POLICY ISSUE
(Notation Vote)

October 19, 2004 SECY-04-0191

FOR: The Commissioners

FROM: Luis A. Reyes
Executive Director for Operations /RA/

SUBJECT: WITHHOLDING SENSITIVE UNCLASSIFIED INFORMATION CONCERNING NUCLEAR POWER REACTORS FROM PUBLIC DISCLOSURE

PURPOSE:

To obtain Commission approval of guidance to be issued to the Nuclear Regulatory Commission (NRC) staff, power reactor licensees, and other agency stakeholders for withholding sensitive unclassified (nonsafeguards) information from public disclosure.

SUMMARY:

In a staff requirements memorandum dated May 7, 2004, the Commission directed the NRC staff to develop guidance to ensure information that could reasonably be expected to be useful to potential adversaries is withheld from public disclosure. In determining whether information should be withheld or released, the NRC staff must attempt to appropriately balance our desire to maintain the openness of NRC's regulatory processes with the need to protect the public from possible terrorist threats. This paper provides for Commission review and approval the NRC staff's proposed approach for determining the appropriate handling of information and more specific guidance for withholding or releasing information about nuclear power reactors (Attachment 1).

CONTACTS: William D. Reckley, NRR/IRT
301-415-1323

Margie Kotzalas, NRR/IRT
301-415-2737

BACKGROUND:

In the aftermath of September 11, 2001, the NRC has been challenged, as have other government and private institutions, to assess and revise controls on withholding from public disclosure information that might be useful to terrorists. The NRC policies and criteria for withholding information currently available to external stakeholders are described in COMSECY-02-0015, "Withholding Sensitive Homeland Security Information From the Public," dated April 4, 2002, and the associated SRM dated May 28, 2002. COMSECY-02-0015 provided criteria for withholding information from public disclosure and a general standard that information should be withheld when its release would provide a clear and significant benefit to a terrorist in a potential attack. In COMSECY-03-0036, "Update on the Withholding From Public Disclosure of Sensitive, Unclassified Information Related to Power Reactors," dated July 17, 2003, the staff proposed clarifications to the guidance in COMSECY-02-0015 and provided draft guidance on protecting sensitive information for the NRC staff and nuclear power reactor licensees.

The SRM dated May 7, 2004, instructed the staff to revise the basic standard for withholding information from the public to cover information that "could reasonably be expected to be useful" to terrorists in planning or executing an attack. The SRM also directed the staff to ensure that NRC guidance is consistent with regulations and guidance promulgated by the Department of Homeland Security (DHS) and addresses issues identified during the use of the existing criteria and guidance for withholding sensitive information. The Commission directed the staff to announce and explain the revised guidance to NRC personnel, licensees, and other agency stakeholders.

DISCUSSION:

The NRC has traditionally provided the public with a significant amount of information about the facilities and materials for which the NRC has regulatory responsibilities. This policy has been and remains a cornerstone of the NRC's regulatory philosophy. The Atomic Energy Act, subsequent legislation, and various NRC regulations, have given the public the right to participate in the licensing and oversight process for nuclear power reactors and other NRC licensees. To participate in a meaningful way, the public must have access to information about the design and operation of regulated facilities or materials. However, the NRC and other government agencies have always withheld some information from public disclosure for reasons of security, personal privacy, and commercial or trade secrets. In light of increased terrorist activity worldwide, the NRC has reexamined its traditional practice of releasing almost all documents to the public. The NRC will continue to work with DHS and other agencies to develop and implement any new guidance or requirements that may impact our strategy to communicate openly with the public.

Per the Commission's direction, the goal of establishing guidance for the NRC staff and licensees is to withhold information that could reasonably be expected to be useful to potential adversaries while minimizing the adverse effects on the NRC goals of openness and effectiveness. The attempt to weigh each of the agency's key goals and reach a balanced decision, inevitably introduces a certain amount of subjective judgment with respect to most

information about the design and operation of nuclear power plants. However, the NRC staff's experience is that you must consider the various competing factors to develop a logical and consistent decision regarding the handling of information. Guidance for reaching a balanced decision was provided in COMSECY-02-0015 and has proven useful to the staff in assessing the appropriate handling of specific documents. Unlike safeguards information (SGI) and security-related information within the reactor oversight process, which deal primarily with security programs, most information on nuclear reactors is developed and maintained to support areas such as engineering, operations, and licensing. The potential usefulness of this information to an adversary is in showing how a facility is constructed or operated, not how it is protected in terms of security. The difficulty in withholding such information is that much of it relates to how a facility was licensed and how it is maintained. The information provides the means for the NRC and public to assess the safety of the facility in areas other than security. Stringent restrictions on information related to plant design and operation (i.e., not directly related to security) could have a negative impact on safety if the controls result in less sharing of information among the appropriate licensee personnel. Therefore, the staff has developed the following general approach, as well as more specific criteria, for controlling information on nuclear power reactors.

The staff is limiting this guidance to nuclear power reactors and will prepare separate consistent guidance for other types of licensed activities.[1] The staff believes this is appropriate because a realistic evaluation of the appropriate controls on information needs to consider the threats, the risks of potential attacks, the security programs in place, and other factors that vary widely among the different types of licensees. For the most part, the staff used this approach in interpreting and implementing the guidance in COMSECY-02-0015. For nuclear reactors, most information on security that is addressed by the criteria in COMSECY-02-015 has been and continues to be controlled as SGI. In addition to the information on security programs, the staff has withheld information regarding some aspects of plant design (e.g., detailed layout drawings of sites or buildings), risk insights comparable to individual plant examination (IPE) documents in terms of identifying critical combinations of equipment, and current plant configurations. In COMSECY-03-0036, the staff proposed to revise the criteria and usually release documents providing risk insights for nuclear power plant designs and operations because such information is already available in the public domain and the withholding of such information is increasingly awkward as the agency moves to incorporate such risk insights into its routine decisionmaking. The SRM dated May 7, 2004, directed the staff to revise the clarifications proposed in COMSECY-03-0036 and the guidance established in COMSECY-02-0015 and the associated SRM.

[1] The staff outlined in SECY-04-0155, "Request From Department of Energy Office of Naval Reactors to Designate Information Related to Nuclear Fuel Services, Inc. And BWX Technologies, Inc., As 'Official Use Only'," dated August 24, 2004, the steps taken and guidance provided to remove information from public access related to Category I fuel cycle facilities.

In determining what information "could reasonably be expected to be useful to potential adversaries," one needs to assess the relevance of the specific information to an adversary's ability to plan or execute an attack or other malevolent act and the ability of a licensee or government agency to respond to such an attack. It is important to develop a logical assessment approach to ensure consistency, to ensure that appropriate information is withheld from public disclosure, and to minimize adverse effects on the agency's openness and effectiveness. It is also important to maintain an appropriate and realistic view about the added security assurance provided by the control of non-SGI information. The withholding of certain design or operational information may introduce a hurdle for potential adversaries during their planning of a malevolent act. The effectiveness of the hurdle, however, depends on the assumed level of sophistication, education, and knowledge of the adversaries. In some cases, it may be more appropriate to assess and, if necessary, revise a security program in recognition that the subject information is in the public domain.

The discussion below is not intended to illustrate a detailed threat or vulnerability assessment since decisions regarding the release or withholding of most information are expected to be made at the staff level within each program office. The following factors provide a general framework that may be used to develop more specific guidance for different types of facilities or materials.

- The threat

  The control of information as part of an overall program to safeguard against the intentional release or diversion of radioactive materials needs to consider those threats for which the withholding of information might be helpful. The assessment is not limited to or even related to the design basis threat (DBT) but instead needs to consider the range of possible malevolent acts against a nuclear power reactor or other licensed activity. The assessments and evaluations are, at this point, based largely on staff judgments unless more detailed simulations, vulnerability assessments, or other guidance are available.

- The consequences

  For each of the possible threats, there is a possible consequence in terms of harm to the public. The consequences of an event involving a nuclear reactor include the possible release of radioactive materials that might adversely affect public health and safety. In the worst case, an attack on a nuclear reactor could cause plant transients and losses of mitigating systems, leading to core damage and a major release of fission products. The consequences for other threats involve lesser releases (e.g., from waste systems) or possibly no releases of radioactive materials. The possible consequences associated with a particular licensed activity are usually reflected in the licensing processes and regulatory controls placed on those activities. The decision to withhold or release information needs to consider the possible consequences of events such that our controls on information correlate to the potential harm (i.e., information would not be treated as sensitive unless it relates to the potential release or diversion of radioactive materials posing a threat to public health and safety).

- The relationship of design/operating limits to security programs

  Information related to security programs at nuclear reactors is generally designated as SGI and is protected in a manner similar to classified confidential information. For nuclear reactors, the security program is quite extensive and is established to protect the plant, including the engineering barriers designed to prevent the release of radioactive materials, from an attack by potential adversaries. Information on the engineering barriers themselves has largely been part of the public record. For other NRC-licensed activities or nonnuclear critical infrastructure, security programs may not be as extensive and the engineering barriers may also serve as the primary security feature. In such cases, protection of engineering information may be more important from the standpoint of security (after factoring in the other factors such as possible threats and consequences).

- Availability of information from other sources

  In assessing the control of information, it is important to assess the availability of the information or similar information from sources outside the control of the NRC or its licensees. If the information is available from open source literature such as text books, Web sites, or other sources, an NRC decision to withhold the information may decrease the openness of our regulatory programs without obstructing an adversary.

- Subsequent controls on the information

  In deciding to withhold information coming to or issued by the NRC, we need to consider how the information will be controlled by other parties with access to it. For example, a situation could negatively affect our goals regarding effectiveness or openness if we strive to withhold information and the information is then released by a licensee or other government agency. A consistent treatment of information may evolve as DHS continues to develop requirements or guidance for controlling information shared among licensees and Federal, State, and local governments when the information is designated “sensitive homeland security information.”

  This assessment will also address how the information and its controls are incorporated into other licensee and regulatory processes. Any concerns regarding conflicting determinations (e.g., a finding that information should be withheld due to an assessment of its possible usefulness to an adversary and a regulatory need to make the information public) should be reported to agency management for resolution.

The above general criteria are expanded upon and applied to the routine (nonsecurity) documents received and generated by the NRC and power reactor licensees to develop the specific guidelines and examples provided in Attachment 1.

The staff has evaluated the information categories developed by other Federal agencies and will include a discussion of the designations with possible implications for nuclear reactors in the guidance being prepared for the NRC staff and licensees. The NRC staff will, whenever possible, maintain practices consistent with other government agencies that are controlling

information related to facilities located near nuclear power reactors. The major designations of information with a potential to affect nuclear reactors are discussed in Attachment 2. A short discussion of selected designations is provided below:

- Protected Critical Infrastructure Information (PCII): PCII is voluntarily provided to DHS, is not customarily in the public domain, and is related to the security of critical infrastructure or protected systems. The NRC staff does not expect that the NRC or nuclear power reactor licensees will need to deal very often with information designated as PCII because nearly all information related to security is addressed by NRC regulations and oversight programs.

- Critical Energy Infrastructure Information (CEII): CEII is a designation defined in the regulations of the Federal Energy Regulatory Commission (FERC) at Title 18 CFR Parts 375 and 388 for information related to energy-related infrastructure. FERC provided additional guidance related to CEII in its rulemaking documents. There is some overlap in the information provided to the NRC by power reactor licensees regarding nearby energy-related facilities (e.g., hydroelectric dams, electric transmission systems) and the information routinely treated as CEII by FERC. Likewise information related to the location of pipelines may warrant review and withholding per guidance from the Department of Transportation. Most of the information regarding electric transmission systems provided to FERC (through its periodic Form 715) is designated CEII. The NRC staff believes we will need to make public some information on electric transmission systems supporting nuclear power plants since the information is integral to major licensing decisions and related environmental findings.

- Homeland Security Information (HSI): The term HSI was introduced in the Homeland Security Act of 2002, 6 USC 482, as part of the effort to ensure that information related to possible terrorist activities would be shared between the appropriate Federal, State, and local governments.

- Sensitive Homeland Security Information (SHSI): The term SHSI has been proposed to address the HSI that must be shared between Federal, State, and local agencies while being withheld from public disclosure. DHS continues to work on requirements and guidance to fully develop the SHSI designation. Given its relationship to HSI and the sharing of information with appropriate agencies, the staff believes that SHSI related to nuclear power plants will most likely involve some information on potential threats and the coordination of responses to a terrorist attack. If information is being shared only between a licensee and the NRC, the staff would more likely use the provisions of 10 CFR 2.390 to withhold the information from public disclosure.

NRC regulations at 10 CFR 2.390 provide a mechanism to withhold from public disclosure information related to the physical protection of nuclear power plants that does not meet the existing criteria for designation as SGI. This type of information was recognized before September 11, 2001, and, when submitted to the NRC by a licensee, was withheld from public disclosure and handled similarly to commercial or financial information as directed by the regulation. The NRC has expanded the application of this regulation to address sensitive

unclassified (non-SGI) information previously made public but now withheld if the information could be useful to a potential adversary (e.g., detailed layout drawings and selected inspection reports). The staff expects that the volume of material withheld from public disclosure according to 10 CFR 2.390 will continue to increase as the process is explained to licensees and the NRC staff. The staff will continue the historical practice of waiving the requirement for an affidavit from the licensee when a request for withholding information (similar to commercial or financial information) is made in accordance with 10 CFR 2.390 because the information concerns a facility's physical protection.

The SRM dated May 7, 2004, directed the staff to consider the experiences and lessons learned since the review activities were initiated following September 11, 2001. The biggest issue related to the withholding of information on power reactors concerns the guidance in COMSECY-02-0015 to withhold risk insights similar to the risk insights provided in documents such as individual plant examinations (IPEs). If the desire is to keep from adversaries the list of important mitigating systems, the staff believes the effort would have little or no benefit because such information is available in open source literature. It may be possible, however, to at least impede efforts by adversaries to obtain information on the plant-specific location of many important components. As a point of clarification, the staff has not withheld and does not expect to withhold information regarding risk importance measures for specific plant systems since these numerical values could not reasonably be expected to be useful to an adversary. A stronger argument could be made for withholding documents that identify specific combinations of systems whose loss, when combined with an identified initiating event, results in core damage. However, this information is available in the public domain, and the staff does not foresee withholding such information for power reactors unless it is related to security activities (e.g., vulnerability assessments). Another issue related to the withholding of information on power reactors concerns both ongoing and past adjudications, including the hearing files, testimony, documents which must be provided in discovery, and documents supporting staff conclusions and licensing actions. Because the public has the right to participate in varying ways in the licensing and other regulatory processes associated with NRC-licensed facilities, the withholding of certain information in staff documents related to those processes may need to be modified on a case-by-case basis. For example, certain information may not be able to be withheld at all under applicable statutory and case law, while other information may have to be provided to parties to proceedings under protective orders. The staff will consult with OGC in such circumstances.

The staff plans to conduct public meetings and issue guidance to the staff, licensees, and stakeholders as soon as practical after finalizing the agency's position on the designation of information as sensitive unclassified (non-SGI) information. The meetings and related interactions will also enable the staff to discuss with stakeholders the potential need for changes in licensees' document control practices to protect sensitive unclassified (non-SGI) information.

RECOMMENDATIONS:

We recommend the Commission approve (1) the general framework presented in this paper for making decisions on withholding information because its release could reasonably be expected to be useful to an adversary and (2) the specific guidance provided in Attachment 1 for making such determinations for information related to nuclear power reactors.

COORDINATION:

The Office of the General Counsel has reviewed this paper and has no legal objections to its content.

/RA/

Luis A. Reyes
Executive Director
for Operations

Attachments: 1. Handling of Sensitive Unclassified (Nonsafeguards) Information on Nuclear Power Reactors That Could Reasonably Be Expected to Be Useful to a Potential Adversary
2. Terminology and Other Government Designations

RECOMMENDATIONS:

We recommend the Commission approve (1) the general framework presented in this paper for making decisions on withholding information because its release could reasonably be expected to be useful to an adversary and (2) the specific guidance provided in Attachment 1 for making such determinations for information related to nuclear power reactors.

COORDINATION:

The Office of the General Counsel has reviewed this paper and has no legal objections to its content.

/RA/

Luis A. Reyes
Executive Director
for Operations

Attachments: 1. Handling of Sensitive Unclassified (Nonsafeguards) Information on Nuclear Power Reactors That Could Reasonably Be Expected to Be Useful to a Potential Adversary
2. Terminology and Other Government Designations

ADAMS ACCESSION #: ML042310663 **SECY-012**

OFFICE	NRR/IRT	NRR/IRT	NSIR	RES	NMSS
NAME	WReckley	MKotzalas (TTate for)	GTracy	CPaperiello	JStrosnider (MFederline for)
DATE	8/18/04; 10/6/04	8/27/04	9/ 20/04	8/19/04	8/26/04
OFFICE	OCIO	OGC	TechEditor	D:NRR	EDO
NAME	JSilber	JGoldberg (w/comments)	PKleene	JDyer (RBorchardt for)	LReyes
DATE	8/17/04	8/30/04	8/16/04	8/30/04	10/19/04

OFFICIAL RECORD COPY

Handling of Sensitive Unclassified (Nonsafeguards) Information on Nuclear Power Reactors That Could Reasonably Be Expected to Be Useful to a Potential Adversary

Safeguards information (SGI) is information not otherwise classified as national security information or restricted data which specifically identifies a licensee's or applicant's detailed, (1) security measures for the physical protection of special nuclear material or (2) security measures for the physical protection and location of certain plant equipment vital to the safety of production or utilization facilities. However, there may be information that could reasonably be expected to be useful to a potential adversary that does not meet the requirements established for designating the information as SGI. This information will be treated as sensitive unclassified (non-SGI) information in accordance with established agency procedures and regulations. Information obtained from or provided to licensees and determined to be sensitive unclassified (non-SGI) information should be treated similar to commercial or financial information and withheld from public disclosure under 10 CFR 2.390. Information shared with other government agencies and licensees may be treated in a similar fashion unless addressed by other handling requirements (e.g., sensitive homeland security information).

In determining what information "could reasonably be expected to be useful to potential adversaries," one needs to assess the relevance of the specific information to an adversary's ability to plan or execute an attack or other malevolent act and the ability of a licensee or government agency to respond to such an attack. The discussion below is not intended to exemplify detailed threat or vulnerability assessments since decisions regarding the release or withholding of most information are expected to be made at the staff level within each program office. It is presented here to provide a thought process that has generally been consistent with the staff's intuitive evaluation of information.

The control of information needs to consider the following factors:

- The threat

  The control of information as part of an overall program to safeguard against the intentional release of radioactive materials needs to consider those threats for which the withholding of information might be helpful. The assessment is not limited to or even related to the design basis threat (DBT) but should consider the entire range of possible malevolent acts against a nuclear power reactor or other licensed activity. The assessments and evaluations are, at this point, based largely on staff judgments unless more detailed simulations or vulnerability assessments are available. The wide range of possible attacks against a nuclear power plant means that few issues will be decided based on the absence of a credible threat. For example, detailed layout drawings of the facility are to be withheld to ensure they do not assist adversaries in planning an attack on critical plant systems even though a security program is in place to thwart such an attack. The primary protection against an attack on a nuclear power plant is the security program. Information related to the security program that is not otherwise designated as SGI (e.g., information on training, inspection reports, performance assessments) may provide insights into the program and is likely to be withheld in accordance with 10 CFR 2.390.

- The consequences

  For each of the possible threats, there is a possible consequence in terms of harm to the public. The consequences of events involving NRC licensees, including nuclear reactors, include the possible release of radioactive materials that might adversely affect public health and safety. In the worst case, an attack on a nuclear reactor could cause plant transients and losses of mitigating systems, leading to core damage and a major release of fission products. The consequences for other threats could involve lesser releases (e.g., from waste systems) or possibly no releases of radioactive materials. The possible consequences associated with a particular licensed activity is usually reflected in the licensing processes and regulatory controls placed on those activities. The decision to withhold or release information needs to consider the possible consequences of events such that our controls on information correlate to the potential harm (i.e., information would not be treated as sensitive unless it relates to the potential release or diversion of radioactive materials posing a threat to public health and safety). Information related to events that are analyzed and result in doses below established regulatory thresholds (including many design basis accidents) may be released since the consequences have been determined to result in minimal risk to the public health and safety. The staff should consider the possible combinations of events and potential losses of mitigating systems that might result from a terrorist attack before concluding too quickly that the consequences of a threat are adequately addressed by an existing licensing-basis type analysis.

- The relationship of design/operating limits to security programs

  Information related to security programs at nuclear reactors is generally designated SGI and is protected in a manner similar to classified confidential information. For nuclear reactors, the security program is quite extensive and is established to prevent the loss of the engineering barriers designed to prevent the release of radioactive materials. Information regarding the engineering barriers themselves has been part of the public record. The design information may be withheld when it is used in the context of a security-related vulnerability assessment. For example, the traditional analysis of a structure against design basis winds will be released but an analysis related to structural failures from an explosive charge will be withheld.

- The availability of information from other sources

  In assessing the control of information, it is important to assess the availability of the information or similar information from sources outside the control of the NRC or its licensees. If the information is available from open source literature such as text books, Web sites, or other sources, an NRC decision to withhold the information may decrease the openness of our regulatory programs without obstructing an adversary. For example:

  < Information on the geospatial coordinates for facilities is released since this information is readily available in the public realm

  < Information on evacuation routes is released since it is routinely provided to the public for emergency planning purposes

< Information clearly visible from locations accessible to the public near the site is generally released. This includes general (low-resolution) layout drawings of the site and adjacent areas, including drawings showing the plant connections to the electric transmission system.

< Information related to the general workings of a nuclear power plant such as the descriptions usually provided in licensing documents (e.g., updated final safety analysis reports, license renewal applications) are released since similar information (at the level useful to a potential adversary) is available in open source literature such as text books and Internet sites. This level of information includes listings and general descriptions of safety-related and important-to-safety systems (including nonsecurity-related probabilistic risk assessments such as those included in accident sequence precursor analyses, risk-informed changes to technical specifications, and significance determination process notebooks). Information regarding such systems will be withheld in a context such as a vulnerability assessment (e.g., how a system might be affected by attacks or other malevolent acts).

- The subsequent controls on the information

In deciding to withhold information coming to or issued by the NRC, we need to consider how the information will be controlled by other parties with access to it. For example, we may negatively affect our goals regarding effectiveness or openness if we strive to withhold information and the information is then released by a licensee or other government agency. DHS may develop requirements or guidance for controlling information shared between licensees and Federal, State, and local governments when the information is designated “sensitive homeland security information.”

This assessment will also address how the information and its controls are incorporated into other licensee and regulatory processes. For example, COMSECY-03-0036 discussed the removal of some specific information from final safety analysis reports (FSARs) to address potential security concerns and the subsequent restoration of the FSARs to the public domain without the need to develop public/nonpublic versions. The proposed handling of FSARs described in COMSECY-03-0036 was also intended to minimize potential adverse effects on regulatory programs such as the evaluations required by 10 CFR 50.59, “Changes, tests, and experiments.” Any concerns regarding conflicting determinations (e.g., a finding that information should be withheld due to an assessment of its possible usefulness to an adversary and a regulatory need to make the information public) should be reported to agency management for resolution.

- The requirements and guidance established by other government agencies

  In deciding on the appropriate handling of information received from or provided to licensees, the staff should consider whether rules or guidance from other Federal agencies are in play. If the information is received from another agency and is identified by that agency as sensitive unclassified information, the staff should honor the designation and handle the information accordingly. Most information addressed by other federal agencies and of concern to the NRC staff or reactor licensees relates to infrastructure located near the nuclear power plant. Examples are the designation critical energy infrastructure information (CEII) for information related to hydroelectric dams regulated by the Federal Energy Regulatory Commission (FERC) and the withholding of maps showing pipelines under the jurisdiction of the Department of Transportation. The staff should make every effort to follow the guidance of other agencies in the review and designation of information related to facilities or activities for which another agency has the lead authority. Most of the Information on electric transmission systems provided to FERC (through its periodic Form 715) is designated CEII. Some documents provided to the NRC (e.g., updated final safety analysis reports and environmental reports related to license renewal applications) include information on electric transmission lines associated with nuclear power reactors. The information usually provided to the NRC is a subset of the information reported to FERC and relates only to power lines easily visible from the site environs. The NRC will need to make public some information on electric transmission systems supporting nuclear power plants since the information is integral to major licensing decisions and related environmental findings.

The staff has applied the above guidance to information routinely exchanged between licensees and the NRC to help the staff and licensees evaluate and control documents. The example subjects addressed in the following table include the technical areas identified in Regulatory Guide 1.70, “Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants,” as well as several other subjects addressed in routine correspondence associated with nonsecurity-related activities for nuclear power reactors. Information presented in the context of vulnerability assessments or other security-related matters will usually be withheld from public disclosure. These or similar examples will be included in guidance documents and will be routinely updated for use by the staff and licensees.

Control of Information by Subject Matter

Subject	Discussion and/or typical controls
General Description of Plant	Decisions regarding the control of information (usually drawings) that describe plant sites and buildings are dependent on the level of detail. Information clearly visible from locations accessible to the public near the site is generally released. This includes general (low-resolution) layout drawings of the site and adjacent areas. Drawings showing details such as the specific locations of equipment within buildings, doorways, stairways, etc. are to be withheld under 10 CFR 2.390.

Subject	Discussion and/or typical controls
Site Characteristics:	
Geography and demography	Uncontrolled
Nearby Industrial, transportation, and military facilities	Guidance related to the control of information related to non-nuclear facilities located near nuclear power plants may be available from other federal agencies (e.g., DHS, FERC, EPA, DOT). The staff should make every effort to follow the guidance of other agencies in the review and designation of information related to facilities or activities for which another agency has the lead authority. Specific examples include pipeline data (usually withheld per DOT) and chemical facilities (some data withheld per EPA). In addition to the guidance from other agencies, the staff will also withhold information related to nearby industrial facilities if the information might reasonably be helpful to those planning an attack on a nuclear power plant.
Meteorology	Uncontrolled
Hydrologic Engineering	Uncontrolled with the exception of information regarding the design of nearby dams. Information on dams may be designated critical energy infrastructure information by FERC.
Geology, seismology, and geotechnical engineering	Uncontrolled
Design of Structures, Components, Equipment, and Systems	Information regarding the design of structures provided to the NRC typically consists of analyses to show that the design feature will withstand the combinations of forces associated with design basis events and natural hazards. The analyses do not typically provide realistic information on the failure of structural features and are not considered sensitive. Information related to actual structural failures that could be useful to terrorists will be withheld.
Reactor (Nuclear, Thermal-hydraulic designs, Materials)	Uncontrolled
Reactor Coolant System	Uncontrolled

Subject	Discussion and/or typical controls
Engineered Safety Features	Information provided to the NRC on engineered safety features usually relates to their design, maintenance, or operation during routine activities or design basis transients (i.e., nonsecurity related events) and is not treated as sensitive. Detailed layout drawings showing the actual location of equipment is withheld under 10 CFR 2.390. Discussions of safety features or mitigation strategies within vulnerability assessments will also be withheld from public disclosure.
Instrumentation and Controls	Uncontrolled
Electric Power	Information provided to the NRC on offsite and onsite electric power systems typically relate to their design, maintenance, or operation during routine activities or design basis transients (i.e., nonsecurity related events) and is not treated as sensitive. It is necessary for the NRC to make public some information on electric transmission systems supporting nuclear power plants since the information is integral to major licensing decisions and related environmental findings (e.g., information usually provided with license renewal applications). Information on the transmission grid beyond that needed for NRC regulatory decisions is likely to be withheld in accordance with the FERC guidance on critical energy infrastructure information.
Auxiliary Systems (Fuel storage, ultimate heat sink)	Uncontrolled- This includes general (low-resolution) layout drawings of the site and descriptions and drawings such as the arrangement of spent fuel within spent fuel pools. Drawings showing details such as the specific location of equipment, doorways, stairways, etc. are to be withheld under 10 CFR 2.390.
Steam and Power Conversion	Uncontrolled
Radioactive Waste Management	Uncontrolled - This includes general (low-resolution) layout drawings of the site. Drawings showing details such as the specific location of equipment, doorways, stairways, etc. are to be withheld under 10 CFR 2.390.
Radiation Protection	Uncontrolled - This includes general (low-resolution) layout drawings of the site and adjacent areas. Drawings showing details such as the specific location of equipment, doorways, stairways, etc. are to be withheld under 10 CFR 2.390.
Conduct of Operations	Uncontrolled (excluding security)

Subject	Discussion and/or typical controls
Test Program (Initial and Inservice Inspections and Testing)	Uncontrolled
Accident Analysis	Uncontrolled - Accident analyses typically included in licensing-related correspondence involve conservative models to demonstrate a plant's ability to respond to design basis transients (i.e., nonsecurity related events), and is not treated as sensitive.
Technical Specifications (including Bases)	Uncontrolled
Quality Assurance	Uncontrolled
Fire Protection	Incoming documents are initially profiled as nonpublic - staff will review for release upon request. Most information related to fire protection will not need to be designated as sensitive. Drawings showing details such as the specific location of equipment, doorways, stairways, etc. are to be withheld under 10 CFR 2.390.
Emergency Planning	Incoming documents are initially profiled as nonpublic - staff will review for release upon request. Most information related to emergency planning will not need to be designated as sensitive. Special attention is needed to determine if information relates to the response by a licensee or government agency to a terrorist attack. Note that some State and local governments consider parts of their emergency plans to be sensitive.
Security	Information related to security programs at nuclear reactors is generally designated as SGI and is protected in a manner similar to classified confidential information. Security-related information within the inspection program and reactor oversight process is withheld from public disclosure under 10 CFR 2.390.
Risk-Informed Decisionmaking (e.g., documents related to risk-informed licensing actions, accident sequence precursor (ASP) analyses, significance determination process (SDP) notebooks, design certifications)	Uncontrolled - exceptions include information related to security activities (e.g., vulnerability assessments) and information related to uncorrected configurations or conditions that could be useful to an adversary. Special attention should be applied to this area and information should be withheld if it describes a vulnerability or plant-specific weakness that is more helpful to an adversary than are the insights provided in open source literature. Detailed computer models have been and will continue to be withheld from public disclosure.

Subject	Discussion and/or typical controls
Inspections & Performance Assessment	Uncontrolled - exceptions include information on security-related inspections or performance assessments and information related to uncorrected vulnerabilities that could be useful to an adversary.
Current Plant Configurations	Information on current plant configurations or conditions that could be useful to an adversary (e.g., important safety equipment out of service) is withheld from public disclosure (usually by simply timing its release) until such time as the information no longer reflects current plant conditions.

Terminology and Other Government Designations

Several discussions or definitions related to this issue are provided below:

- **Section 147, "Safeguards Information," of the Atomic Energy Act, as amended, 42 USC §2167, states:**

  a. In addition to any other authority or requirement regarding protection from disclosure of information, and subject to subsection (b)(3) of section 552 of title 5, the Commission shall prescribe such regulations, after notice and opportunity for public comment, or issue such orders, as necessary to prohibit the unauthorized disclosure of safeguards information which specifically identifies a licensee's or applicant's detailed -

  (1) control and accounting procedures or security measures (including security plans, procedures, and equipment) for the physical protection of special nuclear material, by whomever possessed, whether in transit or at fixed sites, in quantities determined by the Commission to be significant to the public health and safety or the common defense and security;

  (2) security measures (including security plans, procedures, and equipment) for the physical protection of source material or byproduct material, by whomever possessed, whether in transit or at fixed sites, in quantities determined by the Commission to be significant to the public health and safety or the common defense and security; or

  (3) security measures (including security plans, procedures, and equipment) for the physical protection of and the location of certain plant equipment vital to the safety of production or utilization facilities involving nuclear materials covered by paragraphs (1) and (2) if the unauthorized disclosure of such information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of theft, diversion, or sabotage of such material or such facility. The Commission shall exercise the authority of this subsection -

  (A) so as to apply the minimum restrictions needed to protect the health and safety of the public or the common defense and security, and

  (B) upon a determination that the unauthorized disclosure of such information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of theft, diversion, or sabotage of such material or such facility.

- **§ 73.2 Title 10 of Code Federal Regulations**

  Safeguards Information means information not otherwise classified as National Security Information or Restricted Data which specifically identifies a licensee's or applicant's detailed, (1) security measures for the physical protection of special nuclear material, or (2) security measures for the physical protection and location of certain plant equipment vital to the safety of production or utilization facilities.

- **§ 73.21 Title 10 of Code Federal Regulations**

  (b) *Information to be protected*. The specific types of information, documents, and reports that shall be protected are as follows:
  (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:
  (i) The composite physical security plan for the nuclear facility or site.
  (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.
  (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:
(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).
(4) *Correspondence*. Portions of correspondence insofar as they contain Safeguards Information specifically defined in paragraphs (b)(1) through (b)(3) of this paragraph.

- **Critical Infrastructure Information is defined in Title 6 CFR Part 29 as:**

Critical Infrastructure Information, or CII means information not customarily in the public domain and related to the security of critical infrastructure or protected systems. CII consists of records and information concerning: (1) Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms the interstate commerce of the United States, or threatens public health or safety; (2) The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation, risk-management planning, or risk audit; or (3) Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

- **Protected CII is defined in Title 6 CFR Part 29 as:**

  Protected Critical Infrastructure Information, or Protected CII means CII (including the identity of the submitting person or entity) that is voluntarily submitted to DHS for its use regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement as described in Sec. 29.5. This information maintains its protected status unless DHS's Protected CII Program Manager or the Protected CII Program Manager's designees render a final decision that the information is not Protected CII.

- **Homeland Security Information is defined in Section 892(f)(1) of the Homeland Security Act of 2002, 6 USC 482, as:**

  any information possessed by Federal, State, or local agency that:
  (A) relates to the threat of terrorist activity;
  (B) relates to the ability to prevent, interdict, or disrupt terrorist activity;
  (C) would improve the identification or investigation of a suspected terrorist or terrorists organization; or
  (D) would improve the response to a terrorist act."

- **Sensitive Homeland Security Information**

  The Department of Homeland Security continues to develop guidance related to sensitive homeland security information (SHSI). The staff will continue to monitor the DHS activities in this area. The definition is expected to be related to the definition of homeland security information provided above. The designation of information as SHSI would be expected to help protect the information from public disclosure while also maintaining the free flow of such information between Federal, State, and Local governments.

- **Critical Energy Infrastructure Information**

  The Federal Energy Regulatory Commission has provided a definition of Critical Energy Infrastructure Information in their regulations at 18 CFR Parts 375 and 388. § 388.113 states :

  (1) Critical energy infrastructure information means information about proposed or existing critical infrastructure that: (i) Relates to the production, generation, transportation, transmission, or distribution of energy; (ii) Could be useful to a person in planning an attack on critical infrastructure; (iii) Is exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 552; and (iv) Does not simply give the location of the critical infrastructure.

- **Sensitive Security Information (Transportation)**

The Transportation Safety Administration and Department of Transportation have provided the following definition of "sensitive security information" or SSI in their regulations at 49 CFR Part 15. See interim final rule published May 18, 2004 (69 FR 28066).
Sec. 15.5 Sensitive security information.
(a) In general. In accordance with 49 U.S.C. 40119(b)(1), SSI is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which the Secretary of DOT has determined would-- (1) Constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file); (2) Reveal trade secrets or privileged or confidential information obtained from any person; or (3) Be detrimental to transportation safety. (b) Information constituting SSI. Except as otherwise provided in writing by the Secretary of DOT in the interest of public safety or in furtherance of transportation security, the following information, and records containing such information, constitute SSI:
(1) Security programs and contingency plans. Any security program or security contingency plan issued, established, required, received, or approved by DOT or DHS, including-- (i) Any aircraft operator or airport operator security program or security contingency plan under this chapter; (ii) Any vessel, maritime facility, or port area security plan required or directed under Federal law; (iii) Any national or area security plan prepared under 46 U.S.C. 70103; and (iv) Any security incident response plan established under 46 U.S.C. 70104.
(2) Security Directives. Any Security Directive or order-- (i) Issued by TSA under 49 CFR 1542.303, 1544.305, or other authority; (ii) Issued by the Coast Guard under the Maritime Transportation Security Act, 33 CFR part 6, or 33 U.S.C. 1221 et seq. related to maritime security; or (iii) Any comments, instructions, and implementing guidance pertaining thereto.
(3) Information Circulars. Any notice issued by DHS or DOT regarding a threat to aviation or maritime transportation, including any-- (i) Information Circular issued by TSA under 49 CFR 1542.303 or 1544.305, or other authority; and (ii) Navigation or Vessel Inspection Circular issued by the Coast Guard related to maritime security.
(4) Performance specifications. Any performance specification and any description of a test object or test procedure, for-- (i) Any device used by the Federal government or any other person pursuant to any aviation or maritime transportation security requirements of Federal law for the detection of any weapon, explosive, incendiary, or destructive device or substance; and (ii) Any communications equipment used by the Federal government or any other person in carrying out or complying with any aviation or maritime transportation security requirements of Federal law.
(5) Vulnerability assessments. Any vulnerability assessment directed, created, held, funded, or approved by the DOT, DHS, or that will be provided to DOT or DHS in support of a Federal security program.

(6) Security inspection or investigative information. (i) Details of any security inspection or investigation of an alleged violation of aviation or maritime transportation security requirements of Federal law that could reveal a security vulnerability, including the identity of the Federal special agent or other Federal employee who conducted the inspection or audit. (ii) In the case of inspections or investigations performed by TSA, this includes the following information as to events that occurred within 12 months of the date of release of the information: the name of the airport where a violation occurred, the airport identifier in the case number, a description of the violation, the regulation allegedly violated, and the identity of any aircraft operator in connection with specific locations or specific security procedures. Such information will be released after the relevant 12-month period, except that TSA will not release the specific gate or other location on an airport where an event occurred, regardless of the amount of time that has passed since its occurrence. During the period within 12 months of the date of release of the information, TSA may release summaries of an aircraft operator's, but not an airport operator's, total security violations in a specified time range without identifying specific violations or locations. Summaries may include total enforcement actions, total proposed civil penalty amounts, number of cases opened, number of cases referred to TSA or FAA counsel for legal enforcement action, and number of cases closed.
(7) Threat information. Any information held by the Federal government concerning threats against transportation or transportation systems and sources and methods used to gather or develop threat information, including threats against cyber infrastructure.
(8) Security measures. Specific details of aviation or maritime transportation security measures, both operational and technical, whether applied directly by the Federal government or another person, including-- (i) Security measures or protocols recommended by the Federal government; (ii) Information concerning the deployments, numbers, and operations of Coast Guard personnel engaged in maritime security duties and Federal Air Marshals, to the extent it is not classified national security information; and (iii) Information concerning the deployments and operations of Federal Flight Deck Officers, and numbers of Federal Flight Deck Officers aggregated by aircraft operator. (9) Security screening information. The following information regarding security screening under aviation or maritime transportation security requirements of Federal law: (i) Any procedures, including selection criteria and any comments, instructions, and implementing guidance pertaining thereto, for screening of persons, accessible property, checked baggage, U.S. mail, stores, and cargo, that is conducted by the Federal government or any other authorized person. (ii) Information and sources of information used by a passenger or property screening program or system, including an automated screening system. (iii) Detailed information about the locations at which particular screening methods or equipment are used, only if determined by TSA to be SSI. (iv) Any security screener test and scores of such tests. (v) Performance or testing data from security equipment or screening systems. [[Page 28080]] (vi) Any electronic image shown on any screening equipment monitor, including threat images and descriptions of threat images for threat image projection systems.
(10) Security training materials. Records created or obtained for the purpose of training persons employed by, contracted with, or acting for the Federal government or another person to carry out any aviation or maritime transportation security measures required or recommended by DHS or DOT.

(11) Identifying information of certain transportation security personnel. (i) Lists of the names or other identifying information that identify persons as-- (A) Having unescorted access to a secure area of an airport or a secure or restricted area of a maritime facility, port area, or vessel or; (B) Holding a position as a security screener employed by or under contract with the Federal government pursuant to aviation or maritime transportation security requirements of Federal law, where such lists are aggregated by airport; (C) Holding a position with the Coast Guard responsible for conducting vulnerability assessments, security boardings, or engaged in operations to enforce maritime security requirements or conduct force protection; (D) Holding a position as a Federal Air Marshal; or (ii) The name or other identifying information that identifies a person as a current, former, or applicant for Federal Flight Deck Officer.
(12) Critical aviation or maritime infrastructure asset information. Any list identifying systems or assets, whether physical or virtual, so vital to the aviation or maritime transportation system that the incapacity or destruction of such assets would have a debilitating impact on transportation security, if the list is-- (i) Prepared by DHS or DOT; or (ii) Prepared by a State or local government agency and submitted by the agency to DHS or DOT.
(13) Systems security information. Any information involving the security of operational or administrative data systems operated by the Federal government that have been identified by the DOT or DHS as critical to aviation or maritime transportation safety or security, including automated information security procedures and systems, security inspections, and vulnerability information concerning those systems.
(14) Confidential business information. (i) Solicited or unsolicited proposals received by DHS or DOT, and negotiations arising therefrom, to perform work pursuant to a grant, contract, cooperative agreement, or other transaction, but only to the extent that the subject matter of the proposal relates to aviation or maritime transportation security measures; (ii) Trade secret information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out aviation or maritime transportation security responsibilities; and (iii) Commercial or financial information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out aviation or maritime transportation security responsibilities, but only if the source of the information does not customarily disclose it to the public.
(15) Research and development. Information obtained or developed in the conduct of research related to aviation or maritime transportation security activities, where such research is approved, accepted, funded, recommended, or directed by the DHS or DOT, including research results.
(16) Other information. Any information not otherwise described in this section that TSA determines is SSI under 49 U.S.C. 114(s) or that the Secretary of DOT determines is SSI under 49 U.S.C. 40119. Upon the request of another Federal agency, the Secretary of DOT may designate as SSI information not otherwise described in this section.

- **Sensitive Security Information (Agriculture)**

  The USDA's Departmental Regulation 3440-2, "Control and Protection of Sensitive Security Information," defines sensitive security information as follows:

  Sensitive Security Information means unclassified information of a sensitive nature, that if publicly disclosed could be expected to have a harmful impact on the security of Federal operations or assets, the public health or safety of the citizens of the United States or its residents, or the nation's long-term economic prosperity; and which describes, discusses, or reflects:

  (1) The ability of any element of the critical infrastructure of the United States to resist intrusion, interference, compromise, theft, or incapacitation by either physical or computer-based attack or other similar conduct that violates Federal, State, or local law; harms interstate, international commerce of the United States; or, threatens public health or safety;

  (2) Any currently viable assessment, projection, or estimate of the security vulnerability of any element of the critical infrastructure of the United States, specifically including, but not limited to vulnerability assessment, security testing, risk evaluation, risk-management planning, or risk audit;

  (3) Any currently applicable operational problem or solution regarding the security of any element of the critical infrastructure of the United States, specifically including but not limited to the repair, recovery, redesign, reconstruction, relocation, insurance, and continuity of operations of any element;

  (4) The following categories are provided for illustration purposes only as examples of the types of information (regardless of format) that may be categorized as SSI:

      1 Physical security status of USDA laboratories, research centers, field facilities, etc., which may also contain vulnerabilities;

      2 Investigative and analytical materials concerning information about physical security at USDA facilities such as the above-named facilities;

      3 Information that could result in physical risk to individuals;

      4 Information that could result in serious damage to critical facilities and/or infrastructures;

      5 Cyber Security Information, which includes, but is not limited to:

        (a) Network Drawings or Plans
        (b) Program and System Security Plans
        (c) Mission Critical and Sensitive Information Technology (IT) Systems and Applications
        (d) Capital Planning and Investment Control Data (I-TIPS)
        (e) IT Configuration Management Data and Libraries
        (f) IT Restricted Space (Drawings, Plans and Equipment Specifications as well as actual space)
        (g) Incident and Vulnerability Reports
        (h) Risk Assessment Reports, Checklists, Trusted Facilities Manual and Security Users Guide
        (i) Cyber Security Policy Guidance and Manual Chapters