practicable, any documents withheld under the SISP criteria should likely be withholdable under FOIA, either in whole or in part.

3. That the SISP reviews be carefully done so information made available to the public as a matter of administrative discretion does not include sensitive information that the agency would withhold if requested under FOIA.

4. That the Commission endorse the standards for withholding security-related information under FOIA set forth in the attachment to this report and that those standards be incorporated into Management Directive 3.1, Freedom of Information Act.

5. That when the NRC requests that external organizations produce documents under NRC contract, grant or other agreement containing classified information, or sensitive unclassified information (including Safeguards Information), controls over information disclosure are clearly articulated in the document that describes the work to be performed.

Karen D. Cyr
General Counsel

Luis A. Reyes
Executive Director
for Operations

Attachment: Task Force Report on Public Disclosure of Security-Related Information

cc:

EDO	NRR	NMSS	SECY
OPA	CFO	OCA	IG
NSIR	OIP	OCM/DOC	OIS

G:\LC\Holzle\Secy Task Force Pkg.wpd

OFFICE	OGC	OGC	OGC	OIS	EDO
NAME	CHolzle/RA/	TRothschild/RA/	KCyr/RA/	EBaker/RA/	LReyes/RA/
DATE	5/ 7 /2005	5/ 17 /2005	5/ 18 /2005	5/ 17 /2005	5/ 18 /2005

REPORT ON PUBLIC DISCLOSURE OF SECURITY-RELATED INFORMATION

Task Force Members:

Catherine Holzle, Senior Attorney, Office of the General Counsel
Carol Ann Reed, FOIA/Privacy Act Officer, Office of Information Services
Trip Rothschild, Assistant General Counsel, Chair
Lynn Silvious, Chief Information Security Section, Office of Nuclear Security and Incident Response

Task Force Report

INTRODUCTION

Historically, the Nuclear Regulatory Commission (NRC) has made routinely available to the public large amounts of information, more than required by law. In the post-September 11, 2001 environment, however, like many other agencies, the NRC has found it necessary to be more judicious in what it voluntarily releases, so as not to inadvertently provide assistance to those who might use the information for malevolent acts. It was in this context that the Commission reviewed the National Academy of Sciences' (NAS) report entitled, "Safety and Security of Commercial Spent Nuclear Fuel Storage" for sensitive information. In the course of developing its views on this report, the Commission directed the establishment of a task force, comprised of representatives of the Offices of the General Counsel and the Executive Director of Operations, to examine aspects of the Commission's information disclosure policies.

The Commission requested the task force to make recommendations regarding the application of Freedom of Information Act (FOIA) exemptions to security-related information with the aim of ensuring that the NRC strikes the appropriate balance between making information publicly available and withholding information for homeland security reasons. The Commission expressed particular interest in the extent to which information could be withheld from public disclosure under FOIA exemptions pursuant to judicially-sanctioned "compilation" or "mosaic" principles which permit, in limited circumstances, the withholding of information that would not, in isolation, be exempt from disclosure. The Commission also called for the task force, using lessons learned from the NRC's recent information disclosure reviews of the NAS report and the NRC's report to Congress on the NAS report, to recommend the standards for review of future security-related reports developed by or for the NRC, with a view towards ensuring that these standards provide transparency of the staff's process for identifying information appropriately exempt from FOIA disclosure.

The task force has reviewed the applicable statutes, judicial case law, and Commission policy guidance, and discussed pertinent case law with the Office of Information and Privacy of the Department of Justice (DOJ OIP), which has responsibility for coordinating FOIA policy government-wide. The task force has concluded that the Commission has considerable authority to withhold from public disclosure information that could be useful, or could reasonably be expected to be useful, to a terrorist, provided that the information is not readily available to the public already. Since it is generally difficult to defend withholding records under FOIA when the information is widely available to the public, the NRC developed guidance several months ago for conducting a broad security/sensitivity review under the Sensitive Information Screening Project (SISP) to assess whether documents should be made publicly available in the first instance as a matter of administrative discretion. Prior to September 11, 2001, the NRC automatically placed much of the agency's information in the Publicly Available Records System (PARS), without consistent scrutiny for sensitivity or consideration whether release of the information raised any significant concerns about usefulness for terrorist activity. (This is the official name of the public version of ADAMS, the agency's official records management system.)

It is imperative that SISP reviews be carefully performed so that sensitive unclassified information that should be withheld is not inadvertently made available to the public. However, legal considerations in many cases do not dictate whether particular information may or should be withheld. While the law mandates the withholding of classified national security information, Restricted Data, and Safeguards Information, the decision as to whether other information requested under FOIA will be released to the public must be made on a case-by-case basis, with the disclosure decisions in many cases largely driven by technical or security policy considerations. The question of whether public disclosure of information could increase threats to homeland security is often a matter of judgment based on a full understanding of the technical issues underlying the determination, including consideration of such factors as the nature of the threat, the likelihood of harm or degree of risk posed by the public disclosure of the information and the relative usefulness of the information towards accomplishing the potential harm, balanced against whether the benefit to the public from the release of the information would outweigh the security threat. For example, release of information about evacuation routes in a nuclear emergency could be of use to terrorists, but withholding the information from the public may render the emergency plan ineffective for protecting the public.

Thus, independent determinations must be made in each instance after weighing pertinent considerations. The Commission has given the staff some policy guidance on the standards governing information disclosure. Timely processing of FOIA requests, the completion of SISP reviews, and the conduct of agency adjudications would be greatly aided if the Commission gave the staff additional guidance on several issues. The NRC staff is now preparing a paper for Commission review setting forth those issues, and proposing revised SISP disclosure policies. While as noted above, technical and security policy considerations are frequently paramount, we begin with an examination of the legal principles governing disclosure.

MANDATORY DISCLOSURE

Under the FOIA, 5 U.S.C. 552(a)(2), the NRC is required to make available for public inspection and copying:

> (1) final opinions, including concurring and dissenting opinions, as well as orders, made in the adjudication of cases;
>
> (2) statements of policy and interpretations which have been adopted by the agency and are not published in the Federal Register;
>
> (3) administrative staff manuals (*e.g.*, NRC's Management Directives, Inspection and Enforcement Manuals, Regulatory Guides) and instructions to staff that affect a member of the public; and
>
> (4) copies of all records, which have been released to the public pursuant to a FOIA request, and which, because of the nature of the subject matter, the agency determines have become or are likely to become the subject of subsequent FOIA requests for substantially the same records; and

(5) a general index of the documents covered under (4) above.

All records created on or after November 1, 1996, that fall within the five categories above must be made available to the public electronically. In enacting subsection 552(a)(2), Congress sought to preclude agencies from creating "secret law," so that the public would know "agency law" and be able to act in accordance with it. The NRC does have the authority to withhold from the public portions of 552(a)(2) records that are exempt from disclosure under FOIA. *See* discussion of pertinent case law on withholding that information in DOJ OIP's Freedom of Information Act Guide & Privacy Act Overview at pp. 23-24 (May 2004 edition) (hereinafter referred to as the "FOIA Guide.") Pursuant to this authority, the NRC, for example, does not release portions of adjudicatory orders that contain Safeguards Information or proprietary information.

In general, under 5 U.S.C. 552(a)(2) the NRC is not required to make available to the public records that have no precedential value and do not constitute the working law of the agency. By the same token, documents that have the force and effect of law must be disclosed.

SISP REVIEWS

The Commission has long had an established policy of openness, traditionally making broad categories of documents available far beyond 552(a)(2) requirements or what would be required to be released in response to a FOIA request. Shortly after September 11, 2001, the Commission temporarily shut down PARS and removed documents that contained sensitive information that could be useful to terrorists. With a revised perspective on how its policy of openness could be exploited for malevolent purposes, the Commission reassessed its information disclosure policies and directed the agency to employ judicious use of sensitivity criteria. That policy direction was informed, although not governed, by consideration of what information would be disclosed in response to a valid FOIA request. On October 25, 2004, the NRC again shut down PARS to remove additional documents. As part of this effort to reconsider what information would voluntarily be made public, the Commission directed the NRC staff, through the SISP initiative, to screen documents to ensure that they did not contain sensitive information before making them publicly available via PARS.

The agency has wide discretion under the SISP initiative in determining whether information it generates will be released as a matter of administrative discretion. The only governing legal standard is that information that must be released pursuant to 5 U.S.C. 552(a)(2), discussed above, must be promptly disclosed. Generally, in conducting a SISP review, the staff judges whether the document as a whole will be withheld at the outset, based on the inclusion of some sensitive information, or voluntarily disclosed in the entirety as non-sensitive. The staff, in fact, has not been conducting FOIA-type reviews to carry out its SISP screening. Under SISP, if sensitive content is identified, the document is not placed in the PARS. Of course, this approach does not satisfy the requirements of FOIA. If a FOIA request is received for a record, the agency is required to conduct a line-by-line review and may only withhold material that is protectable under one or more of the FOIA exemptions. Thus, at a minimum, the two

reviews differ in approach, if not criteria: for SISP, either the entire document is made available or it is not; for FOIA, all reasonably segregable material that is not exempt under the statute must be disclosed.

The SISP review criteria being used for nuclear power reactor-related documents (approved by the Commission in a November 9, 2004 SRM on SECY 04-0191, "Withholding Sensitive Unclassified Information Concerning Nuclear Power Reactors from Public Disclosure") include examples of the types of sensitive information that would be withheld under a FOIA request, if in conducting an informed review the NRC determined that disclosure of the information would be harmful. The SISP criteria for nuclear materials-related information that are being applied today are being refined, and revised criteria will be presented for Commission review and approval in the coming weeks. The task force's expectation is that those revised criteria will also be generally consistent with FOIA withholding criteria.

FOIA REVIEWS

Once a FOIA request for a document is received, a SISP review is no longer adequate, since under FOIA, the release determination is not limited to whether to withhold a document in its entirety. The Supreme Court has called FOIA a statute whose basic purpose reflects a philosophy of full agency disclosure unless information falls under one of the nine clearly delineated statutory exemptions. *Department of Air Force v. Rose*, 425 U.S. 352 (1976). In that opinion, the Court further asserted that "these limited exemptions do not obscure the basic policy that disclosure, not secrecy, is the dominant objective of the Act." *Id*. at 361. The task force emphasizes that, although the Commission has moved, since September 11, 2001, towards greater restrictions on public release of information that might aid persons intending harm to the United States, Congress has not modified or extended the FOIA exemptions. Accordingly, the Commission is still required to disclose information within the scope of a FOIA request unless one or more of the nine exemptions applies. The scope of the exemptions is amplified in the many judicial decisions interpreting the Act. The exemptions that govern withholding of security-related information are briefly described below.

1. Exemption 1–National Security Information

Exemption 1 mandates the withholding of information meeting standards set forth by an Executive Order to be kept secret in the interest of national defense or foreign policy and that have in fact been properly classified pursuant to that Executive Order. Unauthorized disclosure of such information is subject to criminal sanctions. Currently, classification decisions are governed by criteria set forth in Executive Order 12958, initially issued by President Clinton on April 17, 1995, but amended several times subsequently. Some NRC security-related information, particularly information pertaining to the security of fuel cycle facilities possessing strategic quantities of special nuclear material, has long been classified as national security information. NRC staff is well versed in applying the classification criteria set forth in Executive Order 12958, as amended.

The NRC may classify more security-related information over time, as the recently amended Executive Order permits the classification of information (a) pertaining to United States Government programs for safeguarding nuclear materials or facilities or (b) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism, provided unauthorized disclosure of the information could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

Information classified pursuant to the applicable Executive Order or the Atomic Energy Act should be referred to as "classified information." While Restricted Data is properly referred to as classified information, it is classified under the Atomic Energy Act rather than Executive Order, so the legal basis for withholding is Exemption 3, which requires a separate statutory authority for withholding, rather than Exemption 1, which relies on the classification Executive Order. All other security-related information, including Safeguards Information, is sensitive unclassified information and should not be referred to as classified information, although Safeguards Information is likewise required to be withheld from public disclosure (pursuant to Exemption 3, inasmuch as it is rooted in the Atomic Energy Act). Information is classified by designated classification authorities applying approved classification guidance to specific documents. It is NRC's policy to classify information about the security systems (*e.g.*, guards, alarms, duress codes, etc.) of certain facilities or activities which would aid an adversary in attacking a facility or mode of transportation. It is also NRC policy to protect and appropriately classify foreign government information supplied to the U.S. with the understanding or agreement that the information is considered classified by the supplying foreign government.

2. Exemption 2–Internal personnel rules and practices of an agency

Exemption 2, which on its face applies to information "related solely to the internal personnel rules and practices of an agency," has been interpreted by the courts to encompass two distinct categories of information: (a) internal matters of a relatively trivial nature, such as which employees have agency parking permits, often referred to as "low 2" information; and (b) more substantial internal matters, the disclosure of which would risk circumvention of a legal requirement, often referred to as "high 2" information. FOIA Guide at 191, *citing Schiller v. NLRB*, 964 F. 2d 1205, 1207 (D.C. Cir. 1992).

In *Schiller*, the D.C. Circuit relied on the *Crooker* test, holding that Exemption 2 applies to material used for predominantly internal purposes. *Crooker v. Bureau of Alcohol, Tobacco & Firearms*, 670 F. 2d 1051, 1073 (D.C. Cir. 1981) (en banc). Then, relying on *Schwaner*, the *Schiller* court indicated that if the threshold test of predominant internality is met, an agency may withhold the material, provided either that disclosure may risk circumvention of agency regulation, or that the material relates to trivial administrative matters of no genuine public interest. *Schwaner v. Department of Air Force*, 898 F.2d 793, 794 (D.C. Cir. 1990) (citations omitted).

The opinion by the *Crooker* court is the most instructive. The court there used "high 2" to permit the Bureau of Alcohol, Tobacco & Firearms to withhold a law enforcement agency's

training manual. The court found the "critical considerations" to be that the manual was "used for predominantly internal purposes" and that "public disclosure would risk circumvention of agency regulations," because it was "common sense" that Congress would not compel the disclosure of information that would undermine the effective enforcement of laws. *Crooker, supra.* Under this reasoning, for example, the Commission could use "high 2" to withhold information pertaining to the security of the buildings that house NRC employees. In addition, it appears that internal NRC analysis of licensee security programs, including security inspections, could be withheld if the NRC determined that disclosure of the information could aid a terrorist in circumventing security arrangements. "High 2" may be usable to withhold a security inspection report even if the NRC were to share the report with the licensee, if the report is predominantly for internal use, and the licensee does not share it with others. (Exemption 4, discussed below, could be used to withhold licensee-provided security information.)

Furthermore, no balancing of public interest is warranted, once the agency determines that disclosure of the information could risk circumvention of agency regulations, since the issue of whether there is any public interest in disclosure becomes legally irrelevant under the "anti-circumvention" aspect of the exemption. *See* FOIA Guide at 206, *citing Voinche v. FBI*, 940 F. Supp. 323, 328 (D.D.C. 1996), in which court relied on the *Crooker* test, "where 'public interest in disclosure is irrelevant,' to find FBI information related to security of Supreme Court building and Supreme Court Justices properly withheld under Exemption 2." *aff'd per curiam*, No. 96-5304 (D.C. Cir. June 19, 1997).

While the task force has no hesitancy to recommend the continued use of Exemption "high 2" to withhold internal NRC security information and analyses, the availability and scope of the exemption continue to be the subject of substantial discourse. Although several circuits have explicitly sanctioned use of the "high 2" exemption, not limiting it to information on personnel matters or practices of a trivial nature that could not be of public interest, none of those decisions comes after September 11, 2001, or addresses security-related information of the type withheld by the NRC. In *Living Rivers Inc. v. United States Bureau of Reclamation*, 272 F. Supp. 2d 1313 (D. Utah 2003), where the information sought to be withheld had security implications, the court rejected Exemption 2 in favor of Exemption 7(F), discussed below, to withhold maps of downstream flooding that would occur following a breach of the Hoover or Glen Canyon Dams.

3. <u>Exemption 3–Safeguards Information and Restricted Data</u>

Exemption 3 encompasses any class of information that Congress has explicitly mandated in a statute not be publicly disclosed. One of the primary applications of Exemption 3 by the NRC is to withhold Restricted Data, which is required to be protected by the Atomic Energy Act. Under section 11y. of that statute, Restricted Data is defined to encompass information pertaining to the design, manufacture, or utilization of atomic weapons, or the production of special nuclear material. The classification of Restricted Data under the Atomic Energy Act is used to protect information that concerns the design, manufacture, or utilization of atomic weapons, the production of special nuclear material or the use of special nuclear material in the production of energy. Examples of information within the Restricted Data category include technological details of uranium enrichment technologies (*e.g.*, diffusion, centrifuge, laser based enrichment) and technologies in certain defense systems such as the Navy nuclear

program. NRC staff has no difficulty comprehending or applying this exemption for Restricted Data.

Safeguards Information is another category of information required by the Atomic Energy Act to be withheld from disclosure to unauthorized persons. The Commission's authority to protect Safeguards Information is set forth in Section 147 of the Atomic Energy Act. Safeguards Information is sensitive security information, not otherwise classified as National Security Information or Restricted Data, which pertains to certain NRC regulated facilities and radioactive materials. The unauthorized release of Safeguards Information could result in harm to the public health and safety, the Nation's common defense and security, or damage to the Nation's critical infrastructure. (Unauthorized disclosure of Restricted Data or Safeguards Information may result in imposition of criminal sanctions or civil monetary penalties.)

Section 147 of the Atomic Energy Act requires the NRC to promulgate regulations or orders, consistent with parameters articulated in that section, that set forth with specificity what information meets the statutory criteria for "Safeguards Information." The NRC has implemented the definition, in part, in 10 CFR §§ 73.2 and 73.21, and further amplified or specified it in orders issued to specific classes of licensees post-September 11, 2001. These included orders issued to various classes of licensees on March 25, 2002 and on January 7, February 6, and April 29, 2003. These orders (with any Safeguards Information redacted) may be viewed at the following Web address:

http://www.nrc.gov.reading-rm/doc-collections/enforcement/security/index.html.

Examples of the type of information the NRC considers to be Safeguards Information include information that identifies (1) a licensee's or applicant's detailed security measures for the physical protection of special nuclear material, source material or byproduct material; (2) a licensee's or applicant's detailed security measures for the physical protection and location of certain plant equipment vital to the safety of a facility possessing nuclear materials subject to NRC jurisdiction; (3) the design features of the physical protection system; (4) operational procedures for the security organization; (5) improvements or upgrades to the security system; (6) vulnerabilities or weaknesses in the security measures or systems described above that have not yet been corrected; and (7) such other information as the Commission may designate by order or regulation upon making the necessary findings pursuant to section 147. This exemption is readily comprehended by the NRC staff and applied effectively to withhold Safeguards Information.

On February 11, 2005, the Commission published for public comment (at 70 FR 7196) a proposed rule designating additional information as Safeguards Information based on the definition in section 147. The proposed rule would also codify the requirements imposed by the orders mentioned above. Public comments on that rule have been received and the NRC expects to issue a final rule modifying its regulations later this year.

4. Exemption 4–Proprietary Information

Exemption 4 allows, but unlike Exemptions 1 and 3, does not mandate, the withholding from public disclosure of commercial or financial information obtained from a person and privileged or confidential. In its regulation implementing this exemption, 10 C.F.R. § 2.390 (d), the NRC has construed Exemption 4 to encompass correspondence and reports to or from the NRC which contain information or records concerning a licensee's or applicant's physical protection, classified matter protection, or material control and accounting program for special nuclear material not otherwise designated as Safeguards Information, or classified as National Security Information or Restricted Data. This encompasses some of the security-related information obtained from licensees or applicants.

The courts have expansively construed Exemption 4 to cover "confidential" information received from private sector entities if disclosure of the commercial information is likely to have either of the following effects:

> (1) to impair the Government's ability to obtain necessary information in the future; or (2) to cause substantial harm to the competitive position of the person from whom the information was obtained. *National Parks and Conservation Ass'n v. Morton*, 498 F.2d 765, 770 (D.C. Cir. 1974).

In footnote 17 to that opinion, the court asserted it expressed no view as to whether other governmental interests are embodied in this exemption, but noted that based on its review of the legislative history of the statutory exemption, the problems of compliance and program effectiveness are mentioned as governmental interests possibly covered by the exemption. In at least two decisions, courts have been willing to expansively construe the governmental interests protected by Exemption 4. *9 to 5 Organization v. Board of Governors of the Federal Reserve*, 721 F. 2d 1 (1st Cir. 1983); *Critical Mass Energy Project v. NRC*, 975 F. 2d 871 (1992).

Protection for detailed plant security information is nothing new. The case of *Porter County Chapter of the Izaak Walton League of America v. Atomic Energy Commission*, 380 F. Supp. 630 (N.D. Ind. 1974) pertained to use of Exemption 4 to protect security-related information. In that case, which arose before the enactment of section 147 of the Atomic Energy Act, intervenors in the Bailly power reactor construction permit proceeding challenged the AEC's refusal to provide them documents requested under FOIA that it claimed they needed to participate in the licensing proceeding. Among the records denied by the AEC were detailed plant security information, including various nuclear reactor licensees' control and accounting procedures for safeguarding licensed nuclear material, and detailed measures for the physical security of a licensed facility. The court refused to order the release of the information, finding that the release of such information could facilitate attempts at sabotage, diversion of nuclear material, or other attacks upon nuclear power facilities to the obvious detriment of public health and safety. *Id*. at 634.

It is reasonable to construe Exemption 4 to encompass information that the NRC receives from outside sources, if disclosure could reveal vulnerabilities of nuclear facilities or materials to theft or sabotage or otherwise substantially assist persons intending to cause harm. This application of Exemption 4 would be justified under either the approach that the information is considered to be "confidential information" that is not normally made public and could cause competitive harm to the licensee or applicant if released to the public, or that the disclosure of such information could undermine the effectiveness of the security programs that Congress mandated the NRC oversee. The NRC has used his exemption to withhold, among other things, certain facility design details, drawings of equipment identifying specific weld areas, information about the impact of fire on certain cables, and information about seal damage that could occur if the temperature reached a certain level.

5. Exemption 5–Inter-agency or intra-agency memoranda that could be withheld under civil discovery privilege

Exemption 5 protects all inter-agency or intra-agency memoranda that would be privileged in the context of discovery during civil litigation. A threshold standard of intergovernmental sharing must be met to qualify for the inter-agency or intra-agency aspect of this exemption, reflecting consultation or solicitation of expert advice within an agency or between agencies. The exemption is most commonly applied to withhold material privileged as deliberative process, predecisional analysis, the disclosure of which would injure the quality of agency decisions. This privilege is invoked to preserve the quality of the agency decision making process and is based on the following policy purposes: (1) to encourage open, frank discussions on matters of policy between subordinates and superiors; (2) to protect against premature disclosure of proposed policies before they are adopted; and (3) to protect against public confusion that might result from disclosure of reasons and rationales that were not in fact ultimately the grounds for an agency's action. FOIA Guide at 370.

The material in question must meet two basic requirements to qualify for this privilege, i.e., it must be predecisional or antecedent to a decision, and deliberative, or in the nature of opinion or recommendation on matters leading to a decision. Segregable factual information contained in predecisional documents must generally be released to the public if requested under FOIA. *Montrose Chemical Corp. v. Train*, 491 F.2d 63 (D.C. Cir. 1974). This exemption is readily comprehended by the NRC staff and applied effectively to withhold briefing papers or drafts of security-related documents, and security policy analyses and recommendations produced by agency employees.

Exemption 5 can also be used to withhold legal analysis of security-related matters under other civil discovery privileges. The privilege most commonly invoked in this instance would be the attorney-client privilege, which applies to confidential facts related to the attorney by the client, legal opinions concerning those facts and communications between them on the matter, without being limited to the context of litigation. Another commonly invoked privilege is the attorney work-product privilege, which is restricted to material prepared in contemplation of litigation, including administrative proceedings.

6. Exemption 7–Records or Information Compiled for Law Enforcement Purposes

Exemption 7 covers information compiled for law enforcement purposes to the extent that production of the records would jeopardize one of the enumerated protections specified in the exemption. Among these protections are the right to a fair trial (Exemption 7(B)), the right to be free from unwarranted invasions of privacy (Exemption 7(C)), protection of the identity of a confidential source Exemption 7(D)), and protection of law enforcement techniques and procedures where disclosure could risk circumvention of law (Exemption 7(E)).

Two other statutory protections lend themselves most readily to application in security-related areas. Exemption 7(A) permits the withholding of information compiled for law enforcement purposes, to the extent that disclosure of the information could reasonably be expected to interfere with enforcement proceedings of a civil, criminal or administrative/regulatory nature, although the enforcement activity needs to be fairly focused and not merely general monitoring to ensure compliance with legal requirements. This clearly encompasses, for instance, personnel investigations focused on misconduct or potentially unlawful activity.

The NRC would employ the exemption to withhold security-related information developed by the Office of Investigations that is to be used to determine whether enforcement action should be taken against a licensee, security-inspection reports on a focused investigation that contain information indicating possible violation of regulatory requirements, allegations received from outside the agency of security-related violations, and analyses prepared by, or for, the Office of Enforcement to determine whether sanctions should be imposed against the violator. Exemption 7(A) is temporal, however, meaning that upon conclusion of the process for which the material was compiled, the exemption ceases to be available. The reason for this is clear: disclosure can no longer interfere with a proceeding that has been concluded. The exception to this would be where the information might relate to another on-going, pending, or prospective matter for which disclosure would present similar interference concerns, such as by signaling the existence, nature, or scope of an investigation that was not otherwise known, providing possibilities to avoid detection or evade enforcement. The NRC staff has no difficulty comprehending or applying this exemption.

Exemption 7(F) permits the withholding of information compiled for law enforcement purposes, to the extent that disclosure of the information could reasonably be expected to endanger the life or physical security of any individual. In the *Living Rivers* decision, mentioned above, the court found that the maps of downstream flooding that would occur following a breach of the Hoover or Glen Canyon Dams could be withheld under Exemption 7(F) because disclosure of the information could aid terrorists in evaluating how much damage would be done to downstream communities should either of the dams be breached. The court in that case was willing to invoke Exemption 7(F) after finding that the maps were compiled for law enforcement purposes, noting that the Bureau of Reclamation had express enforcement authority to maintain law and order with Reclamation Projects and used its maps pursuant to that authority. Because the Bureau had presented evidence that the disclosure of the maps could reasonably be expected to endanger the life or physical safety of any individual, the court held that Exemption 7(F) justified non-disclosure. Exemption 7(F) is not subject to the same temporal limitation as Exemption 7(A), since it has an open-ended purpose of protecting individuals from harm, rather than protecting against interference with other law enforcement activities that will eventually be completed, and thus, no longer be subject to interference.

Similarly, the Federal Energy Regulatory Commission (FERC) utilizes Exemption 7(F), along with other exemptions, to withhold critical energy infrastructure information, defined to include documents detailing specifications of FERC-licensed or certified energy facilities, such as oversized maps. *See* "Critical Energy Infrastructure Information," 68 FR 9857, March 3, 2003, amended April 16, 2003, 68 FR 18538. FERC takes the position that it has broad law enforcement authority under its statutes and that it will consider any information in its possession, which if released could endanger a person's life or safety, to be protected from disclosure under FOIA's law enforcement exemption.

7. Mosaic or Compilation Theory

Under the Freedom of Information Act, an agency is required to disclose any information that does not fall within one of the FOIA exemptions. However, some information, while seemingly innocuous or suitable for public release on its own, can be extremely harmful when grouped with other information. To provide protection from public disclosure of information that merits protection because of the context in which it is presented, the courts have sanctioned the use of the "mosaic" or "compilation" theory. The compilation approach is explicitly recognized in Executive Order 12958, supra, which sets forth the standards for applying compilation in classifying national security information.

> Compilations of items of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that: (1) meets the standards for classification under this order; and (2) is not otherwise revealed in the individual items of information. "Compilation" means an aggregation of pre-existing unclassified items of information. Section 1.7(e) of E.O. 12958, as amended by E.O. 13292 or March 25, 2003, 68 FR 15,315 (March 28, 2003).

The courts have applied the theory most commonly in the national security area, where the courts have repeatedly stated that the "mosaic-like nature of intelligence gathering" often changes the way an agency will classify or protect information that seems otherwise innocuous. *Salisbury v. U.S.,* 690 F. 2d 966, 971 (D.C. Cir. 1982). However, its use also has been routinely sanctioned for withholding information under exemptions other than Exemption 1. *See, e.g*., *Dorsett v. Dept. of Treasury*, 307 F. Supp 2d 28 (D.D.C. 2004) (Exemption 2), *Halperin v. CIA*, 629 F. 2d 144 (D.C. Cir. 1980) (Exemption 3); *Timken Co. v. U.S. Customs Service*, 491 F. Supp 557 (D.D.C. 1980) (Exemption 4); *Center for National Security Studies v. U.S. Department of Justice*, 331 F. 3d 918 (D.C. Cir. 2003) (Exemption 7).

While the mosaic or compilation approach can be applied to any exemption, it will not typically be used to limit the release of information that is readily available to the public, particularly if the information is available on the Internet. Withholding such information would not accomplish the objective sought, i.e., shielding the sensitive information, so with limited exceptions, information that is generally publicly available would not be withheld under any of the FOIA exemptions. Thus, information found in NRC publicly available publications, such as NUREGs, the Information Digest, and documents found in PARS would not be withheld. However, agency information that has been wrongfully leaked and not confirmed by the agency would not be considered publicly available information. *Murphy v. FBI*, 490 F. Supp. 1138 (D.D.C.1980). Likewise, information that is considered practically obscure, such as information that was public in the past but is now relatively unavailable to the public, will not be considered to constitute

"publicly available information." An example of such information may be that found in obscure journals.

It is our understanding that, government-wide, the mosaic theory is used sparingly to withhold documents that would not otherwise be exempt under FOIA. Nonetheless, it has been upheld by the courts, for example, to withhold certain seaport cargo-inspection data, which could lead to the identification of highly sensitive information and risk circumvention of law and regulations, when combined with other known data, *Coastal Delivery Corp. v. U.S. Customs Service*, 272 F. Supp. 2d 958, 964-965 (C.D. Cal. 2003); to withhold sales data between a parent company and its subsidiary which would not reveal production costs on its own but which costs could be ascertained when coupled with other available information, *Timken Co. v. U.S. Customs Service*, 491 F. Supp. 557, 559 (D.D.C. 1980); to withhold statistical intelligence-collection data that could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities, *ACLU v. U.S. Department of* Justice, 265 F. Supp. 2d 20, 29 (D.D.C. 2003); or to withhold information so intertwined with sensitive matters at the heart of the case that it would "tend to reveal matters of national security even though the sensitivity of the information may not be readily apparent in isolation," *Edmonds v. FBI*, 272 F. Supp. 2d 35, 47-48 (D.D.C. 2003).

8. <u>Bush Administration FOIA Policy</u>

Pursuant to the Attorney General's statutory responsibility "to encourage agency compliance with the Freedom of Information Act (FOIA)," on October 12, 2001, then-Attorney General John Ashcroft issued a memorandum to the heads of all departments and agencies setting forth the Bush Administration's policy on disclosure of information under the FOIA. The memorandum acknowledged the Administration's commitment to full compliance with the FOIA to ensure a well-informed citizenry. Simultaneously, Attorney General Ashcroft also recognized the Administration's commitment to safeguarding national security, enhancing the effectiveness of law enforcement, protecting sensitive business information, and preserving personal privacy. Regarding discretionary disclosures, Attorney General Ashcroft stated the following:

> I encourage your agency to carefully consider the protection of all such values and interests when making disclosure determinations under the FOIA. Any discretionary decision by your agency to disclose information protected under the FOIA should be made only after full and deliberate consideration of the institutional, commercial, and personal privacy interests that could be implicated by disclosure of the information.
>
> In making these decisions, you should consult with the Department of Justice's Office of Information and Privacy when significant FOIA issues arises, as well as with our Civil Division on FOIA litigation matters. When you carefully consider FOIA requests and decide to withhold records, in whole or in part, you can be assured that the Department of Justice will defend your decisions unless they lack a sound legal basis or present an unwarranted risk of adverse impact on the ability of other agencies to protect other important records.

On March 19, 2002, White House Chief of Staff, Andrew Card, issued a Memorandum for the Heads of Executive Departments and Agencies entitled "Action to Safeguard Information Regarding Weapons of Mass Destruction and Other Sensitive Documents Related to Homeland Security," urging departments and agencies to protect against inappropriate disclosure of any information that could reasonably be expected to assist in the development or use of weapons of mass destruction. Accompanying the Card memorandum was a joint memorandum issued by the National Archives' Information Security Oversight Office (ISOO) and DOJ OIP. The memoranda provided additional guidance on safeguarding homeland security information, including an instruction to make determinations on disclosure of such information under the FOIA in accordance with the Ashcroft memorandum.

The ISOO and DOJ OIP memorandum detailed how to protect three classes of information: classified, previously unclassified or declassified, and sensitive, but unclassified. The joint memorandum echoed the Ashcroft memorandum and reminded agencies that

> [a]ll departments and agencies should ensure that in taking necessary and appropriate actions to safeguard sensitive but unclassified information relating to America's homeland security, they [should] process any FOIA request for records containing such information in accordance with the Attorney General's FOIA Memorandum of October 12, 2001, by giving full and careful consideration to all applicable FOIA exemptions.

Pursuant to the Card memorandum, agencies and departments were to review their records management procedures for compliance with the ISOO/DOJ OIP guidance. Finally, the Card memorandum referred agency officials to DOJ OIP for "assistance in applying exemptions of FOIA to sensitive but unclassified information."

9. Conclusions on Application of FOIA Exemptions

In some respects FOIA case law is settled and easy to comprehend and apply; in other cases it is still evolving. There is relatively little disagreement on the application of Exemption 1 (classified national security information), Exemption 3 (information required to be withheld by statute), and Exemption 5 (inter-agency or intra-agency information that would be withholdable in the context of civil litigation). The scope of other exemptions continues to evolve. Much security-related information generated by licensees that has not been made public and could reasonably be expected to assist terrorists appears to be withholdable under Exemption 4,

particularly if the exemption is construed to include information that, if disclosed, could undermine the effectiveness of NRC's security program for protecting nuclear facilities and materials.

Similarly, most courts appear willing to construe Exemption 2 to encompass predominantly internal information, which, if disclosed, would aid circumvention of legal requirements. How far the courts are willing to go in this regard is uncertain, but there is sufficient legal authority for the Commission to continue to withhold internal security analysis, including inspection reports addressing security issues, and databases containing internally generated information under Exemption 2, if the Commission determines the information is not publicly available and its disclosure could reasonably be expected to aid a terrorist. Exemption 7 can clearly be used to withhold investigatory information developed or used for law enforcement purposes. The mosaic or compilation theory may be used to protect information that by itself is neither sensitive nor withholdable under a FOIA exemption, but which placed in the context of the particular document or group of documents becomes sensitive. Neither the mosaic/compilation theory nor any of the exemptions would be useful, however, to protect information widely available to the public.

The task force believes that these exemptions give the Commission considerable authority to withhold security-related information developed by the regulated community or the NRC from the public once the Commission determines that the information is not already widely available to the public and that its disclosure could aid a terrorist. The determination of whether particular information is exempt from disclosure, and if so, what exemption or exemptions are applicable, must be made on a case-by-case basis. The determination whether a document is exempt will frequently turn on how useful the information would be to a terrorist, fundamentally a technical or policy determination. To illustrate, decisions about controlling information about plant drawings will depend on the level of detail contained in the drawings. For instance, information that is clearly visible from public locations near the site, including low-resolution layout drawings of the site and adjacent areas, generally will be released. Thus, much of the information about plant site characteristics, including geography and demography, meteorology and seismology would not be withheld from public disclosure.

Other aspects of site characteristics may be subject to protection, however, including information about non-nuclear facilities near the power plants. As a general matter, NRC will make every effort to follow the guidance of other agencies regarding the control of information related to facilities or activities for which another agency has lead authority, such as pipeline data (usually withheld per the Department of Transportation) and chemical facilities (some data withheld per the Environmental Protection Agency). Information on the transmission grid for electric power, beyond that needed to support major licensing for nuclear power plants and related environmental findings, would generally be withheld in accordance with FERC guidance on critical energy infrastructure information. Detailed drawings showing specific locations of equipment within buildings, doorways, stairways, etc., would be withheld, consistent with criteria specified in SECY-04-0191, "Withholding Sensitive Unclassified Information Concerning Nuclear Power Reactors from Public Disclosure." Discussions of safety features or mitigation strategies within vulnerability assessments will be withheld under the same criteria.

The state of the law makes it imperative that the NRC use sound judgment in determining what information would be of use to a terrorist and, before utilizing some exemptions, balancing the harm to an informed public if the information is withheld. The SISP reviews must be thorough, and any information that staff believes is not already widely publicly available and that could be useful to a terrorist should be withheld from PARS. Information which is made available on PARS in one document is going to be extremely difficult to withhold if it is found in another agency document that has not been made available to the public and is being sought pursuant to FOIA. Therefore, it is better to withhold documents under the SISP process than to release sensitive information which the agency would most likely withhold even in response to a FOIA request.

10. FOIA Guidance on Withholding Security-Related Information

The attached guidance, suitable for incorporation into NRC Management Directive 3.1 on the Freedom of Information Act, has been developed to assist with evaluating security-related information for appropriate withholding under the FOIA exemptions discussed above. The guidance, entitled Criteria Governing Withholding of Security-Related Information, contains a short outline of the exemptions primarily used to support withholding of security-related information, with their associated criteria, and some illustrative examples of each.

LESSONS LEARNED REGARDING PROTECTION OF INFORMATION RESULTING FROM NAS STUDY EXPERIENCE

The Commission is aware of the history involved in the NRC's negotiations with the National Academy of Sciences (NAS or the Academy) to agree on a public version of the NAS's study of spent nuclear fuel storage at commercial reactor sites and it will not be repeated here. The task force isolated some factors that complicated the review process, however, and these may be distilled into the following lessons learned. In the future, the NRC may task external entities at the direction of Congress, or on its own, to prepare reports on security-related matters. A clear understanding of the parties' expectations regarding any public report to be issued needs to be reached before the parties enter into an agreement for the work to be performed and that understanding needs to be set forth unambiguously in the award document.

The type of agreement used to set forth the parameters of the report may have some bearing on the question of who controls determinations about which portions of the document are suitable for public release; thus, the initial consideration should be the appropriate vehicle for conducting this type of work, *i.e.*, whether it should be done through procurement (a contract) or assistance (a grant or cooperative agreement). A significant factor in the selection of a suitable method to obtain the work is the consideration of primary benefit from the results of the effort. Where the agency will receive the direct benefit of the work, procurement is the proper course to follow, whereas when the benefit to the public may be viewed as paramount, an assistance vehicle may be used. In addition, a contract should be used if the primary purpose of the work is to obtain well-defined research in direct support of the agency's licensing and regulatory mission, and the end result is clearly defined in advance, among other things. On the other hand, an assistance document (grant or cooperative agreement) may be more appropriate when the primary purpose of the work is to aid or support the development of knowledge or understanding of a subject under study, the exact course of the work and outcome are not defined precisely, there will be little involvement with the agency during the course of performance, and the simplicity and economy in execution and administration are

mutually desirable. *See*, Federal Grant and Cooperative Agreement Act, 41 U.S.C. 501; Financial Assistance Program, NRC Management Directive Handbook 11.6, Part I (B).

Compared to the time and effort involved in a sole source acquisition, the assistance process may commend itself to external security reviews as a better means of accomplishing the intended purpose, precisely because of this relative simplicity and economy. However, by the same token, it leaves the parties with rather less formal structure or ability to address disagreements that arise during performance or, ultimately, with project deliverables. That is, the federal acquisition system potentially affords, among other things, relatively robust protection for sensitive information, procedures for inspection of work, approval of works for publication, provisions for progress payments, and various payment consequences for contract non-compliance or breach, contract termination, as well as administrative appeals of contracting officer final determinations, or resort to Boards of Contract Appeals to resolve claims or disputes, and even federal court litigation. To be sure, NRC's general grant provisions also incorporate many of these terms, such as provisions for publication of reports; however, these provisions are quite abbreviated and necessitate the addition of specific language in the award document to effectuate particularized requirements. For instance, even though the NAS grant document was modified to replace the usual security clause, the replacement clause itself was a standard version and not tailored to reflect any unique requirements for this study's report.

Ultimately, with or without the performance assurances and remedies provided by the acquisition system, steps may be taken to provide more prescriptive terms for performance compliance and resolution of disputes. The first and most important measure would be for the award document, whether contract or grant, to incorporate clear, unequivocal requirements for performance, including those regarding production of reports publishing results. Use of standard clauses has some merit, because such clauses often address potential problems that might not be contemplated separately by the parties. However, clauses should be expressly tailored, or special provisions added, to make explicit the non-negotiable expectations of the parties regarding control of publication or approval of publication texts, such as vesting of approval authority in one party or the other, or in the alternative, imposing a requirement for joint review and agreement on publication versions, or a scheme to resolve differences of opinion. The parties might even resort to arbitration by the Office of Management and Budget for interagency issues, or possibly agree to mediation by a third party, such as the Department of Justice, when a matter arises with an entity that is not a federal agency.

In any case, when the NRC tasks an outside entity to prepare a report for it on security-related matters, a clear understanding of the nature of the public report needs to be reached before the parties enter into an agreement for the work to be performed. Clear responsibility should be indicated in the award document to identify the source of sensitive information and mark it as such, so that it can be appropriately classified, or designated as sensitive unclassified information, including Safeguards Information, or other information exempt from disclosure under the FOIA. This should help resolve certain issues prior to award and facilitate determinations on public release of any reports generated under the task. The document could include a milestone schedule with submittal of drafts allowing sufficient time for NRC review, the process for final determination of information to be withheld from public disclosure in the publication document and provide for non-compliance penalties, such as withholding of payment. The document could contain a statement that failure to comply with the pre-publication terms constitutes breach and that certain consequences may result, i.e., non-

payment or termination. Enforcement remains an issue outside the traditional acquisition scheme–*e.g.*, when grants and cooperative agreements are used. In cases where grants and cooperative agreements are used, the best means to ensure a mutually satisfactory effort is a carefully written award document that fully captures the expectations of both parties, particularly as to issues of publication control, and provides for means to resolve disagreements in a fair and timely fashion.

RECOMMENDATIONS

1. That the staff ensure that all agency records within the purview of 5 U.S.C. 552(a)(2) are promptly made available to the public via PARS soon after the records are generated.

2. That to the extent practicable, any documents withheld under the SISP criteria should likely be withholdable under FOIA, either in whole or in part.

3. That the SISP reviews be carefully done so information made available to the public as a matter of administrative discretion does not include sensitive information that the agency would withhold if requested under FOIA.

4. That the Commission endorse the standards for withholding security-related information under FOIA set forth in the attachment to this report and that those standards be incorporated into Management Directive 3.1, Freedom of Information Act.

5. That when the NRC requests that external organizations produce documents under NRC contract, grant or other agreement containing classified information, or sensitive unclassified information (including Safeguards Information), controls over information disclosure are clearly articulated in the document that describes the work to be performed.

CRITERIA GOVERNING WITHHOLDING OF SECURITY-RELATED INFORMATION

General Guidance:

Information may be withheld from public disclosure under the Freedom of Information Act (FOIA) if it falls within one or more of the FOIA statutory exemptions described below. Case-by-case determinations need to be made on whether information can be protected, and if so, which of the exemptions is most suitable.

Exemption 1: **Classified National Security Information**

Statutory description: Matters "specifically authorized under criteria established by an Executive Order to be kept secret" in interest of national defense or foreign policy

Criteria:

information meeting standards set forth by Executive Order to be kept secret in interest of national defense or foreign policy, including information about federal government programs to safeguard nuclear materials or facilities, vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, including defense against transnational terrorism, if unauthorized disclosure of information could be expected to cause damage to national security that original classification authority is able to identify or describe

information properly classified pursuant to Executive Order by designated classification authorities applying approved classification guidance to specific documents and marked accordingly

information not in public domain

mosaic/compilation approach acceptable when compiled information reveals additional association that meets classification standards in Executive Order and is not otherwise revealed in individual items of information (see Mosaic summary below)

Examples of classified information:

information pertaining to security of fuel cycle facilities possessing strategic quantities of special nuclear material

information about security systems (e.g., guards, alarms, duress codes, etc.) of certain facilities or activities which would aid an adversary in attacking a facility or mode of transportation

foreign government information provided with understanding or agreement that information considered classified by supplying foreign government

Examples of information that is not classified:

Safeguards Information

critical infrastructure information that does not fall within the purview of the criteria set forth in the Executive Order governing classification of information

information labeled “official use only”

<u>Exemption 2</u>: Substantial internal matters, disclosure of which would risk circumvention of a legal requirement–“high 2”

Statutory description: Matters “related solely to internal personnel rules and practices of an agency”

Criteria:

information predominantly internal

disclosure presents risk of circumvention of law or legal requirement

no balancing of public interest (no legitimate public interest in disclosure of information that would assist in evasion of law or detection)

mosaic/compilation approach acceptable when information would not by itself reveal sensitive information but assembly of different pieces of similar information could cause damage

Examples of “high 2” information:

information pertaining to the security of buildings that house NRC employees

internal NRC analysis of licensee security programs, including security inspections, where disclosure of information could aid a terrorist in circumventing security arrangements

security inspection report shared with licensee, if report is predominantly for internal use, and licensee does not share it with others (Exemption 4 could be used to withhold licensee-provided security information)

Examples of information that does not fall within “high 2”:

externally-generated analyses, including vulnerability assessments performed by non-government parties

NRC data bases consisting predominantly of licensee-generated information (but these may be protected under another exemption, such as Exemption 1 or Exemption 3)

Exemption 3: **Information mandated by federal statute to be withheld from public disclosure**

Statutory description: Matters “specifically exempted from disclosure by statute” that leaves no discretion on withholding, or establishes particular criteria for withholding or refers to particular types of matters to be withheld

Criteria:

nondisclosure mandate must be contained in federal statute

general disclosure of information must be prohibited on face of statute, or by establishing particular criteria or reference to specific types of information to determine which information is within scope of statute’s prohibition

Restricted Data, under section 11y. of Atomic Energy Act, encompasses information pertaining to design, manufacture, or utilization of atomic weapons, or the production or use of special nuclear material

Safeguards Information, under section 147 of Atomic Energy Act, encompasses information prescribed by regulation in 10 C.F.R. §§ 73.2 and 73.21 (or by order) that specifically identifies a licensee's or applicant's detailed (1) security measures for the physical protection of special nuclear material; (2) security measures for the physical protection and location of certain plant equipment vital to the safety of a facility possessing nuclear materials subject to NRC jurisdiction; (3) the design features of the physical protection system; (4) operational procedures for the security organization; (5) improvements or upgrades to the security system; (6) vulnerabilities or weaknesses in the security measures or systems described above which have not yet been corrected; and (7) such other information as the Commission may designate by order or regulation upon making the necessary findings pursuant to section 147. [Note: description augmented subject to Commission promulgation of final rule amending Part 73.]

Examples of information within mandatory prohibition against disclosure:

Restricted Data includes technological details of uranium enrichment technologies (e.g., diffusion, centrifuge, laser based enrichment) and technologies in certain defense systems such as navy nuclear program

Safeguards Information includes details from licensees' physical security plan, such as number of guards, specific location of security equipment

Examples of information outside mandatory prohibition against disclosure:

security measures for physical protection of facility in plain sight of public

physical protection design details readily available to public

Exemption 4: Information about physical protection, classified matter protection, or material control and accounting program for special nuclear material that is not Safeguards, Classified National Security Information, or Restricted Data, or security-related information that could reasonably jeopardize government program effectiveness if disclosed to public

Statutory description: Matters involving "trade secrets and commercial or financial information obtained from a person and privileged or confidential"

Criteria:

information must originate outside federal government

information must be "confidential" within meaning of exemption

disclosure would likely impair government's ability to obtain necessary information in future or cause substantial competitive harm to person who provided information, or disclosure could impair government interests of compliance or program effectiveness

Examples of information that may qualify for Exemption 4 protection:

detailed plant security information, including licensees' control and accounting procedures for safeguarding licensed nuclear material, or detailed measures for the physical security of a licensed facility, particularly information that could facilitate attempts at sabotage, diversion of nuclear material, or other attacks detrimental to public health and safety

information generated outside government revealing vulnerabilities of nuclear facilities or materials to theft or sabotage

certain facility drawing details showing specific locations of equipment or materials within buildings

private sector information whose disclosure could reasonably jeopardize a government security program's effectiveness

Examples of information that would not qualify for Exemption 4 protection:

general descriptions of safety-related systems in nuclear power plants, particularly where available in open source literature or on websites accessible to public

general information about workings of nuclear power plant, such as that provided in licensing documents

low-resolution drawings of plant site and adjacent areas

Exemption 5: Inter-agency or intra-agency material privileged in context of civil discovery

Statutory description: Matters involving inter-agency or intra-agency memoranda that "would not be available by law to a party other than an agency in litigation with the agency"

Criteria:

communication must be internal to government (within the agency or among government agencies)

reasonably segregable material not covered by exemption must be disclosed

deliberative process privilege covers material reflecting predecisional analysis, recommendation or opinion on matters leading to final decision

attorney-client privilege covers confidential facts related by client to attorney and legal opinions and communications between them concerning the consultation

attorney work-product privilege covers material prepared in contemplation of litigation, including administrative proceedings

Examples of privileged material:

portions of briefing papers or drafts of security-related documents

security policy analyses and recommendations produced by agency employees

analysis of agency's litigative risk in security-related hearing

description of agency's legal strategy in proceeding on security-related matters

Examples of material outside privilege:

final agency decisions that expressly incorporate predecisional analysis

after-the-fact descriptions or explanations of agency policy or decision

segregable facts from documents otherwise subject to deliberative process privilege

Exemption 7: Investigatory and other information compiled for law enforcement purposes

Statutory description: Matters involving "records or information compiled for law enforcement purposes" to extent that production of such records would implicate one of six enumerated protections

Criteria:

information compiled for law enforcement purposes to extent production of records would jeopardize statutory protections, including information that, if disclosed, could reasonably be expected to interfere with enforcement proceeding (Exemption 7(A)), right to fair trial (Exemption 7(B)), right to be free from unwarranted invasions of privacy (Exemption 7(C)), protection of identity of confidential source Exemption 7(D)), protection of law enforcement techniques and procedures where disclosure could risk circumvention of law (Exemption 7(E)) and to extent disclosure could reasonably be expected to endanger life or physical security of any individual (Exemption 7(F))

law enforcement activity must be fairly focused and not merely general monitoring to ensure compliance with legal requirements but may be civil, criminal or administrative/regulatory in nature

use of Exemption 7(A) is temporal, i.e., limited to pendency of matter involved

Examples of qualifying law enforcement information:

investigations focused on misconduct or potentially unlawful activity

security-related information developed by Office of Investigations used to determine whether enforcement action should be taken against licensee

security-inspection reports related to a focused investigation with information addressing whether there has been a possible violation of regulatory requirements

allegations of security-related violations received from outside agency and related analyses prepared by or for Office of Enforcement to determine whether sanctions should be imposed against violator

Examples of non-qualifying law enforcement information:

routine security inspection reports

investigatory or enforcement material on closed investigatory or enforcement matters

Mosaic or Compilation Theory

Under FOIA, an agency is required to disclose any information that does not fall within one of the FOIA exemptions. However, some information, while seemingly suitable for public release on its own, can be extremely harmful when grouped with other information. To provide protection from public disclosure of information that merits protection because of the context in which it is presented, the courts have sanctioned the use of the "mosaic" or "compilation" theory, which is explicitly recognized in the classification Executive Order 12356, setting forth the standards for classifying national security information.

> Compilations of items of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that: (1) meets the standards for classification under this order; and (2) is not otherwise revealed in the individual items of information. "Compilation" means an aggregation of pre-existing unclassified items of information. Section 1.7(e) of E.O. 12958, as amended by E.O. 13292 of March 25, 2003, 68 FR 15315 (March 28, 2003).

Mosaic theory also is available to withhold information under any other FOIA exemption.

Criteria:

material, when aggregated and discussed in context of other responsive information, reveals other underlying facts, associations or relationships that are protected

protected information need not be compiled in a single document

not used to limit release of information exactly the same as agency already has disclosed, although material that is merely similar may be subject to protection

not used to protect readily available information, such as information in widely available publications or on Internet

may be used for information considered practically obscure, such as information public in the past but now relatively unavailable to the public

information that has been wrongfully leaked and not confirmed by agency would not be considered publicly available

do not need conclusive proof of compromise or jeopardy of protected information

June 30, 2005

MEMORANDUM TO: Karen D. Cyr
General Counsel

Luis A. Reyes
Executive Director for Operations

FROM: Annette L. Vietti-Cook, Secretary **/RA/**

SUBJECT: STAFF REQUIREMENTS - SECY-05-0091 - TASK FORCE REPORT ON PUBLIC DISCLOSURE OF SECURITY-RELATED INFORMATION

The Commission has approved the Task Force recommendations on public disclosure of security-related information. The staff should make the Task Force report available to the public.

The second recommendation should be restated to read: "That to the extent practicable, the SISP criteria should follow the principles for withholding security-related information under FOIA."

The staff should advise the Commission of the actions it has taken or plans to take to implement the recommendation regarding contracts, grants or other arrangements for preparation of reports on security-related matters.

In light of the "Lessons Learned" section of the report, OGC should formulate model language to be incorporated into future contracts and grants that would prescribe clear requirements for production of reports, publication of results, and responsibility for identifying and marking sensitive information. OGC should carefully consider the report's recommendations to determine if other areas might benefit from development of model language. Any model language should be carefully reviewed prior to inclusion into future documents and if necessary, specifically tailored to meet the needs of the Agency in a particular agreement.

The staff, in consultation with OGC, should develop and implement an enhanced and regularly-scheduled periodic training program for NRC staff members who routinely deal with FOIA matters. Because FOIA continues to evolve through court decisions, the training program material should be updated on a periodic basis and the updated information routinely provided to those with FOIA duties. Additionally, in developing this training program, the staff should consider developing a program that would allow the material to be accessed with ease, perhaps a web-based training module, so that staff members with periodic FOIA questions would be able to easily review the latest agency guidance. The staff should also consider integrating this enhanced FOIA training with training regarding the marking and protection of sensitive documents.

cc: Chairman Diaz
Commissioner McGaffigan
Commissioner Merrifield
Commissioner Jaczko
Commissioner Lyons
DOC
CFO
OCA
OPA
PDR